



# **MONEY LAUNDERING AND TERRORIST FINANCING NATIONAL RISK ASSESSMENT REPORT**

**10 MAY 2018**

## Appreciation

The process of conducting the National Risk Assessment (NRA) on money laundering and terrorist financing was approved by the Ministry of Finance, Economic Planning and Development in mid-2017. The Financial Intelligence Authority (FIA) would like to thank the Minister and the Secretary to the Treasury for their acceptance of this project.



The FIA further expresses its gratitude to the Department for International Development (DfID) of the United Kingdom for its technical and financial support towards this project.

The support provided through the Basel Institute on Governance comprised the technical services of a consultant, Dr. Giuseppe Lombardo, and financial support for workshops and meetings facilitated by the Country Program Manager for the International Centre for Asset Recovery (ICAR), Mrs. Joan D'Souza.

In addition, the FIA is highly indebted to all heads of public and private sector institutions who allowed their officers to participate in this exercise. Their commitment has made this project a reality.

As we enter the phase of implementation of the NRA recommendations, it is my hope that the institutions will continue being committed to ensuring that the identified gaps are addressed.

Atuweni Juwayeyi-Agbermodji  
DIRECTOR GENERAL  
**FINANCIAL INTELLIGENCE AUTHORITY**

## Contents

	Page
<b>1 RISK ASSESSMENT OVERVIEW</b> .....	<b>2</b>
1.1 Introduction .....	2
1.2 Objectives .....	2
1.3 Methodology .....	3
1.4 Limitations .....	5
1.5 Executive Summary .....	6
1.5.1 Analysis of the ML Threat.....	8
1.5.2 Analysis of the Terrorism/TF Threat and TF Vulnerability .....	9
1.5.3 National Vulnerability.....	10
1.5.4 Sectorial ML Vulnerabilities: Financial Sector .....	12
1.5.5 Designated Non-Financial Businesses and Professions .....	15
1.5.6 Financial Inclusion .....	16
<b>2 DETAILED PRESENTATION OF THE ASSESSMENT</b> .....	<b>0</b>
<b>2.1 Money Laundering Threat</b> .....	<b>0</b>
2.1.1 Introduction .....	0
2.1.2 Objectives.....	0
2.1.3 Overall Assessment of ML Risk.....	0
2.1.4 Overall ML Threat.....	0
2.1.5 Analysis of Foreign Threats .....	11
2.1.6 Sectoral Breakdown .....	12
2.1.7 Recommendations .....	13
<b>2.2 Terrorist Financing and Terrorism Threat Analysis</b> .....	<b>13</b>
2.2.1 Background .....	13
2.2.2 Part A – Terrorism Threat.....	14
2.2.3 Part B – TF Threat.....	15
2.2.4 Part C – Terrorism Financing Vulnerability.....	18
2.2.5 Strengths, Weakness and Key Recommendations .....	21
<b>2.3 National Vulnerability to Money Laundering</b> .....	<b>23</b>
2.3.1 Background .....	23
2.3.2 National Combating Ability .....	0
2.3.3 Quality of AML Policy and Strategy .....	0
2.3.4 Effectiveness of ML Crime Definition .....	1
2.3.5 Comprehensiveness of Asset Forfeiture Laws.....	3
2.3.6 Quality of FIU Intelligence Gathering and Processing .....	5
2.3.7 Capacity and Resources for Financial Crime Investigations (including Asset Forfeiture) .....	8
2.3.8 Integrity and Independence of Financial Crime Investigators .....	11
2.3.9 Integrity and Independence of Financial Crime Prosecutors .....	12
2.3.10 Capacity and Resources for Judicial Processes (including Asset Forfeiture).....	12
2.3.11 Integrity and Independence of Judges (including Asset Forfeiture) .....	13
2.3.12 Quality of Border Controls.....	14
2.3.13 Comprehensiveness of Customs Regime on Cash and Similar Instruments .....	15
2.3.14 Effectiveness of Customs Controls on Cash and Similar Instruments .....	15
2.3.15 Effectiveness of Domestic Cooperation .....	16

2.3.16	Effectiveness of International Cooperation.....	17
2.3.17	Availability of Independent Audits .....	18
2.3.18	Level of Financial Integrity.....	20
2.3.19	Effectiveness of Tax Enforcement .....	21
2.3.20	Level of Formalisation of the Economy .....	23
2.3.21	Availability of Reliable Identification Infrastructure .....	24
2.3.22	Availability of Independent Information Sources .....	25
2.3.23	Availability and Access to Beneficial Ownership Information.....	26
<b>2.4</b>	<b>Banking Sector Vulnerability .....</b>	<b>26</b>
2.4.1	Background .....	26
2.4.2	Overall Vulnerability.....	28
2.4.3	Assessment of Variables.....	28
2.4.4	Assessment of General Input Variables.....	28
2.4.5	Assessment of Product Variables .....	37
2.4.6	Recommendations for the Sector .....	44
<b>2.5</b>	<b>Insurance Sector Vulnerability .....</b>	<b>45</b>
2.5.1	Background .....	45
2.5.2	Overall Vulnerability.....	46
2.5.3	Assessment of Variables.....	46
2.5.4	Product-Specific Input.....	50
2.5.5	Deficiencies / Gaps Identified and Proposed Actions to Rectify the Issues.....	60
<b>2.6</b>	<b>Securities Sector Vulnerability.....</b>	<b>61</b>
2.6.1	Background .....	61
2.6.2	Overall ML Risk Assessment .....	62
2.6.3	Sub-Sectors Assessment.....	63
<b>2.7</b>	<b>Other Financial Institutions Vulnerability .....</b>	<b>70</b>
2.7.1	Background .....	70
2.7.2	Money Transfer Operators (MTOs).....	71
2.7.3	Foreign Exchange Bureaus (FEBs) .....	76
2.7.4	Mobile Payment Services .....	81
2.7.5	Microfinance Institutions Vulnerability.....	86
<b>2.8</b>	<b>Designated Non-Financial Businesses and Professions Vulnerability .....</b>	<b>91</b>
2.8.1	Background .....	91
2.8.2	DNFBPs Overall Assessment.....	92
2.8.3	Casinos .....	93
2.8.4	Dealers in Precious Metals and Precious Stones.....	101
2.8.5	Lawyers .....	106
2.8.6	Accountants .....	111
2.8.7	Real Estate.....	116
<b>2.9</b>	<b>Non-Governmental Organisations Vulnerability.....</b>	<b>123</b>
2.9.1	Background .....	123
2.9.2	Definition of an NGO.....	124
2.9.3	Reporting Requirements .....	126
2.9.4	Source of Funds of NGOs .....	127
2.9.5	Adverse Reports to NGO Board and CONGOMA and How they were Handled .....	128
2.9.6	Recommendations .....	129

<b>2.10</b>	<b>Legal Persons and Arrangements Vulnerability .....</b>	<b>129</b>
2.10.1	Background .....	129
2.10.2	Assessment of Vulnerability .....	129
2.10.3	Corporate Entities .....	129
2.10.4	Relevant Observations on the Companies Act 2013 .....	132
2.10.5	Business Names Registration under Business Registration Act of 2012 .....	133
2.10.6	Incorporation under Trustees Incorporation Act .....	134
2.10.7	Settlement/Private Trusts .....	134
2.10.8	Accessibility of Information by LEAs on Legal Persons and Arrangements Created .....	134
2.10.9	Features of Legal Arrangements That Make Them Particularly Vulnerable to ML .....	134
<b>2.11</b>	<b>Financial Inclusion Products Vulnerability .....</b>	<b>136</b>
2.11.1	Background .....	136
2.11.2	Findings .....	137
2.11.3	Recommendations .....	147
<b>3</b>	<b>CONCLUSION .....</b>	<b>0</b>
<b>4</b>	<b>APPENDIX 1 – NRA ACTION PLAN .....</b>	<b>2</b>

## List of Tables

Table 1: Malawi's overall ML risk.....	7
Table 2: Estimate of proceeds from criminal offences.....	1
Table 3: Estimate of proceeds laundered.....	3
Table 4: Tax crime cases.....	7
Table 5: Wildlife cases.....	9
Table 6: Statistics of STRs received by the FIA.....	7
Table 7: Banking sector supervision.....	29
Table 8: Administrative sanctions imposed on banks.....	31
Table 9: Statistics of training for bank staff.....	33
Table 10: Statistics of STRs filed by banks.....	35
Table 11: Banking products vulnerability to ML.....	37
Table 12: Insurance products ML assessment.....	51
Table 13: Prioritisation of general AML controls for insurance sector.....	61
Table 14: Prioritisation of general AML controls for securities sector.....	69
Table 15: Regulation of other financial institutions.....	70
Table 16: Profile of regulated OFIs.....	70
Table 17: Priority ranking for AML controls for the Other Financial Institutions sector.....	90
Table 18: DNFBP sub-sectors overall assessment.....	93
Table 19: Prioritisation of general AML controls for DNFBPs.....	122

## List of Figures

Figure 1: Malawi's vulnerability to ML.....	0
Figure 2: Insurance products vulnerability to ML.....	51
Figure 3: Securities products vulnerability to ML.....	62
Figure 4: DNFBPs ML risk.....	92

## Abbreviations and Acronyms

ACB	Anti-Corruption Bureau
AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism
BAM	Bankers Association of Malawi
CDD	Customer Due Diligence
DNPW	Department of National Parks and Wildlife
DNFBPs	Designated Non-Financial Businesses and Professions
DPMS	Dealers in Precious Metals and Stones
DPP	Directorate of Public Prosecution
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
FATF	Financial Action Task Force
FCA	Financial Crimes Act
FIA	Financial Intelligence Authority
FIU	Financial Intelligence Unit
GAM	Gemstones Association of Malawi
ICAR	International Centre for Asset Recovery
IPO	Initial Public Offer
KYC	Know Your Customer
LEAs	Law Enforcement Agencies
MAWIMA	Malawi Women in Mining Association
MGB	Malawi Gaming Board
MoJ	Ministry of Justice
ML Act	Money Laundering, Proceeds of Serious Crime and Terrorist Financing Act
MRA	Malawi Revenue Authority
MoFEPD	Ministry of Finance, Economic Planning and Development
ML	Money Laundering
MWEITI	Malawi Extractive Industries Transparency Initiative
NGOs	Non-Governmental Organisation
NRA	National Risk Assessment
OFAC	Office of Foreign Assets Control – U.S. Department of Treasury
PEP	Politically Exposed Persons
RBA	Risk Based Approach
RBM	Reserve Bank Malawi
STR	Suspicious Transaction Report
TA	Technical Assistance
TC	Technical Compliance
TF	Terrorist Financing
UN	United Nations
UNSCR	United Nations Security Council Resolutions

## RISK ASSESSMENT OVERVIEW

---

### Introduction

This is a second report for Malawi on Money Laundering (ML) and Terrorist Financing (TF) self-assessment by the country using the National Risk Assessment (NRA) 5th generation Tool developed by the World Bank. The first assessment was done in 2013.

The authorities that took part in this assessment were as follows: Ministry of Finance, Economic Planning and Development; Ministry of Justice and Constitutional Affairs; Ministry of Foreign Affairs and Internal Cooperation; Ministry of Lands, Housing and Urban Development; Ministry of Defence; Financial Intelligence Authority (FIA); Reserve Bank of Malawi (RBM); Malawi Gaming Board (MGB); Malawi Revenue Authority (MRA); Directorate of Public Prosecutions (DPP); Malawi Police Service (MPS); Anti-Corruption Bureau (ACB); National Intelligence Bureau (NIB); Department of Immigration and Citizenship Services; Department of National Parks and Wildlife (DNPW); Department of Mines; Department of the Registrar General; Non-Governmental Organisation (NGO) Board; Council for non-governmental organisations in Malawi (CONGOMA); Malawi Law Society (MLS); Bankers Association of Malawi (BAM); Life Insurance and Pensions Association of Malawi; Insurance Association of Malawi; Insurance Brokers Association of Malawi; Association of Real Estate Agents (AREA); Institute of Chartered Accountants in Malawi (ICAM), and Malawi Microfinance Network (MAMN).

The Basel Institute on Governance through ICAR provided financial and technical support. Its role was limited to guidance on the use of the World Bank tool and review of the sub-group reports. The data was populated onto templates of the National Money Laundering and Terrorist Financing Risk Assessment Tool by Malawian authorities.

All findings, interpretations, and judgments under the scope of the NRA completely belong to the Malawian authorities and do not reflect the views of DfID, Basel Institute on Governance or ICAR.

### Objectives

The objectives of the NRA were:

- 1.1 Understand the level of proceeds of crime generated in Malawi or coming into Malawi and the ML/TF threat they pose;



- 1.2 Determine and understand the weakness in the legal framework, by considering the criminal and administrative justice system, and existing preventative systems;
- 1.3 To identify the overall ML and TF vulnerability of the various sectors assessed;
- 1.4 To identify products/services/channels with high ML/TF vulnerability;
- 1.5 To prioritise action plans that will strengthen AML/CFT in the various sectors assessed; and
- 1.6 Determine the best manner to allocate resources for the prevention, investigation and prosecution of ML and TF.

## Methodology

The NRA involved workshops which took place from 2nd to 5th October 2017 and 11 to 15th December 2017. During the first workshop, participants were divided into 10 sub-groups depending on their expertise. After this, the sub-groups gathered information from public and private sector sources. Following which they held their respective meetings in November 2017 to analyse the data and prepare draft reports which were reviewed by the consultant in December 2017 and January 2018. The consultant held meetings with the sub-groups separately from 4 to 8th December 2017 and 12 to 16th March 2018. After this, the report was consolidated and finalised.

The finalised report was presented to the Minister of Finance, Economic Planning and Development in early May 2018 for his approval with a view of disseminating it to stakeholders before the end of the 2017/2018 financial year.

The 10 sub-groups that looked at the country's risk and vulnerability to ML and TF as are briefly explained below:

*i) Sub-Group One – ML/TF Threat Analysis*

This sub-group analysed the ML/TF threat by identifying and compiling data on the criminal offences that generate proceeds of crime which can be laundered.

*ii) Sub-Group Two – TF Risk*

The sub-group assessed the level of internal and external terrorism and TF threat as well as TF vulnerability.

*iii) Sub-Group Three – National ML Vulnerability*

This sub-group analysed the national vulnerability to ML and TF by considering how well law enforcement agencies (LEAs) are equipped to tackle this problem. This included assessing the levels of training, integrity and resources in these institutions including how these institutions cooperate with one another and other institutions outside Malawi.

*iv) Sub-Group Four – Banking Sector Vulnerability*

The sub-group assessed the ML/TF vulnerability arising from provision of various bank products. The assessment involved analysing the volume of bank products and their inherent vulnerability and these were assessed against the AML general and product specific controls.

*v) Sub-Group Five – Insurance Sector Vulnerability*

The sub-group assessed the ML/TF vulnerability that arises from life and general insurance products. This also included an analysis of the control measures that are in place within the sector.

*vi) Sub-Group Six – Securities Sector Vulnerability*

The sub-group assessed the ML/TF vulnerability that arises from capital markets and related securities products. This also included an analysis of the control measures that are in place within the sector.

*vii) Sub-Group Seven – Other Financial Institutions' Vulnerability*

The sub-group assessed the ML/TF vulnerability that arises from foreign exchange bureaus, money remittance service providers, microfinance companies and mobile payment services. The assessment also included an analysis of the control measures that are in place within the sector. This sub-group combined with assessment of products under financial inclusion.

*viii) Sub-Group Eight – DNFBPs Vulnerability*

This sub-group analysed the ML/TF vulnerability of DNFBPs which included casinos; real estate; dealers in precious metals and precious stones, lawyers, and accountants.

*ix) Sub-Group Nine – Non-Governmental Organisations Vulnerability*

The sub-group analysed the TF vulnerability of non-profit making organisations (NPOs) which are known as non-governmental organisations (NGOs) in Malawi.

**x) Sub-Group Ten – Legal Persons and Arrangements Vulnerability**

The sub-group analysed the ML vulnerability of legal persons and arrangements. This was done through assessing the legal framework and practices in place regarding the legal persons and arrangements.

Data for the NRA was collected through the following methods:

- a) Databases of the FIA, RBM, MGB, DPP, MPS, ACB, MRA, NIB, Ministry of Lands, Housing and Urban Development; Ministry of Defence, Department of Mines, NGO Board, CONGOMA, MAMN, MLS and ICAM;
- b) Questionnaires administered to the financial institutions and DNFBPs;
- c) Review of publications by the RBM, FIA, MGB and other stakeholders;
- d) Telephone and face-to-face interviews with financial institutions and DNFBPs;
- e) Public information sources including Malawi's AML/CFT Mutual Evaluation Report (2008), Baker Tilly Report on the 2013 fraud in Malawi, 2013 Malawi National Risk Assessment Report, Malawi Money Laundering Typologies Reports (2011 & 2017) and other media publications; and
- f) Review of legislation which included the Financial Crimes Act (FCA); Financial Services Act (FSA), Banking Act, Reserve Bank of Malawi Act, Gaming Act, Penal Code, and National Parks and Wildlife (Amendment) Act 2017.

## Limitations

The NRA faced several limitations as outlined below:

- ML and TF issues are still relatively new to many stakeholders in Malawi. Before 2013, many people including law enforcement officers did not clearly understand the law on money laundering. Consequently, ML charges were easily ignored by investigators and prosecutors. Currently there is growing awareness especially with some convictions on *cash-gate* cases and most of the cases used in the NRA relate to the *cash-gate*.
- Proceeds generated from criminal activities are usually not captured in reports by LEAs hence it was difficult to come up with concrete statistics in some instance during this

assessment. Therefore, the major focus was the number of investigations, prosecution and convictions.

- LEAs also find it difficult to trace proceeds of crime because Malawi is still a predominantly cash-based economy where most transactions are conducted in cash and a significant percentage of people do not use financial services. The use of cash is an obstacle to tracing of proceeds of crime. While LEAs are able to find evidence on commission of an offence, often times they fail to trace the proceeds generated because most offenders prefer to use cash to avoid detection. This is common in wildlife crimes, corruption, human trafficking, theft and other crimes.
- For LEAs, there is no centralised database from which information can be easily accessed by LEAs. With some LEAs still handling data manually, this made data collection difficult.
- In some instances, inadequate data was available from the targeted sources such as LEAs and DNFBPs.

## Executive Summary

Malawi conducted its second National Risk Assessment (NRA) to assess its Money Laundering (ML) and Terrorism Financing (TF) risks from mid-2017 to May 2018. The first NRA was conducted from 2012 and approved in 2013 by the Minister of Finance.

This NRA analysed the ML threat to which the country is exposed and the major predicate offences that generate larger amounts of criminal proceeds, and the level of the terrorism threat the country faces. It also examined the country's ML/TF combating ability and the vulnerabilities of the financial sector as well as DNFBPs to ML/TF abuse, financial inclusion, the risk associated with the types of legal entities and arrangements that can be created in Malawi and the risk of the non-governmental organisations (NGO) sector. The NRA assessed how criminals utilise their ill-gotten funds and the methods they use to launder criminal proceeds. Furthermore, the NRA analysed the TF risk Malawi is facing.

The NRA was undertaken by a Working Group representing various government institutions and chaired by the Director General of the Financial Intelligence Authority (FIA). The assessment used the latest methodology developed by the World Bank and technical assistance provided by the Basel Institute of Governance, in the context of a project funded by DFID. It relied on both quantitative information (statistics and data) and qualitative information, such as surveys and interviews, including with representatives of financial and non-financial institutions and DNFBPs, which complemented the information and data provided by the members of the Working Group.

Although the country has a robust legal framework, which is largely in line with the international standard, there are some significant vulnerabilities that affect the overall ML and TF risk in some areas. Capacity issues affect, to different degrees, the ability of stakeholders to prevent and repress ML and TF in an effective manner. Other material elements such as the widespread use of cash, the informal economy, the only very recently introduced national ID system and porous borders increase the country’s vulnerability to ML and TF.

Malawi subjects to AML/CFT requirements all the types of financial institutions and DNFBPs required by the FATF standards. However, effective implementation of these requirements by reporting entities is uneven, and near absent in certain sectors, particularly the DNFBPs, which are not as supervised as FIs for AML/CFT compliance. Real estate, lawyers, dealers in precious metals and stones and some types of financial institutions present the highest risk to ML. Although the banking sector is the more compliant with and knowledgeable of AML/CFT requirements, most of the ongoing ML investigations concern the use of banks products or services show a higher risk of ML for the sector. There is a robust, risk-based approach to supervision of the banking sector, but other FIs are still subject to a more compliance-based AML/CFT supervision and, except for the casino sector, AML/CFT supervision is near absent for other DNFBP types.

The table below summarises the overall ML risk in Malawi, as a combination of threat and vulnerability for each of the sectors analysed by the NRA.

*Table 1: Malawi’s overall ML risk*

Sector	Sector Final ML Vulnerability	Priority Ranking Among Sectors
BANKING	0.60	2
INSURANCE	0.60	4
SECURITIES	0.30	
FOREIGN EXCHANGE BUREAUS	0.60	4
MONEY REMITTERS	0.70	3
MOBILE PAYMENTS	0.60	6
MICROFINANCE	0.40	12
CASINOS	0.60	8
REAL ESTATE	0.90	1
LAWYERS	0.70	7
ACCOUNTANTS	0.70	10
DEALERS IN PRECIOUS METALS AND STONES	0.70	9
NGOs/NPOs	0.40	11

Sector	Sector Final ML Vulnerability	Priority Ranking Among Sectors
LEGAL PERSONS AND ARRANGEMENTS	0.60	13

**Analysis of the ML Threat**

The analysis of the ML threat based on the cases identified showed that the overall ML threat is medium-high, and an increase in proceeds-generating predicate offences if compared to the data analysed for the previous NRA. The most proceeds-generating predicate offences are corruption, fraud, tax crimes, smuggling, wildlife offences, and illegal externalisation of foreign exchange and these were followed by illegal logging, drug trafficking and human trafficking.

Corruption-related proceeds are posing a high ML threat to Malawi, although the number of identified and investigated ML cases may not give an accurate and full-scale picture of the threat. The total number of cases investigated on money laundering from 2013 to 2017 was 104 while the number of cases prosecuted in the same period is 78, number of money laundering convictions was 16 and number of people convicted on money laundering was 16. The total amount of proceeds identified from 2013 to 2017 was US\$17,010,112.72, proceeds frozen US\$384,501 while proceeds confiscated was US\$2,723,992. There were considerable serious cases of abuse of public funds reported in the period between the last National Risk Assessment in 2012/2013 and this NRA. There was huge plunder of public funds through the bogus contracts involving private businesses and civil servants popularly referred to as *cash-gate*.

Illegal externalisation of forex, fraud, wildlife and tax crimes proceeds also constitute a high ML threat to Malawi. There are a considerable number of cases investigated and convictions (particularly for wildlife and tax crimes), however criminal repression of illegal externalisation of foreign currency and other unlicensed financial activities is not commensurate to the threat posed by the magnitude of the illegal market. In general, although the number of ML investigations and prosecutions has increased, the ML associated to these specific crimes appears not to be identified or pursued, given the near absence of ML investigations, prosecutions and convictions for ML associated to these predicate offences.

The analysis of the external ML threat<sup>1</sup> shows as a predominant feature the externalisation of proceeds of crimes committed in Malawi rather than the case of proceeds generated from crimes

---

<sup>1</sup> External threat means predicate offences committed outside Malawi that have generated proceeds laundered in or through Malawi, or proceeds generated by crimes committed in Malawi, which are transferred to be laundered in foreign countries.

committed in foreign jurisdictions which are transferred to and laundered in Malawi. There were no cases reviewed which showed predicate offences being committed in a foreign jurisdiction and the proceeds laundered in Malawi, indicating that the ML threat from abroad is low. Some cases showed a pattern in which the predicate offence is committed in Malawi and the proceeds are initially laundered in Malawi, and the proceeds are later transferred to other jurisdictions. The main feature observed is the transfer abroad of proceeds generated by crimes committed in Malawi (particularly tax crimes), through illegal externalisation of funds and trade-based ML. The main countries where the funds are transferred are China, Hong Kong, UAE, Pakistan, and BVI. As regards, wildlife crime there are cases in which the predicate crime is committed in Malawi and the initial stage of laundering is done in Malawi and later the proceeds are transferred to foreign jurisdictions, predominantly China. For drug trafficking, the major destination countries of the drugs are South Africa and Zimbabwe. In case of human trafficking, the major destination is South Africa; however, there are some cases involving the Middle East as the final destination of the proceeds.

The analysis of the threat at sectoral level and the analysis of the most common ML methods show that the banking sector and some illegal financial activities (such as 'black market' foreign exchange, informal money value transfer systems and illegal money lenders), and the real estate sector pose the highest ML threat. Investigations of predicate offences that have yielded proceeds, particularly the cash gate cases showed that the perpetrators were using banks and then invest in or acquire real estate, both for their own benefit and/or for the generation of legitimate income. Of the DNFBPs in addition to the real estate agents, lawyers and dealers in precious metals and stones pose the higher ML threat.

The threat analysis concerning the financial sector presents different degree of ML threat, with securities posing the lowest ML threat and other financial institutions operating illegally such as money lenders, money for value transfers and forex exchange the highest, with banks posing a medium-high risk to ML. The banking sector accounts for the highest number of STRs; but this is also due to the higher level of compliance with the AML/CFT requirements and the longer-standing implementation of such requirements by banks.

### **Analysis of the Terrorism/TF Threat and TF Vulnerability**

The NRA indicates that the overall threat of terrorist financing is low, and that the TF threat is primarily external. There have been no incidents of terrorism in Malawi, but there have been instances in which Malawi was used as a transit from neighbouring countries to travel to conflict zones such as Syria. Malawi is also used as a transit point for migrants from northern Africa to South Africa where incidents of terrorism/TF have been reported. There have been several cases of

suspected terrorists arrested in nearby countries of Malawian nationality, but investigations established that Malawian passports were obtained fraudulently.

There are no cases which have been identified showing that funds have been generated in Malawi or outside Malawi for terrorist operations in Malawi. However, there are unconfirmed suspicions/assumptions of undetected funds generated outside Malawi like Egypt, the middle east, Dubai which may be used for radicalisation through donations (like scholarships) and basic necessities (like food relief items, clothes) and start-up capital for small scale businesses for vulnerable groups and the youth. This might indicate that, in addition of transit country-related risk, there could also be an external threat aimed at fuelling radicalisation. Malawi shares boundaries with Tanzania where there have been reported incidents of terrorism.

A specific assessment was undertaken to determine whether the NPO sector and, in particular, specific NPO types could be exposed to the risk of TF (in addition to the ML risk). While the assessment did not reveal any vulnerability specifically associated to particular types of NPO, the sector as a whole present some TF risk, due to the fact that a relatively high number of NPOs are unregistered and unregulated, to the lack of transparency and accountability on how such NPOs operate and on how they acquire their funds and to poor implementation of the registration requirement and oversight.

The overall vulnerability to terrorist financing is Medium Low: while there are significant strengths in the antiterrorism framework, there are also some inherent, significant vulnerabilities. Vast and porous borders facilitate and enable movement of people, cash and goods across the borders without detection; the informal financial sector like *hawala* and black market forex can facilitate and attract TF with minimal detection. Malawi relies greatly on imports, and it cannot be ruled out that importation funds may be mingled with funds for TF through over invoicing, or forging import documents. The importation funds are mostly from foreign traders residing in Malawi some of which are from risky geographic regions. The poverty levels and desperation can lead to people falling for 'donations' which may be aimed at radicalisation and recruitment into terrorist groups. The quality of intelligence generated for this specific crime is still at formative stage.

### National Vulnerability

Malawi's vulnerability to ML is 0.63 (Medium High). Malawi has a solid legal framework, a long-standing Financial Intelligence Unit and, lately, a fair record on financial investigations, and several convictions on ML cases, particularly in regard to the *cash-gate* scandal. AML supervision of the banking sector is robust and ML/TF risk-driven. Despite these strengths there remain some significant risk factors that affect the country's vulnerability, such as the cash economy, porous borders and a system of national identification that is relatively new. Other major vulnerabilities



identified by NRA include the absence of an AML policy; partial implementation of an action plan of the previous NRA; widespread corruption and the risk of interference in the criminal investigations, inadequate resources (both technical and financial) of FIA and law enforcement agencies.

There is a good level of domestic coordination, although not in the framework of a specific AML/CFT risk-based policy, but there is room for improvement, particularly for the cooperation among LEAs and between the FIA and the RBM. There are several MOUs in place between the most important AML/CFT stakeholders. The MOUs have the purpose of enhancing information sharing among the parties. LEAs and the FIA meet regularly on a number of issues. On major cases that have a common interest, the LEAs form ad hoc taskforces to share information. FIA interacts also with financial and DNFBP supervisors. A comprehensive, risk based, AML/CFT policy, which is currently lacking, would significantly enhance AML/CFT efforts and be conducive to a more effective system, particularly by allowing allocation of resources where the risks are higher.

Apart from few technical deficiencies, Malawi's AML/CFT legal framework is solid, but its implementation is not yet fully effective and commensurate to the ML risks identified by the NRA. ML and TF are criminalised in line with the relevant UN conventions, and preventive measures such as requirements for accountable persons to undertake customer due diligence (CDD) and reporting of suspicious transactions are in place, in line with the FATF standard. The country has comprehensive laws to seize, freeze and forfeit proceeds and instrumentalities of crime. However, effective implementation remains critical. The number of STRs (particularly from DNFBPs) and amounts of assets frozen and confiscated are low and not commensurate to the ML risks identified by the NRA.

The FIA is created under the FCA, which empowers it to carry out several functions aimed at controlling and preventing ML/TF activities, largely in line with the international standards. However, resource constraints, access to information and low quality of STRs hinder effective implementation of FIU's core functions. One of the challenges faced by the FIA has been on the quality of STRs submitted by the reporting entities. As much as the FIA saw an increase in the STR numbers, most of the STRs were of poor quality and as such they were relegated to Low Priority using the prioritisation Tool. Another challenge is on the FIA's access of additional information from other agencies to be part of the analysis of cases.

Financial investigators and prosecutors have been using financial intelligence more proactively, particularly in relation to the Cash gate cases, and ML convictions were secured. However, the number of ML investigations, prosecutions and convictions remains low if compared to the overall ML threat. The investigative authorities in Malawi use financial intelligence in their work. There are a number of sources of financial intelligence at the disposal of financial investigators, including intelligence that received or obtained from the FIA which is a result of STR analysis or requests for

information. The Police, ACB, Malawi Revenue Authority and Reserve Bank of Malawi have effectively used financial intelligence to successfully investigate and prosecute several cases in 2016 on tax evasion and illegal externalisation of foreign currency and money laundering.

Seizure and confiscation of ill-gotten funds is not commensurate to the criminal environment and the ML threat. The analysis of the ML threat shows a high occurrence in Malawi of proceed-generating crimes, such as corruption, fraud, and tax crimes, among others. However, the approach to seizure and confiscation is not yet pursued systematically as a policy objective, but it appears to be driven primarily by the choices of the individual agencies. There have been a number of confiscations, particularly with reference to the *cash-gate* cases, but seizure and confiscation of proceeds of crime is not in line with the country's risk profile. The lack of a proper implementation of asset management of confiscated assets and the recourse to restitution hamper the effectiveness of the confiscation systems (and, in general, hinder the effectiveness of the AML system, which provides for strong confiscation measures).

Legal entities that can be created in Malawi do not present specific inherent factors that make them more vulnerable to ML; however, for those companies that were created under the previous legal regime, there may be insufficient data concerning ownership held by the Registrar. Settlement trusts and private trusts present a higher risk of ML than companies. While companies were used during the *cash-gate* to launder proceeds, they were not used because of the loopholes in the legal framework or for inherent risk factors related to their types, but simply because the registered businesses or companies were the ones that resources from government could easily be syphoned out through without easy detection. Companies created under the repealed 1984 Act may present more vulnerability because of less information being required to be stored or verified by the Registrar General (compared to the new regime).

### Sectorial ML Vulnerabilities: Financial Sector

**The ML vulnerability of the banking sector is 0.62 (Medium High).** The banking sector is the most significant sector with a total asset value of MK1.3 trillion as of April 2017, which is the highest among the financial sectors in Malawi and this is a significant jump for the sector which had an asset value of K531-billion in 2013. Furthermore, the significance of the sector comes in when it is considered that it is vulnerable to both money laundering and terrorist financing owing to the factors that transactions in the sector are huge, swift and attract all kinds of customers carrying various money laundering and terrorist financing risk levels, and that it has ever been used to facilitate money laundering instances.

Although the banking sector's rating has gone down as compared to the 2013 rating of 0.71, there still exist key areas requiring improvements. On the assessment of the general input variables the banking sector scored relatively well, featuring several strong factors, such as a comprehensive legal

framework including strong entry controls, a prudential and ML risk-based supervision. There are, however, some areas of improvement, in the detection of suspicious transactions and in the effectiveness of the compliance functions and availability and enforcement of administrative and criminal sanctions. The majority of the *cash-gate* cases that have been prosecuted involve banks. The Baker Tilly Report on the 2013 *cash-gate* indicated that a total of 104 '*cash-gate*' cheques were paid into at least ten different commercial banks throughout Malawi with 22 cheques linked to 10 different businesses being banked at one bank.

The banking sector products/services vulnerability has an average inherent vulnerability of 0.56 (Medium High) and average final vulnerability of 0.46 (Medium). The most vulnerable top 5 products/services are Trade Finance, Deposit Product SME, Funds Transfer (International), Private Banking, and Deposit Product Retail with inherent vulnerabilities ranging from Medium High to Medium.

**The ML vulnerability of the insurance sector is at 0.62 (Medium High).** The insurance sector is categorised into two sub-sectors, namely: life insurance and general insurance. As at 31<sup>st</sup> December 2017, the insurance sector comprised 13 insurance companies (with 8, dealing in general insurance business and 5 dealing in life insurance business); one (1) re-insurance company; 16 insurance brokers (one of which is a re-insurance broker); 33 insurance agents; 5 agents for brokers and 15 Loss adjusters/ assessors. The total assets in the industry as at 31<sup>st</sup> December 2016 were MK371.0 billion, of which 89 percent (MK332.7 billion) belonged to the Life insurance sector. Gross total premium for both sub-sectors stood at MK55.0 billion, of which 64 percent belonged to the general insurance sector. The insurance sector analysed 5 products out of which endowment is rated Medium High (0.7) because the product is mostly accessed by high-net worth customers including PEPs, and allows for non-face-to-face transactions.

**The overall vulnerability for securities sector is rated at 0.33 (Medium Low).** The securities sector has 23 players: stock exchange (1), portfolio managers (5), investment advisors (7), stock brokers (3), collective investment schemes (2) and transfer secretaries (5). The stock market had a market capitalisation of K956.7 billion with 698.9 million shares traded in 2017 at a turnover of K13.5 billion. Total funds under management by portfolio managers amounted to K827.3 billion<sup>2</sup> while stock brokers had K1, 458.5 million and collective investment schemes were at K7, 263.1 million as at December 2017. Transactions in the securities sector are done through cheques and bank transfers and are in the local currency, the Malawi Kwacha.

Portfolio management was considered riskier than stock brokerage. Portfolio management is more vulnerable mainly because of its size (K827.3 billion in value of funds under management) in comparison to the stock brokerage at K1.5 billion. In addition, the client profile for the portfolio

---

<sup>2</sup> Life insurance funds account for 55% of the funds while pension funds account for 23% of the funds

management include some high net worth individuals and PEPs who raise the vulnerability of the sub sector. In contrast, stock brokerage has a low ML/TF risk mostly because of its low asset size, low risk client base, no deposit features and the lack of cash transactions or activity. There is also low frequency of international transactions.

**Other Financial Institutions (OFIs)** in Malawi comprise of both regulated and illegally operating institutions, with mobile phone payments being the largest sector in size. The Regulated institutions include mobile money products, forex bureaus, money remitters and Microfinance Deposit-taking Institutions (MDIs, which include financial cooperatives-SACCOs) and all of which are under the supervisory purview of the Reserve Bank of Malawi. Currently, the number of mobile money subscribers reached 4.5 million out of which only 1.4 million subscribers were active as at 31<sup>st</sup> October 2017. The agent network that support the delivery of mobile money services in Malawi was at 30,568 in October 2017 with only 19,625 being active over a 90-day period. The volume of mobile money transactions averages 11.9 million per month whereas the corresponding value of transactions averages K50.3 billion per month in the year 2017. This trend shows great improvement compared to the 2013 assessment period when mobile money services had just been launched in Malawi.

The Malawi microfinance and financial cooperatives industry is still in its nascent stage providing limited financial services to low income and underserved customers excluded from the formal financial system. As at December 2017, the microfinance sector comprises thirty-five (35) registered microcredit agencies, nine (9) licensed non-deposit taking microfinance institutions, one (1) licensed deposit taking microfinance institution whereas the financial cooperatives (SACCOs) sector comprises thirty-four (34) licensed SACCOs. The microfinance sector in Malawi is highly cash intensive as both loan disbursements and loan repayments are usually done in cash. The asset size for the microfinance sector stood at K35.5 billion in September 2017 while the financial cooperatives reported total assets amounting to K11.8 billion. The volume as measured by gross loans stood at K21.3 billion and K7.7 billion for microfinance and financial cooperatives sectors respectively. As at 30 October 2017, the Reserve Bank of Malawi had licensed 15 foreign exchange bureaus with 45 branches across the country. Of the 15, three bureaux are subsidiaries of Commercial banks while the rest are stand-alone operators. In March 2015, the bank issued a new regulation which allows foreign exchange bureaux to operate through agents (however, only one bureau has a branch and 4 agents). As at 31 December 2016, total foreign exchange sales were at \$94,884,703.00 while total purchases totalled \$78,884,703.00. The total assets of 6 out of the 15 bureaux that responded to the RBM request for audited financial statements and the total asset value as at 31 December 2015 was MK901,510,543.00 (US\$1,226,544.96).

The most vulnerable OFI sectors are money remittances, foreign exchange bureaus and mobile payments vulnerability ranging from 0.6 to 0.7.

The main threat to the sector and an opportunity for criminals to launder money (and, possibly for TF), is the existence of a thriving market of illegal foreign exchange, illegal money lenders and loan sharks (*“katapila”* which can charge between 50% to 100% interest rates or even more depending on the level of desperation shown by the borrower). Further to this, the existence of an informal money value transfer systems (*hawala*) also poses a great threat. The asset size of this market is not known. However, there has been movement of huge sums of money outside the formal financial system through this system and it is a potential breeding ground for ML/TF as source of the funds cannot be established. Repression of these illegal activities is very poor, which increases the vulnerability of the sector.

### Designated Non-Financial Businesses and Professions

The Financial Crimes Act recognises casinos, real estate agents, dealers in precious metals and stones, lawyers and accountants as Designated Non-Financial Businesses and Professions (DNFBPs). All these DNFBPs are subject to the AML/CFT requirements. Due to their interface with the financial sector, these professions and businesses run the risk of being exploited by criminals and money launderers who resort to the non-financial sector to conceal their criminal revenues.

There are several weaknesses that are common to all DNFBPs, and contribute to increase the ML risk for the sector, but specific vulnerabilities inherent to the real estate, lawyers and DPMS expose these particular sectors to a higher risk of ML.

**The level of money laundering risk of the DNFBP sector is assessed at 0.71 (Medium High)**, largely due to the absence of an effective AML supervision and oversight and poor entry controls (except for casinos), near-absence of implementation of AML/CFT requirements by DNFBPs, and the widespread use of cash noted in the assessment of the National Vulnerability. In addition to these issues that are largely common to all DNFBPs, the assessment has found that the real estate sector has the highest vulnerability rating, followed by lawyers and DMPS; then accountants and lastly Casinos. In terms of inherent vulnerability, the real estate sector again tops the list, followed by DPMS, then lawyers, accountants and again casinos.

The vulnerability of casinos is 0.6 (Medium High). Casinos are subject to a rather basic, compliance-based AML supervision by the Gaming Board, but all other DNFBP types have not been subject to AML/CFT supervision. This constitutes a serious vulnerability, particularly for those types of DNFBPs that have been identified as posing a higher ML risk (e.g. real estate agents or lawyers).

The Real Estate industry is comprised of both regulated and non-regulated groups, property valuers, and auctioneers. The non- regulated real estate agents pose a high vulnerability to ML. The vulnerability of real estate is at 0.89 (High). It is alleged that some proceeds from the *cash-gate* were invested in the real estate.

The vulnerability of lawyers is at 0.73 (Medium High). There is close to nothing on effectiveness of supervision/oversight, STR submission, and AML/CFT knowledge.

The vulnerability of DPMS is at 0.72 (Medium High). There is close to nothing on effectiveness of supervision/oversight, STR submission, and AML/CFT knowledge.

The size of the business is medium as there are 250 officially registered miners with the Department of Mines but over 40,000 Malawians are engaged in mining activities whether registered or not. This increases the vulnerability of the sector to the ML/TF threat. The law however is clear that no-one should engage in mining without a license. Moreover, there exist DPMS at retail level who are not subject to registration requirements, except for having a business licence. The Client base profile of the business/profession is high risk as Domestic/international peps, high net-worth individuals, non-resident clients from various jurisdictions, clients with foreign business or personal interests, clients with business links to known high-risk jurisdictions, are in one way or the other engaged in the sector as buyers or agents whether legally or illegally hence the high-risk rating. There is a medium level of cash activity associated with the business/profession because many small-scale and artisanal miners prefer cash transactions to subsist on. Tracing the transactions is difficult and time consuming considering that there are unregistered players in the sector and Malawi is a cash economy.

### Financial Inclusion

There are 8 products under financial inclusion, namely; Basic Savings, Basic Banking Credit, Ordinary Farmer Account, Mobile Banking, Mobile Money, Local Money Remittances, Member-based Savings, and Micro-credit. The product poses low vulnerability except for Member-based Savings which has Medium Low vulnerability because of it has no thresholds.

## DETAILED PRESENTATION OF THE ASSESSMENT

---

### Money Laundering Threat

#### Introduction

The group analysed the ML threat in Malawi, by identifying and compiling data on the criminal offences that generate proceeds of crime which can be laundered. The group also considered the level of ML external threat from neighbouring countries and beyond.

#### Objectives

The objectives of the ML threat assessment were:

- To determine the level and composition of proceeds of crime generated in Malawi or from outside Malawi;
- Understand the extent and types of prevailing crimes that pose Money laundering threat;
- Determine the level of the country's attractiveness to money laundering; and
- Understand the environment in which the predicate crimes are committed, and proceeds of crime are generated.

#### Overall Assessment of ML Risk

Owing to the increase of the predicate offences there are indicators that the overall ML risk for Malawi is increasing. This is informed by the overall threat which is rated Medium and the overall vulnerability which is rated *Medium High*. The findings and details that underlie this assessment are as outlined below:

#### Overall ML Threat

##### *Domestic ML Threat Analysis*

A clear determination and understanding of the ML threat are important in the process of assessing the ML threat. The ML threat analysis considered the level and trend of predicate offences reported and the amount of proceeds identified in the cases that were investigated. The assessment also considered the unrecorded/unreported predicate offences and the unidentified proceeds of the predicate offences. The assessment took notice that there are many predicate offences recognised for having the potential to lead to intent to launder funds. However, through the expert judgment, the available sources of information, existing legislation and criminal behaviour the assessment came up with predicate offences which are more relevant in the context of Malawi.

The ML threat assessment identified predicate offences that generate a significant amount of proceeds in Malawi and these are Corruption, Illegal externalisation of foreign currency, Tax evasion, Smuggling, Wildlife crime, Fraud, Drug trafficking and Fraud. Over the past five years there have been several methodologies used to launder funds in Malawi the most prevalent have been Cash Based Money laundering (use of cash intensive businesses to disguise criminal proceeds) and Trade Based Money laundering (use of import and export system to disguise and transfer proceeds through the movement of goods and funds).

The table below shows the predicate offences and the corresponding amount of proceeds generated in cases investigated from 2013 up to 2017. The amounts of proceeds generated include an estimate of the proceeds from undetected or unrecorded occurrences of the predicate offences and the proceeds generated. The estimate of the 'undetected or unrecorded' was arrived at by expert opinion by estimating that it is ten percent of the proceeds generated.

*Table 2: Estimate of proceeds from criminal offences*

ITEM	TYPE OF OFFENCE	PROCEEDS (in USD)
1	Illegal Possession of specimens of protected species and dealing in Government trophies - ivory, rhinos, turtles, pangolins, lions and leopards)	45,959,716.00
2	Disturbing indigenous trees of protected species (Illegal logging)	30,479,300.50
3	Tax evasion	20,959,469.30
4	Illegal externalisation of forex	27,666,819.36
5	Corruption	18,711,123.99
6	Smuggling	1,526,306.10

The assessment also showed that there is increase in these predicate offences if compared to the data analysed for the previous NRA. The overall ML threat is therefore considered to be medium high.



There was limited information on values of proceeds linked with offences because LEAs have challenges in generating and maintain records of these. Therefore, the assessment under this section needs to be re ad with this fact in mind. However, it has to be noted that “drug trafficking” refers to cases of actual trafficking and not to other drug-related offences (e.g. possession for personal use or consumption), which typically do not involve significant amounts of proceeds. Below is a detailed analysis of the ML threat stemming from important predicate crimes:

### **Corruption**

Corruption in Malawi is criminalised in the Corrupt Practices Act. The Act does not define corruption but rather Corrupt Practice. A corrupt practice is, “*the offering, giving, receiving, obtaining or soliciting of any advantage to influence the action of any public officer or any official or any other person in the discharge of the duties of that public officer, official or other person*”<sup>3</sup>. The strategy however defines corruption as “*the abuse of power for private gain*”<sup>4</sup>. However, the meaning of corruption in Malawi is not different from the one given in the literature by Rose-Ackerman (2004), Transparency International (2000) and the World Bank (1997). The emphasis is on the misuse of public office for private or political gain.

The Anti-Corruption Bureau (ACB) is the agency mandated under the Corrupt Practices Act (CPA) to investigate and prosecute corruption cases in Malawi. The CPA also gives the ACB additional powers to investigate any other offence discovered during the course of its investigations, including ML. The total number of cases investigated on corruption-related ML from 2013 to 2017 was 104 while the number of cases prosecuted in the same period is 78, number of ML convictions was 16. The total amount of proceeds generated in 2013/2017 was US\$18, 711, 123.99, proceeds frozen US\$384,501 while proceeds confiscated was US\$2,723,992.

The ML threat is High considering that all the cases involve significant amounts of public funds.

There were considerable serious corruption cases reported in the period between the last National Risk Assessment in 2012/2013 and the review in 2017 particularly the plunder of public funds through the bogus contracts involving private businesses and civil servants popularly referred to as *cash-gate*. Almost all the statistics referred to above involve the cash gate cases. The plunder of public funds through abuse of the Pensions and Gratuities fund by some civil servants was also

---

<sup>3</sup> The Corrupt Practice Act, 1995, pp 4

<sup>4</sup> Malawi Government: *National Anti-Corruption Strategy (2008) pp 12.*

uncovered. The cases are yet to be prosecuted. The statistics provided mainly refers to the some of the 2013 cash gate cases which have been concluded in court.

a. **Some Significant Corruption Cases in Malawi from 2013 to 2017**

Table 3: Estimate of proceeds laundered

Case	Brief description	Estimated amount of proceeds laundered in MK	Case status
<b>Case 1</b>	Corruption in relation to looting of Malawi Government funds in 2013 ( <i>cash-gate</i> ) through two registered businesses	4.3 Billion	The suspect was convicted on his plea of guilty. Sentenced to 11 years' imprisonment. The case is under restitution.
<b>Case 2</b>	Corruption in relation to looting of Malawi Government funds in 2013 ( <i>cash-gate</i> ) through 17 registered businesses	3.7 Billion	The suspect was convicted on his plea of guilty and was sentenced to 7 years' imprisonment. The case is under restitution.  Six buses were handed back to Malawi Government.
<b>Case 3</b>	Corruption in relation to looting of Malawi Government funds in 2013 ( <i>cash-gate</i> ) through her registered business	63 Million	The suspect was convicted on her plea of guilty and was sentenced to 3 years and 9 months.

			The convict gave back to government one house in restitution
<b>Case 4</b>	Corruption in relation to looting of Malawi Government funds in 2013 ( <i>cash-gate</i> ) through her registered business	12.9 Million	Suspect convicted on her plea of guilty and sentenced to 39 months' imprisonment.  Gave back MK15 Million in restitution to Malawi Government.
<b>Case 5</b>	Corruption in relation to looting of Malawi Government funds in 2013 ( <i>cash-gate</i> )	2.4 Billion	The case is still under prosecution.
<b>Case 6</b>	Corruption in relation to looting of Malawi Government funds through payment to a business which did not provide services to the Army.	1.9 Billion	The case is still under prosecution.

***Illegal Externalisation and Abuse of Foreign Currency***

Illegal externalisation of foreign currency involved cases of externalisation of foreign currency using fake or falsified MRA importation documents, invoices and travel documents. There were 154 cases investigated and only 4 were prosecuted, resulting in the conviction of one individual. Most cases were unearthed through joint investigations by RBM and FIA and showed significant amount of funds being illegally externalised by some foreign business persons. The common destination of the funds is China, Dubai and Hong Kong.

In one joint investigation in 2015, about US\$16.9-million was established to have been illegally externalised by 22 foreign owned businesses through two financial institutions. The funds were externalised disguised as import payments, but the import documents were fake which is violation of the Exchange Control Regulations. In 2016, investigation by the FIA and RBM established abuse of foreign currency through illegal claims for foreign travel allowance. A total of US\$4.2-million was suspected to have been abused through one financial institution in 2016 alone. In 2017, investigations also established that about US\$4.1-million was illegally externalised by 4 foreign

nationals in a period of about 7 months through two financial institutions. In summary about US\$25.2-million was illegally externalised. This was done mainly through fake importation documents. ML threat is *High*.

In its September 2016 report '*Illegal Externalisation of Forex: Status, Challenges and Solutions*', the Malawi Revenue Authority's Tax Investigations Division outlined the following observations and challenges:

#### **OBSERVATIONS**

- Culprits involved in the illegal externalisation of forex operate well-coordinated and sufficiently resourced syndicates.
- The culprits use counterfeit invoices with inflated values to match the money being repatriated to their so-called foreign suppliers.
- The importers use falsified bill of entries to reflect the higher amounts being requested to finance the dubious importations.
- Some of the importers feign importation of high-priced machinery and advise their commercial banks to effect payment for the same.
- Other culprits present to Customs, documents of a bulky importation and negotiate a preclearance arrangement. However, after importing a few lots, they advise the banks to make full payment for the consignment after which the so-called bulky importation is abandoned.
- There are high chances that the syndicate of illegal externalisation of forex benefits from the assistance rendered to them by officers at the commercial banks and clearing agents who effect remittance even when the documents are conspicuously suspicious and provide fake MRA date stamps respectively.

#### **CHALLENGES:**

- The offenders, in anticipation of being discovered at some point, declare fictitious details of telephone numbers, physical business and residential addresses when opening their business accounts at the commercial banks. Such misleading information has always frustrated investigations in tracing the culprits.
- The offenders keep changing names of their businesses after trading for a while. For instance, during the arrest of Mr. Guo Jiansi who according to our files was trading as Wu Chun Trading, we noted that the name Wu Chun Trading was unsuccessfully erased and replaced with Zhou Min Investments at the front wall of the same shop. However, the regular changing of trading names has proved quite a challenge to locate the actual place of the culprits.
- In making the foreign currency application, the offenders provide very sketchy personal particulars of the applicant. For instance, only a signature is provided for in most instances. With such scanty information, tracing the actual culprits has been very difficult.
- Some information was sourced from third parties who provided the information later than required. And since the information sought passed through a number of offices, its confidentiality could not be guaranteed and it was highly prone to compromise. This might explain cases where suspects could no longer be reached on the same mobile phones we had contacted them earlier on prior to seeking their further information from other offices.

## **Tax Evasion**

There is no specific definition for Tax Evasion provided in the Tax laws such as the Customs and Exercise Act, VAT Act and the Income Tax Act. However, it has been defined as the act of illegally paying less taxes (or not paying at all) than the amount legally required by the tax law<sup>5</sup>.

During the 2016/17 fiscal year, MRA investigated a total of 50 cases compared to 95 cases investigated in 2014/15, representing a decrease of 47.4%. Out of the 50 cases investigated, 26 were settled administratively and 24 were referred for prosecution. In terms of revenues, all the cases had a cumulative value of MK35.6 billion which was 145.3% higher than MK14.5 billion of the 2014/15 fiscal year of which only MK422.3 million was collected (MK35.2 billion is still held up in courts). Compared to year on year performance, the collection for 2016/17 year was 53.7% lower than what was collected in 2014/15 fiscal year.

However, there are also figures on Tax evasion which relate to audited cases from domestic taxes. These include tax avoidance, which refers to reducing taxes by legal means, and tax evasion which refers to the criminal non-payment of tax liabilities.

Customs and Excise Division's Post-Clearance Audits planned in 2015/16 fiscal year were 182 of which 83 were finalised and a total of MK154.6 million was collected from a total assessment of MK242.6 million. The 2015/16 collections were below 2014/15 fiscal year by 19.3% despite that more audits were planned in 2015/16. Non-compliance issues that were commonly observed include, but not limited to: misclassification of goods, abuse of country of origin, abuse of industrial rebate scheme and under-declaration of values. To deter recurrence of such practices, MRA imposed administrative penalties on traders who failed to comply with Customs Laws and Regulations and those traders who engaged in unlawful activities, were duly prosecuted.

There are no ML cases connected to Tax Evasion reported. In terms of typologies an analysis of investigated cases on tax evasion indicate that the most prevalent cases involved under-invoicing, concealment/suppression of sales, claiming non-allowable expenses, claiming non-allowable VAT, non-remittance of withholding tax, undervaluation of imports, undervaluation of imports and misclassification of goods. However, through analysis the FIA has also established that there is a trend of some individuals and companies using personal or private bank accounts to evade tax<sup>6</sup>.

### **b. Some Significant Tax Crime Cases from 2013 to 2017**

---

<sup>5</sup> MRA Tax Investigations Division Annual Report. July 2016-June 2017.

<sup>6</sup> Money Laundering Typologies in Malawi, September 2011.

Table 4: Tax crime cases

Case Title, Court	Dispute and Amount involved	Status
<b>Case 1</b>	The accused person was arrested and charged with forgery and uttering false documents. He had submitted a fake Bill of Entry to a Bank on an application for outward transmission of about <b>\$39, 000</b> to an alleged supplier in China.	The accused person pleaded not guilty to all counts and was granted bail. All disclosures have been filed and served. Trial is yet to commence as the Magistrate handling the case was appointed Assistant Registrar and the case needs to be re-assigned to another Magistrate. The Reserve Bank intends to apply to prosecute.
Case 2	The accused person, who is the managing Director of a company, was arrested and charged with fraudulently using customs documents to externalise forex amounting to a total of US\$1, 488,000 to an alleged supplier in Hong Kong.	The accused person pleaded not guilty to all counts and was granted bail. All necessary documentation is in place – including disclosures filed - and the case is ready for trial. Similarly, as in the case above, there still remains intimation by the Reserve Bank to make an application to co-prosecute.
Case 3	The accused person, who was the proprietor of a company in Lilongwe was arrested and charged with fraudulently using customs documents to externalise a total <b>US\$650,561.36</b> to an alleged supplier in China.	Pursuant to the Consent Order of 28 September 2016, the accused pleaded guilty and was, accordingly, convicted and his sentence suspended on condition that he had to pay <b>MK44, 235, 320. 40</b> as duty and an additional <b>MK13, 270,597.13</b> as a penalty.

Case 4	The 1 <sup>st</sup> , 2 <sup>nd</sup> and 3 <sup>rd</sup> accused are proprietors of a company A and the 4 <sup>th</sup> accused was a clearing agent. Collectively, they were charged with fraudulently using customs documents to externalise a total of <b>US\$ 45,663.02</b> to an alleged supplier in China.	All the accused pleaded not guilty to the charges against them. They are currently on bail. The case is ready for trial and is awaiting a date to be issued by the court for commencement of hearing.
--------	---	---

**Fraud**

Fraud is covered under sections 332 to 336 of the Malawi Penal Code. The most common type of fraud in Malawi is swindling of public funds, defrauding of private organisations and banks,<sup>7</sup> forgery of bank cheques, identity fraud, forgery of import/export documents, vehicle registration documents, and creation of false public workers. Where fraud happens in an organisation, it is sometimes conducted with the involvement of employees within the organisations. For example, some bank officials have been prosecuted and convicted for conniving with criminals. The assessment managed to find statistics for bank fraud, theft by servant and theft by Public servant. For Bank fraud the total number of cases investigated in 2016 was 68, of which 52 cases were prosecuted resulting in 50 convictions involving 116 convicted persons. For theft by servant the total number of cases investigated in 2016 was 152, of which 122 were prosecuted resulting in 105 convictions involving 112 convicted persons. For theft by Public Servant the total number of investigated cases was 74, of which 69 were prosecuted, resulting in 52 convictions, and 83 convicted persons 83. The records do not indicate the ML proceeds identified and confiscated.

A recently identified trend on fraud involves traders, especially Pakistani and Chinese nationals, forging or falsifying customs documents to illegally externalise foreign currency. Since 2013, the MRA, RBM and FIA have been working on cases bordering on dubious foreign exchange transactions, originating from commercial banks. It is suspected that some of the money externalised, especially that linked to Pakistan nationals, may not have been generated domestically thus there is a likelihood of the existence of unsanctioned financial activities connected to money laundering, corruption, illicit financial flows and even terrorist financing. Through experience and expert judgment, it is observed that fraud cases are increasing. The ML threat is **Medium High**.

---

<sup>7</sup> Fiscal Police and Money Laundering Typologies in Malawi, September 2011

### Wildlife Crime

Wildlife crime is generally defined as all crimes committed against wildlife species and may include illegal trade in trophies or specimens of endangered species. In Malawi prime legislation on wildlife crimes is the National Parks and Wildlife (Amendment) Act 2017. It is supported by other legislation such as the Penal Code, the Firearms Act, the Customs and Excise Act, the Financial Crimes Act and the Environmental Management Act. In the last five years there has been an increase in wildlife crime in Malawi, mainly due to the lucrative illegal market for wildlife products in South East Asia and China. The criminal syndicates in these countries recruit local nationals to undertake the killing of wildlife and facilitate the trafficking of wildlife products. Currently the most common wildlife being targeted are Elephants for their tusks, rhinos for their horn and Pangolin for their scales.

There has been significant progress in combating wildlife cases from 2014. This was also enhanced further with the review of the National Parks and Wildlife Act, 2017 which significantly raised the penalties and introduced forfeiture of instrumentalities. Over the past five years the number of wildlife cases investigated are 171, of which 164 were prosecuted. The number of convictions and convicted persons is 162. The amount of potential proceeds that could have been generated is US\$41,781,560.00. ML threat is **Medium High**.

#### c. Some Significant Wildlife Cases in Malawi from 2013 to 2017

Table 5: Wildlife cases

Case	Brief description	Case status
Case 1	Exporting specimen of protected species- 39 kg of rhino horn seized in Shanghai-China	The suspects are on bail
Case 2	Exporting specimen of protected species- 330 kg of ivory seized in Thailand	The suspect was convicted on his plea of guilty and was sentenced to 7 years' imprisonment. The case is under prosecution.
Case 3	Three suspects suspected of possession of specimens of protected species and killing black rhino in Liwonde National Park and dealing in government trophies - 4 kg of rhino horn	The suspects were convicted and sentenced to 18 years, 7 years and 10 years imprisonment respectively



Case 4	2 suspects (all Malawian nationals) found in possession of 781 pieces of ivory weighing over 2.6 tonnes worth over MK4 Billion.	The suspect prosecuted and convicted of Money laundering. Fine MK5 Million or 5 years' imprisonment in default. The suspects paid the fine.
Case 5	35 suspects (Chinese, Mozambican and Malawian) found cutting down trees in Lengwe National Park and charged with illegal logging.	All the suspects were prosecuted and convicted and sentenced to 3 years' imprisonment. All the equipment used in the logging was forfeited to the State.

**Human Trafficking**

Human trafficking is the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, or fraud, or deception, or the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation<sup>8</sup>. It is difficult to quantify human trafficking cases because of lack of awareness and poor record keeping. Information from Law Enforcement indicates that people are trafficked locally from rural to urban areas and also from to foreign destinations with Malawi being used as a transit route for passage from other African countries like Ethiopia and Somalia en route to South Africa. In Malawi the prime legislation on trafficking in persons is the Trafficking in Persons Act, 2015 and the Childcare, Protection Justice Act of 2010. The total number of cases investigated from 2009 to June 2012 was 340. In 2014 alone 25 people were convicted on human trafficking offences while in 2015 58 were convicted. From 2013 to 2016 the number of cases investigated was 79, of which 63 were prosecuted, resulting in 54 convicted cases and 116 convicted persons. Looking at the information on the number of occurrences, there may be a downward trend in occurrence of human trafficking cases, however, some cases are undetected and unreported. Through the experience and expert judgement, it was observed that there is economic motivation for committing the crime of human trafficking. There are no records captured on proceeds identified and confiscated. The ML threat is Medium Low.

**Drug Trafficking**

Drug trafficking is a global illicit trade involving the cultivation, manufacture, distribution and sale of substances which are subject to drug prohibition laws<sup>9</sup>. The principal legislation governing drug trafficking offences is the Dangerous Drugs Act, Chapter 35:02 of The Laws of Malawi. In Malawi

---

<sup>8</sup> UN Protocol to Prevent, Suppress and Punish Trafficking in Persons, Article 3, paragraph (a)

<sup>9</sup> United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988

this mainly involves the trafficking of *Cannabis Sativa* locally known as *chamba*. Records from 2013 to 2016 indicate that 775 cases were reported, of which 737 were prosecuted, resulting in 520 convicted case involving 570 persons. Both Malawians and foreigners have been arrested and convicted for drug trafficking which suggest that a transnational network may be involved. Annually about 70,000 kilograms is seized. The positive effect of production of Cannabis on the overall Malawi economy is negligible. The Cannabis is mainly produced for the export market and the trend shows that there is an increase in drug trafficking cases. However, available records do not have information on the actual ML proceeds that have been identified and confiscated. The ML threat is **Medium High**.

### **Smuggling**

Smuggling means the importation or exportation, or the loading onto or unloading from conveyance, or the diversion for consumption, of any goods subject to customs control with intent either to defraud the Government of any duty payable thereon or to evade any of the provision of the Customs laws section 210. The most common type of goods smuggled into Malawi are cosmetics from South Africa, cooking oil from both South Africa and Mozambique, alcohol (Beer, ciders, brandy, whisky) from both South Africa and Mozambique, cigarettes, mainly from Mozambique because of higher rates of custom duty<sup>11</sup>. Due to the porous nature of the Malawi borders, there has recently been an increase in smuggling of high-end motor vehicles such as Toyota Fortuners from South Africa, Frozy fizzy drinks from Mozambique and Super Shake drinks from Zambia. On the other hand, the most common type of goods smuggled out of Malawi are maize and timber. Maize is smuggled out because it is a controlled produce and timber because of export tax<sup>12</sup>. The ML threat is rated **Medium High**.

### **Analysis of Foreign Threats**

While most of the financial transactions in Malawi may be legitimate, in the cases reported, suspects and offenders were mostly other nationalities who take advantage of relaxed vetting and requirements to do business in Malawi. This was most prevalent in the offences of illegal externalisation of foreign currency, tax evasion and wildlife crimes.

In some cases, like illegal externalisation of foreign currency, the source of funds externalised is not clearly defined because the pattern was that huge cash deposits were made at the financial institutions followed by a request for externalisation of funds. However, the volume of funds was

---

<sup>10</sup> Customs and Excise (Amendment) Act, 2011

<sup>11</sup> Malawi Revenue Authority

<sup>12</sup> Malawi Revenue Authority

not commensurate with the type of business of those involved in the cases. The pattern raised the suspicion that the funds may be generated elsewhere, and Malawi was used to launder the funds, however this is not conclusive since the origin cannot be identified as being Malawi or elsewhere. Therefore, the ML threat from unidentified origin is **Medium High**.

There were no cases reviewed which showed that the predicate offence was committed in a foreign jurisdiction but the proceeds were laundered in Malawi. Therefore, the ML threat from abroad is **Low**.

Some cases showed a pattern in which the predicate offence is committed in Malawi and the proceeds are initially laundered in Malawi, and later transferred to other jurisdictions. For illegal externalisation of funds, the main countries where the funds are transferred are China, Hong Kong, United Arab Emirates, Pakistan, United Kingdom, and British Virgin Island. With regard to wildlife crime cases the predicate crime is committed in Malawi and the initial stage of laundering is done in Malawi and later the proceeds are transferred to foreign jurisdictions, predominantly China. For drug trafficking the major destination countries are South Africa and Zimbabwe while for human trafficking the major destination is South Africa, with some cases involving also the Middle East as the final destination.

### Sectoral Breakdown

The ML threat analysis assessed the ML threat as it occurred in the Banking, Securities, Insurance, Remittance, Foreign Exchange Bureaus, Casinos, Real Estate Agents, Dealers in Precious Metals and Stones, Auditors and Accountants, Lawyers and Notaries Sectors. The assessment reviewed the sectors and identified how proceeds of crime were laundered and invested. The analysis identified three significant sectors namely; Banking, Remittance and Real Estate, as most vulnerable to ML.

**The banking sector** featured the highest in predicate offences, including illegal externalisation, and involvement in the *cash-gate* cases. Two hundred twenty-nine cases reviewed may have originated from lapses in transactions in the banking sector. The lapses may have also been due to the fact that Malawi is cash-based economy with about three quarters of all business transactions being conducted through cash payments. In 2013 some Malawians were found in possession of huge amounts of cash in their vehicles and houses. The cash was suspected to have been connected to the plunder of government funds known as *cash-gate*. There were also huge cash withdrawals from Bank accounts of businesses suspected to have been involved in *cash-gate*. The widespread use of cash affects the AML regime in Malawi. The ML for the Banking sector is **Medium High**

**The money remittance sector** also featured high in predicate offences, with 154 cases connected to this sector. The cases involved illegal externalisation of foreign currency with indications that

proceeds were laundered through remittances for alleged importation of goods. This was largely due to lack of interface between the commercial banks and the Malawi Revenue Authority which deprived the banks of the capacity to authenticate customs clearance documents the majority of which were used in the commission of the illegal externalisation of foreign currency. There was also suspected connivance between bank officials and some customers to illegally externalise foreign currency without support documentation. The ML threat for the remittance sector is **Medium High**.

**The real estate sector** also featured in some predicate offences. There were some cases on corruption which showed that funds were laundered through the real estate sector. In the famous *cash-gate* case in 2013 and also in other predicate offences such as theft of public funds, suspects invested the ill-gotten funds in real estate. The ML threat from the real estate sector is **High**.

### Recommendations

- a) The focus of investigations and prosecutions should also include identification, recovery and confiscation of proceeds of crime.
- b) Law enforcement agencies should improve their data capturing systems by including proceeds identified, recovered and confiscated.
- d) Authorities need to consider developing mechanisms to review some foreign currency policies and legislation to prevent any possible terrorist financing threat that could be used through this system.
- e) Authorities should consider establishing a unit responsible for asset forfeiture as this is currently not well coordinated in the country.
- f) Authorities should also consider enhancing the capacity of law enforcement agencies in financial investigations related to wildlife crimes and cooperation between the Department of National Parks and Wildlife and other LEAs.

## Terrorist Financing and Terrorism Threat Analysis

### Background

Malawi has never experienced any terrorist incidents. Furthermore, no individual or group in Malawi has ever been convicted of TF or terrorist activities. However, there was a case in which an individual who claimed to be a Malawian was arrested on 30<sup>th</sup> August 2017 in Kenya after being accused of drawing a sketch plan of standard gauge railway terminus in Mombasa for use in commission of a terrorist act<sup>13</sup>. It transpired that he was not a Malawian and that his passport was

---

<sup>13</sup> [www.standardmedia.co.ke](http://www.standardmedia.co.ke)

a forgery. There have also been other cases of suspected terrorists arrested in nearby countries and found bearing the Malawian passport. However, investigations into these cases established that the Malawian passports had been obtained fraudulently. There is also suspicion that Malawi could be used as a transit route for some foreign nationals travelling to conflict zones.

Regionally, terrorist attacks by Al Shabab took place in Kenya at Garissa University where 148 people were killed in April 2015, and Westgate Mall attacks in September 2013.

Based on the facts presented, the TF risk for Malawi is rated at Low.

### **Part A – Terrorism Threat**

The overall rating for Terrorism Threat is **Low** and this has been based on the following variables:

#### ***Domestic (Targeting Home or Foreign Jurisdictions)***

There are no known terrorist groups in Malawi targeting the country or foreign jurisdictions. All factors being equal, the situation might likely be the same in the foreseeable future. Therefore, the rating for this variable is **Low** considering that there are no reported cases on domestic terrorism.

#### ***Regional (Targeting Home Jurisdiction)***

There are no known regional terrorist groups targeting Malawi. However, some terrorist groups are known to operate in the region. For instance, there have been reports that ISIS has been using South Africa as a logistics hub and hide-out<sup>14</sup>. Furthermore, there are reported cases of terrorist attacks by Al-Shabab in Kenya in 2016 on a variety of targets including police stations, mosques and universities. It was further reported that some Tanzanians joined ranks of Al-Shabab operating in Kenya and Somalia<sup>15</sup>.

In addition to the above, it has also been reported that Kenya experienced multiple terrorist incidents by ISIS and Al-Shabab including killing of five police officers in Mandera county and high-profile attacks in Mombasa and Nairobi<sup>16</sup>. In the absence of any factors changing the situation might likely be the same in the foreseeable future.

This variable is rated therefore **Low**.

#### ***Global (Targeting Home Jurisdiction)***

ISIS and Al-Qaeda are some of the groups that operate at global level with regional presence. However, there are no known Malawian nationals linked to the international terrorist groups.

---

<sup>14</sup> 2016 Country Reports on Terrorism published by the USA, p. 58

<sup>15</sup> 2016 Country Reports on Terrorism published by the USA, pp. 59-60

<sup>16</sup> 2016 Country Reports on Terrorism published by the USA, p. 34

In the absence of any factors changing the situation might likely be the same in the foreseeable future. This variable is rated therefore **Low**.

#### ***Home Jurisdiction is Used as a Transit Point***

It is suspected that nationals from the region and beyond use Malawi as a transit point en route to other countries. The high influx of foreign nationals migrating within the region, through Malawi, and the increase in human trafficking cases, increases the country's vulnerability to TF and terrorist related activities. This variable is rated therefore Medium Low.

### **Part B – TF Threat**

The overall TF threat is rated **Low** and this is due to a number of variables as explained below:

#### ***Direction of Funds***

##### ***a) Funds Generated in Home Jurisdiction for Operations in Home Jurisdiction***

There are no known cases which have been identified showing that funds have been generated in Malawi for terrorist operations in Malawi. In addition, there are no known or identified terrorist groups in Malawi.

According to records and expert knowledge, there is no indication that there has been any case reported, investigated or prosecuted relating to terrorist financing, and as such there have been no convictions recorded either. Similarly, there have been no requests from other countries and no assistance has been provided to other countries in this regard. The country has not made any seizures and confiscations relating to this variable

Based on the factors above, the rating for this is Low. All factors being equal, the trend will remain the same.

##### ***b) Funds Generated in Home Jurisdiction for Operations in Foreign Jurisdiction***

There are no known cases which have been identified showing that funds have been generated in Malawi for operations outside Malawi. However, there is a likelihood that with the increase of trade-based money laundering funds that are laundered could be used to facilitate or raise funds for TF. Foreigners with businesses in Malawi have been known to provide false or fake importation invoices to enable them to transfer foreign currency. Through false invoicing there is likelihood that some of the beneficiaries who receive the forex sent from Malawi could be linked to terrorism or terrorism financing.

Apart from this, there are relatively high economic and financial activities and migration between Malawi and Tanzania, Malawi and South Africa, Malawi and Kenya, there might be undetected or unreported incidents of TF from or through Malawi to terrorist groups within the region.

Notwithstanding of the above expressed expert opinions, there have nevertheless, there are no investigations, convictions, seizures and confiscations related to terrorist financing, therefore the rating for this is Low. All factors being equal, the trend will likely remain the same.

***c) Funds Generated in Foreign Jurisdiction for Operations in Malawi***

There are no known cases which have been identified showing that funds have been generated outside Malawi for operations in the country. Therefore, there are no investigations, convictions, seizures and confiscations in this regard.

The rating for this is Low. All factors being equal, the trend will remain the same.

***d) Funds Generated in Foreign Jurisdiction for Operations Outside (Transit Point)***

There were 2 suspicious transactions reports from banks to FIA between 2011 and 2017, which were made because the banks suspected terrorism financing. After analysis, FIA had suspicion that these may have been funds from one country being re-routed through Malawi to other countries for unknown purposes one of which could be terrorist financing. The cases were disseminated to LEAs for investigations.

There is no confirmation that funds have been generated outside Malawi for operations outside Malawi; that is, using the country as a transit point for the funds. This variable is rated therefore Medium Low. In the absence of any change, the trend will remain the same.

***e) Origin and Destination Cannot be Identified***

There are no reported cases, investigations or prosecutions related to terrorist activity. However, there are some NPOs whose origin of funds are anonymous (*Refer to NGO vulnerability*, thus increasing the country's vulnerability to TF). The rating for this is Low, and this trend is likely to continue in the absence of any change.

***Sources of Funds***

Based on intelligence gathered by one of the intelligence agencies, some NPOs were suspected to have been beneficiaries of some funds from organisations linked to individuals on the UN sanctions list. The NPOs are in the education sector and offer secondary school education and scholarships to the youth. Preliminary inquiries into the allegations dispelled the suspicions and the connection of the NPOs to entities on the UN sanctions list. There are no cases on NPOs whose source of funds are linked to TF. The rating for this is Low. All factors being equal, the trend will likely remain the same.

## *Channels*

There are no records to backup and ascertain channels for TF in Malawi.

## *Sectoral Assessment*

### **d. Banking**

Comparatively, banks provide the medium to transfer considerable sums of funds in real time and international transfers makes them attractive to criminals. (*Refer to Banking Sector Vulnerability*). The growing trends in trade-based money laundering where traders fraudulently externalise funds disguised as import payments through the banks are indicative of the possibility and vulnerability of banks being used unscrupulously. There have been cases which have been investigated where dubious import payments have been made to jurisdictions such as Pakistan, Hong Kong and UAE. Therefore, it may be likely that TF funds may also be channelled through trade-based money laundering. However, there are no cases which have been linked to TF. The rating is therefore *Medium Low*.

### **e. Insurance**

There are no known cases in the country on TF cases in the Insurance sector. However, Life insurance products such as Endowment could be targeted by some unscrupulous individuals for TF purposes. The products are accessed by high-net worth individuals who carry a high ML risk. In addition, payment for this is done through tied agents (i.e. agents working for life insurance companies on commission basis) who do not have adequate capacity. However, there are no records of any TF cases under the insurance sector. (*Refer to Insurance Sector Vulnerability*). The rating is therefore *Low*.

### **f. Cash Couriers**

There are some cases of individuals found with huge amounts of foreign currency at airports while leaving the country for example in 2017 among others an Indian national was arrested at a port of exit with \$622, 820 cash going to Dubai, a Malawian national was arrested at the same port with \$40, 500 cash going to Tanzania and a Nigerian national was found with \$57, 000 going to Nigeria. Further to this, due to porous borders, some migrants use uncharted routes to and from Malawi. However, it has not been established if any such cases are related to TF. The rating for this is therefore *Low*.

### **g. Money Exchange Bureaus**

The black market foreign exchange is a thriving business in the major cities of Malawi. The customers of the black market traders are not subject to KYC. Further, there is low KYC or CDD



conducted by licensed foreign exchange bureaus since most of their clients are walk-in, without established business relationships. The rating for this is therefore **Low**.

**h. Money Transfer Operators (MTOs)**

This comprises inward and outward transfers and the beneficiaries are adequately identified by the MTO. Money transfers are done through banks and one mobile MTO. There are no records of any cases on TF for this product. The rating for this is therefore **Low**.

**i. Illegal Money Value Transfers**

There are illegal money value transfer operators in the country, however, it is difficult to quantify their existence and the amounts involved due to the clandestine nature of their operation. These mainly operate on trust and no records are kept of the transactions. The secrecy behind their operations therefore increase the country's vulnerability to TF. The rating for this is therefore **Medium High**.

**j. Real Estate**

The sector is mostly unregulated. Transactions for this sector are mainly settled by cash, and most dealers do not keep records. However, there are no cases relating the sector to TF. This variable is rated Low.

**k. Non-Profit Organisations (NPOs)**

NPOs are at a great risk of being used for TF because some NGOs operate without registering with appropriate regulatory bodies as such it is difficult to monitor them. Similarly, there are some NGOs whose source of funds are anonymous hence it is difficult to monitor their operations. These factors increase their vulnerability to TF. However, there are no confirmed cases of abuse of the sector for TF purposes. This variable is rated **Medium Low**. All factors being equal, the trend will remain the same.

## **Part C – Terrorism Financing Vulnerability**

**l. Quality of Legislation**

Malawi has criminalised TF in line with international standards under section 43 of the FCA, with a penalty of life imprisonment. In addition to the FCA, the Suppression of TF and Proliferation Regulations of 2017 provides mechanisms to deal with targeted financial sanctions and implementation of the UN Security Council Resolutions on TF. This variable has therefore been rated **Low** for negative impact on vulnerability.

**m. Quality of Intelligence**

The FIA is responsible for gathering and analysing TF intelligence based on suspicious transactions while NIB and MPS gather and analyse TF intelligence based on allegations. The NIB, MPS and FIA are also responsible for conducting the TF investigations. Prior to 2017, the FIA would not conduct TF investigations but would disseminate intelligence on suspected TF activity to either NIB or MPS. However, challenges emanating from lack of capacity and skills in intelligence gathering techniques and limited financial resource compromises the quality of intelligence. While the FIA may have staff with adequate knowledge and skills to gather and analyse TF intelligence, this may not be the same for the MPS.

Furthermore, the parallel and informal sector also affects the quality of intelligence since some crucial information passes outside the radar. For instance, it is not easy to get complete information on movement of goods and funds where uncharted routes or informal markets have been used.

There is some domestic cooperation between the FIA, MPS and NIB. Further to this, The Suppression of TF and Proliferation Regulations of 2017 has established the National Counter-Terrorism Panel to be chaired by the NIB. However, this Panel is yet to be operationalised. It is envisaged that the Panel will further enhance domestic cooperation.

Taking into the account the number of intelligence reports shared and disseminated, also bearing in mind the capacity and skills in intelligence gathering, the quality of TF intelligence is low.

Based on the above factors, the rating for negative impact on vulnerability is **Medium**.

#### **n. Effectiveness of TF-related Suspicious Transaction Reporting, Monitoring and Analysis**

Between 2013 and 2017, the FIA received 2 STRs on TF from the financial institutions. Most of the financial institutions use manual systems to monitor their customer transactions. As such, they may not be able to detect some transactions, especially those where customers split the transactions to avoid reporting thresholds. In addition, financial institutions, especially the small ones, rarely screen their customers against sanctions lists. Such financial institutions can therefore unknowingly accept designated individuals as their customers.

Furthermore, the FIA has limited human resource capacity to effectively analyse or monitor transactions for TF, particularly monitoring transactions occurring outside the formal financial markets. The FIA has only 4 staff dedicated to monitor and analyse the transactions.

The rating for negative impact on vulnerability is **Medium**.

#### **o. Adequacy of Resources**

The human and financial resources are inadequate to carry out operations both at the FIA and LEAs especially relating to analysis and investigation of suspicions related to TF. For instance, FIA only

has 4 staff that are involved in analysis and investigations of TF allegations. The frequent transfer of staff to various departments within MPS also affects the implementations of CFT measures as skilled staff may be transferred to other departments that not involved in TF intelligence work. This ultimately has an impact on continuity of TF cases. Most of the LEAs do not have adequate funding to procure IT systems and solutions to aid in CFT measures. The rating for negative impact on vulnerability is Medium.

**p. Effectiveness of International Cooperation**

Malawi, through its agencies such as the FIA, LEAs, Regulatory and Supervisory bodies, is a member of various international organisations, and these include Egmont to which the FIA has been a member since 2009. The Egmont group of FIUs allows its members to regularly share information either upon request or spontaneously. Malawi has also been a member of the ESAAMLG since the organisation was formed in 1999. In this forum Malawian agencies exchange information with their counterparts in other member countries. The FIA has since its inception signed 21 MOUs with other FIUs on cooperation and exchange of information. The MPS is a member of INTERPOL, an international organisation that facilitates international police cooperation. INTERPOL has been playing a crucial role on international investigations as they are available in most countries and within reach to provide assistance in any investigations which have international dimensions. The MPS, through its Anti- Organised Crime Unit, is affiliated to the African Centre for Study and Research on Terrorism which is an African Union (AU) commission forum for interaction and cooperation in counter terrorism on the African continent.

The NIB is affiliated to the Committee of Intelligence and Security Services of Africa (CISSA) under the AU Commission which provides intelligence to policy making organs of the AU and allows them to share information.

The FIA, MPS and NIB face challenges in sharing of information with other jurisdictions that are not members of or affiliated to any of the international organisations mentioned above. As such, this also has an impact on mutual legal assistance.

The rating for negative impact on vulnerability is Low.

**q. Awareness and Commitment to Fight TF**

Awareness on Terrorism and TF issues is relatively low among most stakeholders. There are no deliberate plans or actions to carry out sensitisation programmes and brainstorm on TF and terrorism.

There is political will and commitment to fight TF as shown by the recent amendment to the offence of TF where the penalty has been increased from 15 years' imprisonment to life imprisonment.

Further, Regulations for the Suppression of TF to deal with sanctions were also issued in 2017. However, the level of funding to the relevant agencies is low. The rating for negative impact on vulnerability is Medium.

**r. Geographic and Demographic Factors**

The country is within the region that has experienced incidents of terror attacks and political instabilities like DRC, Tanzania, Kenya, and South Africa.

Malawi has porous borders which make the country prone to illegal entry of individuals and illegal movement of cash. This makes the country prone to harbouring terrorists. In addition, Malawi's participation in peace keeping operations in troubled regions like DRC and Sudan might trigger and expose it to terror attacks as has happened to Uganda and Kenya who are involved in Somalia. The rating for negative impact on vulnerability is Medium.

Based on the analysis presented above, the overall rating for TF Vulnerability is **Medium Low**.

**Strengths, Weakness and Key Recommendations**

**Strengths**

- The country has legislation in place which criminalises TF.
- The country has agencies that have oversight over TF issues, NIB, Anti Organised Crime branch under the MPS, and FIA all of which have investigative powers.
- The Anti-Organised Crime Unit is affiliated to the African Centre for Study and Research on Terrorism in Algeria (African Union) which conducts specialised training sessions.
- NIB is affiliated to the Committee of Intelligence and Security Services of Africa (CISSA) and share information.
- FIA is a member of the Egmont Group of FIUs.
- The Anti-Organised Crime Unit, FIA, and NIB engage in SADC and ESAAMLG activities and workshops on combating TF and terrorism.

**Weaknesses**

- Low staffing and skills levels of officers.
- Low funding levels for the Agencies
- TF is given low priority in some government Ministries, Departments or Agencies mostly because Malawi has not experienced terror attacks.

### *Vulnerabilities and Gaps*

- Porous borders can facilitate movement of people, cash and goods across the borders without detection
- illegal money value transfer systems like *hawala* and “black market” foreign exchange dealers can facilitate and attract TF with minimal detection.
- Malawi relies greatly on imports and this means sending a lot of funds outside Malawi to pay for goods and services to various countries. Funds for the imports may be mingled with funds intended for TF through over-invoicing and forging import documents.
- The poverty levels and desperation among some people may make them fall prey to ‘donations’ which may be aimed at radicalisation and recruitment into terrorist groups.
- The country’s deliberate policies to woo investors might make it attractive to undesirable individuals which could increase vulnerability to TF. For instance, no thorough checks maybe done on business resident permits applicants due to limited resources and time bound for which the permits have to be processed and granted.
- High levels of corruption make the country susceptible to TF and Terrorism. Corruption can influence wrong actions and omissions that may affect the country.

### *Key Recommendations*

- Government should regularise the informal forex market to curb *hawala* and the black market;
- Empower officers at FIA, NIB and Police through specialised training on combating terrorism and TF, and trade-based money laundering with long-term trainings and attachments;
- Funding for counter-terrorism programmes should be increased;
- Agencies involved in analysis and issuance of BRPs should conduct enhanced due diligence on the applicants;
- The fight against corruption in all sectors of the country should be enhanced;
- Domestic agencies should enhance information sharing on TF and terrorism and help each other in referrals for information from their international counterparts;

- Capacitate officers with skills on TF intelligence and investigations.

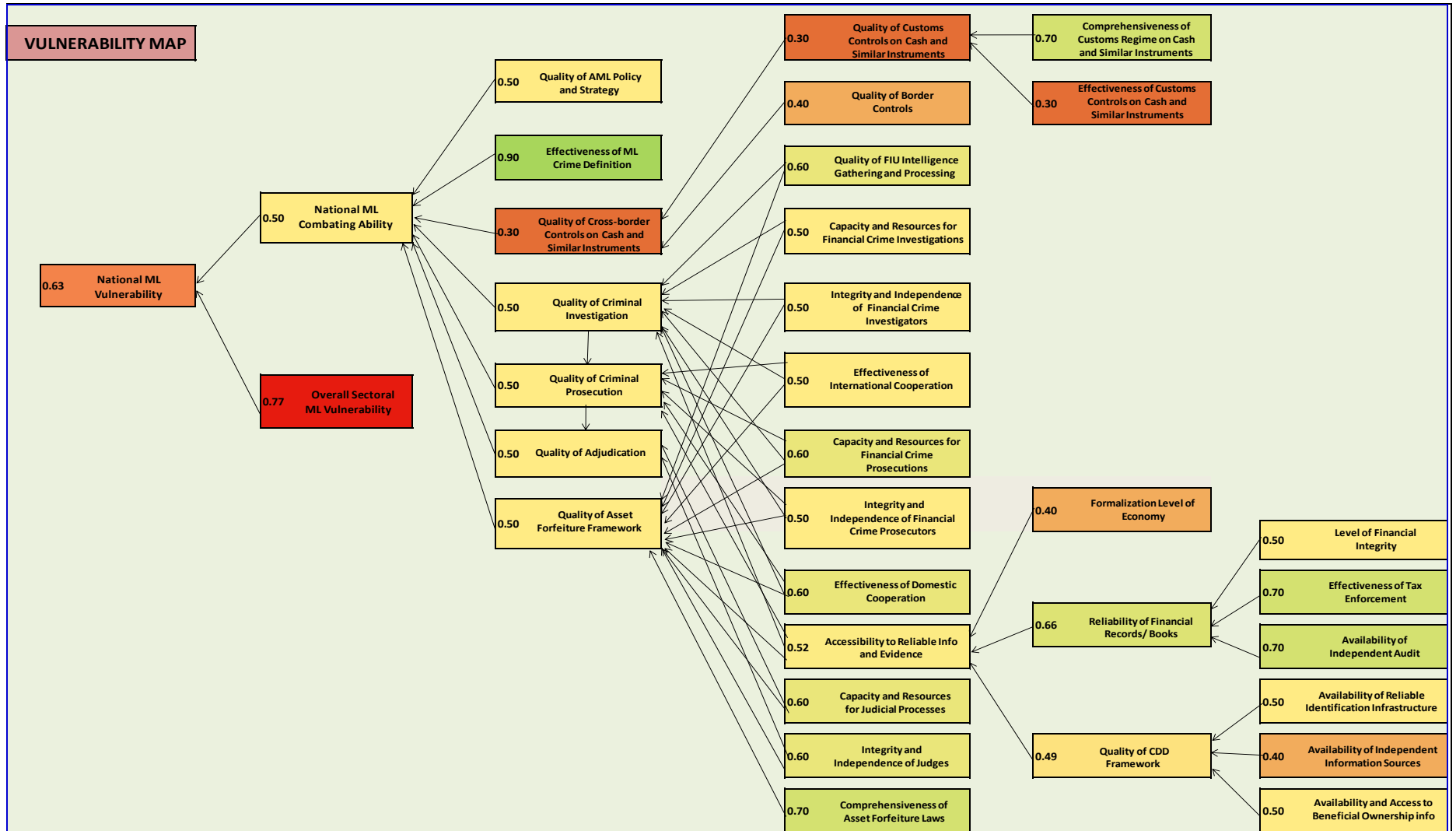
## National Vulnerability to Money Laundering

### Background

The purpose of the national vulnerability assessment was to identify Malawi's overall vulnerability to ML and to identify the weaknesses and gaps in the country's ability to combat ML. The 2013 NRA rated the country as having Medium High (0.64) vulnerability to ML. During the past 5 years, many changes have taken place, including regarding AML legislation, AML awareness and implementation of AML combating measures. Vulnerability to ML is higher where there are opportunities and is affected by the overall sector vulnerability and the country's ability to combat ML. Many factors can contribute to the vulnerability of a country to ML. Some factors have more direct impact while others have indirect impact. The importance and impact of a single factor often depends on the existence or absence of other factors.

In summary, the overall national vulnerability is rated Medium High with a score of 0.63. This is driven by two factors: the national combating ability which is rated Medium (0.50) and overall sector vulnerability which is rated Medium High (0.77).

Figure 1: Malawi's vulnerability to ML



### National Combating Ability

The national combating ability has been assessed as **Medium** with a score of 0.50, meaning that Malawi has average ML combatting ability. The NRA tool used a total of 22 input variables to assess Malawi's ability to combat money laundering. Each variable is rated on a scale of 0 to 1 and the higher the rating for the variable, the better the performance. The variables are as explained below:

### Quality of AML Policy and Strategy

Malawi has never had a stand-alone national policy on AML/CFT but had a National AML Strategy which was championed by the FIA. The National AML Strategy expired in 2015 and plans are underway to update it. Plans are also underway to develop a national policy on AML/CFT by June 2018. Despite not having a National AML/CFT Policy, structures are in place to combat money laundering and terrorist financing. The Financial Intelligence Authority (FIA), previously called the Financial Intelligence Unit (FIU), was established in 2007 as the principal national agency responsible for preventing and combating financial crimes. It was established under section 11 of the ML Act, 2006, a law which was repealed by the Financial Crimes Act in February 2017. The FIA has the mandate to coordinate the formulation and implementation of the country's AML policies and strategies with relevant stakeholders. The FIA's powers emanate from the FCA and administratively, the institution reports to the MoFEPD.

There is a National AML/CFT Committee comprising various agencies to facilitate close cooperation and information sharing required for effective AML/ CFT in the country, and also to make AML/CFT policy recommendations to the Minister of MoFEPD. The Committee was formally established in September 2017 with its terms of reference approved by the MoFEPD. Previously, there was a committee which was not formally set up and met on ad-hoc basis. The Committee is co-chaired by the Secretary to the Treasury (represented by the Director of Pension and (Financial Sector Policy in the MoFEPD) and the Director General of FIA. Its powers and responsibilities are not sanctioned by any law; therefore, its decisions are not legally binding.

There is political commitment and support to AML/CFT as evidenced by passing of the Financial Crimes Act, 2017 and the Suppression of Terrorist Financing and Proliferation Regulation, 2017 which have taken into considerations recommendations of the 2008 mutual evaluation report and recommendations of the Eastern and Southern Africa Anti Money Laundering Group (ESAAMLG).

This assessment took into account vulnerabilities of some of the largest sectors of the economy including the financial sector. Despite the previous risk assessment highlighting some shortfall in the nation's AML policies, there was no clear linkage with policy/strategy as the resulting action plan was not formally adopted. The findings of the 2013 assessment were not widely disseminated



to all relevant government departments/agencies and the private sector. This therefore puts into question whether allocation of resources in the implementation of preventive and mitigation measures is based on risk levels.

Furthermore, the repealed ML Act did not oblige financial institutions and DNFBPs to conduct their own risk assessments. As such, they could not formulate well-informed policies that addressed risks associated with their various business operations.

In view of the foregoing, this variable is rated **Medium (0.5)** as there are still a number of weaknesses in as far as AML policy/strategy and implementation is concerned.

### Effectiveness of ML Crime Definition

The FCA<sup>17</sup> criminalises money laundering and defines circumstances under which the offence is committed as:

*A person who, knowingly or who has reasonable grounds to believe that any property, including his own property, in whole or in part, directly or indirectly, represents proceeds of a predicate offence;*

- (a) converts or transfers property with the aim of concealing or disguising the illicit origin of that property, or of aiding any person, including himself involved in the commission of the offence to evade the legal consequences thereof;*
- (b) conceals or disguises the true nature, origin, location, disposition, movement or ownership of the property;*
- (c) acquires, possesses or uses that property; or*
- (d) participates in, associates with or conspires to commit, attempts to commit and aids, abets and facilitates the commission of any act or omission referred to in paragraphs (a) (b) (c)*

The definition provided in the repealed ML Act and that in the FCA are in line with the Vienna and Palermo Conventions. There have been several judgements from the courts which have showed that it is and was possible to enforce and obtain convictions based on both laws. The FCA has been applied and there have been resultant convictions just on the offence of Money Laundering alone.

The crime of money laundering is applicable to all the serious offenses, with a view to including the widest range of predicate offenses, including tax crimes.

The cases which have been before the courts in the *cash-gate* scenario have demonstrated that a defendant can be charged with money laundering alone as a standalone offence and a conviction

---

<sup>17</sup> Financial Crimes Act, section 42

can be obtained solely on that charge.<sup>18</sup> The definition further includes self-laundering as ML can be done by the individual on their own for their sole benefit.

Further, the FCA has stiffer penalties in comparison with other Acts, such as the Penal Code. The maximum penalty for ML is life imprisonment. Criminal penalties for ML offenses are proportionate and this can be seen from the fact that they have been pegged higher than penalties for other serious financial crimes such as fraud which has a maximum sentence of seven (7) years and corruption with a maximum sentence of twelve (12) years as provided in other Acts. Further to that, the penalties are also applicable to appropriate offenses which are linked to ML. For example, section 48 of the FCA refers to and adopts the provisions of section 149 of the Criminal Procedure and Evidence Code.

The offences of ML under the FCA can be committed by both natural and legal persons. As such, penalties are applicable to both natural and legal persons with varying penalties depending on the offending party. For example, Section 42 (3) of the FCA provides that:

*A person who commits an offence under this section shall, on conviction, be liable -*

*(a) in the case of a natural person, to imprisonment for life.*

*(b) in the case of a legal person, a fine of K500,000,000 and revocation of a business licence.*

Further to this, the FCA gives the FIA powers to impose administrative sanctions. The administrative sanctions include warnings, directions to do or refrain from doing a specific act monetary penalties and publication of non-compliant reporting institutions, among others. Under section 53, the FCA provides for confiscation of tainted property of accused persons who have died or absconded based on application of Rules of Evidence as obtaining in civil procedure. There is also provision of preservation and freezing orders<sup>19</sup> which can be used in the event that the criminal penalties are not applicable.

FCA has provided the Courts with enough measures of dealing with offenders by providing for a varying range of Orders which can be invoked both under Criminal and Civil liability. There are provisions of imprisonment, fines and forfeiture under the Criminal aspect, and there are provisions for freezing and preservation orders under the civil liability aspect.<sup>20</sup>

---

<sup>18</sup> Republic v. Victor Sithole (sentenced to 9 years); Oswald Lutepo (sentenced to 9 years).

<sup>19</sup> Freezing Orders come under Section 62 of the FCA

<sup>20</sup> Republic v. Victor Sithole (sentenced to 9 years); Oswald Lutepo (sentenced to 9 years); Republic v. Luke Kasamba (sentenced to 41/2 years); Republic v. Maxwell Namata (sentenced to 5 years); Republic v. Tressa Senzani (sentenced to 3 years); Republic v. Wyson Zinyemba Soko (sentenced to 31/2 years); Republic v. Esnart Ndovie (sentenced 3 years);

This variable is rated Close to Excellent (0.9).

### Comprehensiveness of Asset Forfeiture Laws

The forfeiture laws extend to (1) the proceeds and instrumentalities of ML and its predicate offenses, (2) profits derived from those offenses, and (3) property of corresponding value held by the criminal defendant or third parties.

The FCA is the main law that provides competent authorities with power to forfeit proceeds of ML and the associated predicate offences. The FCA has defined competent authority to mean, *“where appropriate, office of the attorney general, office of the Director of Public Prosecutions, office of the registrar general, office of the administrator general, a police officer, an immigration officer, a revenue officer, the anti-Corruption Bureau, the authority, the Reserve Bank of Malawi, the Registrar of Financial Institutions as defined in the Financial Services act, and includes any person authorised by any of them in that behalf and any other person the minister may, by notice published in the Gazette, designate.”* The definition is very wide and covers all the LEAs in the country.

Section 2 of the FCA further defines “Proceeds of crime or proceed of an offence or proceeds of predicate offence” to mean; “any property directly or indirectly derived or realized from an offence, and includes, on a proportional basis, property into which any property derived or realized directly from the offence was later successively converted, transformed or intermingled, as well as income, capital or other economic gains derived or realized from the property at any time since the commission of the offence;”

“Realizable property” has been further defined as;

- (a) property held by a defendant;
- (b) property possessed by a person to whom a defendant has directly or indirectly made a gift as defined in this Act; or
- (c) property of corresponding value;”

Overall, Forfeiture laws in Malawi provide authorities with a legal basis to identify and trace the proceeds or property.

The FCA provides for both conviction-based asset forfeiture (criminal forfeiture) and non-conviction based asset forfeiture (civil forfeiture). The criminal forfeiture is provided for in sections 48 to 53. Section 48 empowers the court to order for forfeiture and confiscation of tainted property upon

---

Republic v. Allan Magombo ( sentenced to 4 years); Republic v. Caroline Savala (sentenced to 7 years); Republic v. Godfrey Dzanjalimodzi (sentenced to 8 years); Republic v. Stanley Mtambo (sentenced to 16 months).

conviction. It further empowers the court to order compensation of victims of the financial crime in question. Section 49 on the other hand empowers the court to make any determination regarding the identification of tainted property and further allows the court to give any directions necessary or convenient for giving effect to confiscation orders made.

Civil forfeiture is provided for under Part VI of the FCA in sections 54 to 116. In civil forfeiture proceedings under section 74 of the FCA, the standard of proof to be used to prove that property is proceeds of crime is proof on a balance of probabilities.

Section 72 (1) of the FCA provides for civil forfeiture of property under a preservation order by stating that: "If a preservation order is in force, a competent authority may apply to a court for an order forfeiting to Government all or any of the property that is subject to the preservation order."

According to Section 77 (1) and (2) of the FCA a court can make a default order for forfeiture if no one challenges a preservation order and it is satisfied that the competent authority has satisfied the standard of proof.

In addition, the FCA provides for powers of search in pursuit of proceeds of crime. Section 59 of the FCA provides that; the authority can enter into the premises of a reporting institution or the premises of an employee of a reporting institution to search the premises and remove any document, material of other thing for the purpose of the Authority. The FCA further provides for the enforcement of forfeiture orders made outside Malawi under Section 127, which according to the Act, should be enforced in a manner similar to an order made in Malawi.

In addition, the FCA provides for protection of third party rights in a bid to comply with international standards in asset forfeiture and to achieve a balance with constitutional requirements. Section 75 of the FCA provides for the protection of third party interest in the property subject of the forfeiture. Section 76 of the FCA further provides for the protection of any person who purchases proceeds of crime in good faith.

Apart from the FCA, other laws also provide for asset forfeiture as follows:

#### *The Corrupt Practices Act (CPA)*

Section 23(1) of the CPA provides for issuance of a restriction notice on property subject of investigations or prosecution for a period of three months, subject to renewal. The Director General of the Anti-Corruption Bureau (ACB) exercises this power. Section 23(1) provides that; "Where the Bureau has instituted an investigation or a prosecution in respect of an offence under this Act, the Director may, by written notice to any person, direct that such person shall not, without the written consent of the Director, dispose of or otherwise deal with any property, or proceed with any

contract, transaction, agreement or other arrangement, specified in such notice, which is the subject of, or is otherwise implicated in, such investigation or prosecution.”

Section 23A of the CPA further stipulates that: “At any stage during the investigation of, or the proceeding for, an offence under this Act, a court may issue a warrant authorising the Director, the Deputy Director or a senior police officer to seize or freeze any document, or other records or evidence or any asset, account, money or other pecuniary resource, wealth, property, or business or other interest”. The Section gives the Anti-Corruption Bureau officers and a senior police officers power to seize and freeze any document including asset connected with any investigations or proceeding.

Section 36A of the CPA also allows tracing of property as it states that: “Where a court is satisfied in proceedings for an offence under this Part that, having regard to the closeness of his relationship to the accused and to other relevant circumstances, there is reason to believe that any person was holding pecuniary resources or property in trust for or otherwise on behalf of the accused or acquired such pecuniary resources or property as a gift or loan from the accused without adequate consideration, such pecuniary resources or property shall, until the contrary is proved, be deemed to have been under the control or in the possession of the accused.”

### ***The Police Act***

Section 35 of the Police Act allows senior police officers to search and seize. It provides that; “(1) Whenever a police officer of or above the rank of sub-inspector has reasonable grounds for believing that anything necessary for the purposes of an investigation into any offence which he is authorized to investigate may be found in any place and that such thing cannot in his opinion be otherwise obtained without undue delay, such officer may, after recording in writing the grounds of his belief and specifying in such writing, so far as is possible, the thing for which search is to be made, search, or cause search to be made, for such thing in any place and, if such thing be found seize it and carry it before the nearest magistrate empowered to take cognizance of the offence to be dealt with according to law.”

This variable is rated **Medium High (0.7)**.

### **Quality of FIU Intelligence Gathering and Processing**

The FIA is created under the Financial Crimes Act number 14 of 2017 and is mandated to receive disclosures from reporting institutions. The FIA’s Monitoring and Analysis (M & A) department is responsible for intelligence gathering and processing. The department currently has five members of staff with all of them having been trained in various techniques in financial intelligence analysis and use of specialised software. According to the FIA organogram, M & A department is supposed to have 13 staff members, including investigators. The FIA has taken a graduated approach in

recruiting the additional staff in line with governments yearly recruiting specifications. In view of the number of analysts, the FIA is in the process of automating a number of its activities to ease the workload. To this effect, the FIA is commissioning a new generation online reporting platform and Case Management System.

The FIA has access to several of sources of information that is important for its work. There are agencies that provide information to the FIA once requested such as the Registrar General's department for beneficial ownership information, Traffic Directorate for plant and motor vehicle ownership and Department of Lands and Urban Housing for ownership of real property, and the Malawi Revenue Authority for tax and customs information. However, there is usually time lag in providing the information largely due to bureaucratic tendencies within these agencies and the fact that some agencies hold records in manual format. The FIA also has access to an international platform to screen entities if they have adverse or any related reports on them including OFAC and UK's HM Consolidated Lists of targets for sanctions.

The FIA operates under a high degree of independence in terms of analysis and other processes. To this effect, the FIA has Standard Operating Procedures (SOPs) that are defined and are void of any external influence. The FIA is committed to a values regime that is governed by Conditions of Service and a strict Code of Ethics. All employees of the FIA sign an Oath of Confidentiality upon joining the institution and complete asset declaration forms. In addition, all members of staff are obliged to declare interest in matters that are being handled by the FIA. FIA Malawi's work has been acclaimed by other similar institutions within the region and beyond as a model FIU. Just like other Ministries, Departments and Agencies (MDAs), the FIA faces funding challenges. Funding has been erratic for the past few years. However, the situation improved in the 2016/2017 financial year.

Financial institutions and DNFBPs are obliged to submit reports (LCTRs, STRs and EFTRs) to the FIA. The banking sector has been the predominant source of these reports while the Insurance sector has improved significantly in terms of reporting albeit mostly on LCTRs other than STRs. The DNFBPs have also started submitting reports, with the casinos and gaming houses sector taking the lead in the reporting.

Once received, STRs are prioritised and this forms a critical part of the analytical process. The reports are classified under three priority categories namely; high, medium and low. Due to the inadequate number of staff within the FIA, low priority STRs are filed to the database for future use and reference. The STRs are analysed using various tools and once the FIA substantiates an offence, the files are disseminated to appropriate LEAs as intelligence. The STR reporting regime is continually being improved.

The passing of the FCA has empowered the FIA to conduct investigations into ML to track, and where appropriate confiscate proceeds of crime. The FIA has received 514 STRs from financial institutions during the past 5 years as follows:

*Table 6: Statistics of STRs received by the FIA*

Year	2013	2014	2015	2016	2017
STRs received	70	82	81	134	147

There has been a significant increase in the STR numbers owing to various initiatives taken by the FIA in the period 2014 to 2016, including conducting training for reporting institutions upon request. Between 2013 and 2017, the FIA disseminated a total of 195 reports to various stakeholders, of which 123 were sent to LEAs (MRA, Police, ACB and DPP). Other reports were disseminated to RBM and other regulatory bodies for their noting and action.

The FIA has been an active member of Egmont Group of FIUs since May 2009. As a result of this membership, FIA is able to exchange information spontaneously or upon request.

In accordance with section 55 (1), the FIA is also mandated to receive declarations made by travellers leaving or entering Malawi with cash or bearer negotiable instruments over a given threshold. The declarations will be made under form number 47 and will be administered by an authorised officer which includes officers of the Malawi Police and the Malawi Revenue Authority. The FIA has not yet started receiving these declarations, as the declaration system is not established. However, the FIA is a member of the task team established to implement the cross border currency declaration regime.

The main challenge faced by the FIA has been on the quality of STRs submitted by the reporting entities, which are sometimes of poor quality as they do not contain sufficient information to establish reason for suspicion. As such about 20% of the STRs received by the FIA were relegated to low priority after using the prioritisation tool and were filed to the database.

A second challenge relates to the delays faced by the FIA to obtain information from other agencies. Often, other agencies are unwilling or slow to in providing information on business, land, motor vehicle and other property ownership in their databases to the FIA on cases under analysis/ investigation.

In addition, the FIA has faced challenges in handling financial intelligence due to poor coordination with the LEAs. In the past, the FIA did not have the power to require LEAs to provide feedback on the cases investigated from information provided by the FIA. The FCA has put obligations on LEAs,

as recipients of financial intelligence, to provide feedback on all disclosures that they receive from the FIA.

FIA staff are generally of high integrity. However, there has been one incident in which the integrity of the FIA staff was brought into question resulting in one member of staff answering criminal charges. The individual was dismissed from work following arrest and subsequent disciplinary proceedings. This happened in 2015 and since the incident FIA instituted additional measures to monitor its staff.

In view of the above, this variable is rated *Medium High (0.6)*.

### **Capacity and Resources for Financial Crime Investigations (including Asset Forfeiture)**

#### **Capacity**

Financial Investigators in Malawi fall under distinctive areas of expertise, tax investigations, corruption, ML and general financial crime investigations. The capacity of the key institutions in financial investigations is inadequate. Despite attempts made to recruit the best people on the market, most competent and qualified people prefer to work in the private sector. In recent years' new recruits in various agencies are not accorded the training comparable to what was accorded to new recruits of past years due to unavailability of funds.

The investigative authorities in Malawi use financial intelligence in their work. There are several sources of financial intelligence at the disposal of financial investigators, and the MRA, Police and ACB have their own mechanisms in place to collect such intelligence on the cases that they are investigating. However, these institutions also use intelligence received or obtained from the FIA resulting from STR analysis or requests for information. The Police, ACB, MRA and RBM have effectively used financial intelligence to successfully investigate and prosecute a number of cases in 2016 on tax evasion and illegal externalisation of foreign currency.

There is, however, a need to incorporate ML investigations as an additional dimension to the investigation of predicate offenses. The FCA now gives the FIA additional powers; to investigate. This provides an opportunity to ensure that money laundering aspect form part of an investigation at an early stage.

#### **Resources**

In terms of resources, there is a perennial challenge facing investigative institutions, which starts from the budgetary allocations. An institution is often given low budget ceilings which would nonetheless be approved by Parliament. The actual funding and cash flows is another serious



challenge as by the end of the financial year some institutions may not be funded all the appropriated budget by the Parliament. The report is cognizant of the financial challenges Government is going through. The challenges cascade through to the financial investigations chain.

Another challenge is the stringent approval, by Government, to fill established positions. This challenge is mainly faced by FIA and ACB. This leads to the institutions operating below human resource requirements. Some officers leave the service to join other institutions, particularly the private sector, where there may be better perks career progression. This leads to the losing institution having to replace the officers and train the replace staff.

In the case of the ACB, the recently approved establishment indicates that the institutions should have 46 investigators. In 2013 the investigator contingent was 27 but it is currently at 21 as five resigned in pursuit of better perks or career progression. This leaves the ACB at below 50% of the required investigator capacity. It is not known when funds will be available to fill the vacant positions.

Fiscal and Fraud Unit of the MPS has 43 investigators country wide. The number is inadequate considering the volume of cases that the department handles. There haven't been any cases of officers leaving the service lately but few have been transferred to other departments of the MPS. All officers have undergone training and have varying levels of knowledge and competence in ML, financial investigation and asset recovery. One of the challenges experienced by MPS is lack of basic equipment such as laptops, desktop computers and other basic office equipment.

The FIA currently has four analysts, two of which double as investigators. One is on long-term training outside the country. There are plans to recruit one more analyst and two investigators in the medium-term. The total establishment for the FIA's analysis and investigations sections is 13. Most of the members have undergone training programmes, most of which is mostly development partner driven.

Currently, the major challenge is mobility. This problem is endemic mostly to FIA, Police and ACB. Most of the vehicles in service are old and hazardous and costly to maintain. Even where they are maintained, fuel is sometimes not readily available because of long gaps between monthly funding. When the funding does come it is mostly about half of the monthly cash flows, and payments are further delayed because of the centralised Integrated Financial Management Information System (IFMIS) payment system.

Funding challenges often delay investigation programmes up to 30 days or beyond. This leads to delayed execution of activities, and an accumulation of programmes which defeats the agenda of the institutions.

Although the CPA was amended in 2014, there are still some provisions that affect effectiveness and efficiency of the operations of the ACB. For instance, Section 15 empowers an officer to arrest an offender but only upon obtaining a warrant from a magistrate. It should be noted that in some cases by the time a warrant is obtained, the crime scene would have been tampered with and therefore making it difficult to obtain the required evidence.

The FIA has recently been mandated with investigative powers. This will assist the current workload on financial investigations. However, the institution is yet to fully implement the powers. The FIA has drawn up an action plan which will see the investigative powers fully applied by January 2019.

The FCA provides for robust asset forfeiture regime with powers to obtain records held by reporting entities. Under Parts IV to VI (i.e. Sections 54 to 116 of the FCA), the law has empowered ML investigators to not only have access but also identify assets without prior notice to the owner.

The FCA has provided for procedures to be used by ML and asset forfeiture investigators. The procedures include search of premises, taking witness statements and seizure.

The investigative authorities cooperate on ad-hoc basis or as part of a task force to tackle specific investigations that are of mutual interest. The FIA also has a number of MoUs with other agencies including MRA, Police and ACB. Agencies are working together more in the recent times unlike the period before 2013. Police, ACB and FIA continue to jointly work on a number of cases that are under investigation. Domestic LEA cooperation has not always been on a very good footing. Operational spaces for agencies usually overlap and this caused some friction in the past. There are now corroborative efforts to achieve ultimate goal through better communication.

The agencies mentioned above including other non-investigating authorities such as Immigration, Ministry of Trade and Industry are members of the Committee on Exchange Control and Trade Issues. This committee is not only a source of wide ranging information on the Exchange Control issues but also other financial crimes. There is a collaborative effort in working together to solve cases.

The other collaboration is on combating wild life crime, the agencies are members of the Interagency committee on wild life crime and ancillary money laundering that follows.

Due to lack of training and inadequate resources at the disposal of investigative agencies, the vulnerability for this variable is therefore Medium (0.5).

### **Integrity and Independence of Financial Crime Investigators**

Investigators have largely been of high integrity. According to the law, the heads of institutions of the ACB, FIA, MPS, MRA and the DPP's Chambers are appointed by the state president. Heads of these institutions report to parliament as a check and balance. However, there is perception that their independence is on paper and that they might ignore or delay pursuance of investigations on high profile figures since they are appointed by the executive.

Heads of the institutions hold the mandate to approve the investigation of cases. The setback in this area is that apart from the ACB and MRA who have guiding manuals on when to open and an investigation, organisations such as MPS do not have the same. The lack of such guiding manual in some investigative organisations has led to slow and sometimes disorganised investigation on money laundering and forfeiture cases involving public and politically exposed persons.

Recently there have been frequent sensitisation programmes for investigators on how to maintain their integrity. This has improved the rating for this variable. There has also been improved legislation such as the new FCA which has eased the way forfeiture is conducted. That will likely improve investigators' integrity since it will be easy to question why they are not using the simple forfeiture methods provided by the new law. The score for this variable is 0.50 (Medium) because integrity is important for successful investigation and prosecution, and where this is lacking, the whole system falls apart.

### **Capacity and Resources for Financial Crime Prosecutions (incl. Asset Forfeiture)**

The DPP is the lead agency in all prosecutions in Malawi and is supported by the RBM, ACB, MRA and MPS. However, the DPP has few prosecutors dedicated to financial crimes and asset forfeiture cases. The RBM, ACB and MRA have qualified lawyers to carry out prosecution of the cases and the standards of the prosecutions are good. The MPS has fewer prosecutors who are qualified lawyers as compared to those who are not lawyers. Prosecutors who are not qualified lawyers, can only appear before the Magistrate Courts.

Despite challenges mentioned above, Asset Forfeiture applications have been pursued in cash-gate and other cases. The Penal Code has always had the provides for conviction-based asset forfeiture as long as it is done within a year of conviction. However, due to capacity challenges, these cases are sometimes not pursued within the timeframe.

There are resource constraints in the tracing and management of seized assets. Most of the LEAs do not have sufficient resources to implement effective asset management systems.

Based on the above information, this variable is rated **Medium High (0.6)**.

### **Integrity and Independence of Financial Crime Prosecutors**

According to sections 99 and 100 of the Malawi Constitution, the DPP is the overall in-charge of all criminal prosecutions in Malawi with powers to commence and discontinue proceedings. This acts as a check on the integrity of prosecutors because the DPP can call for the case when in doubt of a prosecutor's integrity. Further to this, the DPP reports to the Legal Affairs Committee of Parliament when proceedings are discontinued. Sections 76 to 79 of the Criminal Procedure and Evidence Code further elaborate on such powers. In addition, under section 42 of the CPA, the ACB has to obtain consent from the DPP before commencing prosecutions. The overall effect of these legal provisions is to ensure that prosecutorial decisions are guided by rule of law, and not subject to political or personal interests.

Despite the checks above, LEAs responsible for financial crimes prosecutors namely MPS, MRA, RBM and DPP are headed by people who are appointed by the state president. This has been perceived as creating a possibility to compromise the independence of the institutions. However, prosecutors can commence prosecutions without undue political interference, social pressure, intimidation or abuse of office.

There are no specific reports showing lack of integrity by financial crimes prosecutors. However, the integrity of prosecutors has been called into question especially from media reports. The ACB has also registered some cases since the last assessment.

This variable is rated **0.50 (Medium)**.

### **Capacity and Resources for Judicial Processes (including Asset Forfeiture)**

There has been limited AML training for judicial officers during the assessment period under review. Most judicial officers are therefore lacking in capacity and are not conversant with AML issues. This notwithstanding, the judiciary was part of the crucial stakeholders that were consulted when the Money Laundering, Proceeds of Serious Crimes and Terrorist Financing Act was being repealed by the FCA.

Despite the said lack of capacity, judicial officers have still been able to reside over ML case which have been successfully concluded with in convictions and in some instance asset forfeiture. For example, in the cash-gate cases, about 20 convictions have been secured, most notable ones being

those of The Rep vs Tressa Senzani, The Rep vs Oswald Lutepo<sup>21</sup> and The Rep vs Leonard Kalonga<sup>22</sup>. A number of cases still pending in court at various stages.

The courts have also made asset forfeiture orders allowing the State to recover MK212, 621,204.09, ZAR40, 000.00 and USD 20,000.00 on cash-gate cases. Further, the State has applied for a confiscation order against Oswald Lutepo for the sum of K1.4 billion and is commencing forfeiture proceedings against Leonard Kalonga.

Much as the convictions are a welcome development, there is need for judicial officers to undergo specialised financial crimes training for them to effectively and efficiently preside over such cases. Most judicial officers have general training and rely on submissions by the parties. It is important to note that capacity building for judicial officers is usually hampered by inadequate funding to enable officers acquire specialised skills when one considers all the cases that come before the courts. The judiciary therefore requires more funding to build the capacity of its officers.

This variable is therefore rated **Medium High (0.6)**.

### **Integrity and Independence of Judges (including Asset Forfeiture)**

An analysis of the cases that have gone before the Courts seem to demonstrate integrity and independence. There are few cases in which the integrity of judges has come under question. For instance, there have been media reports on “judge shopping” whereby lawyers look for particular judges who can make decisions in their favour. In addition, there is the question of the judicial appointments by the state president, which have been seen as based on other factors and not merit or deserving because of seniority on the bench. Such appointments are seen as compromising the independence of the judges.

In the past there have been unsubstantiated media reports on judge shopping by lawyers, where specific judges are sought to hear certain cases. In another reported case, a judge made a ruling on a case that was heard by another judge. The judge in question died while the case was still under investigation.

In terms of AF, the Judges have shown good performance on both factors. The AF that has happened is in cash-gate cases and perhaps the Courts also feel outraged just as part of the general population. It is yet to be seen and tested in other cases outside the *cash-gate* setting.

---

<sup>21</sup> Criminal case No. 2 of 2014

<sup>22</sup> Criminal case No. 68 of 2014

This variable is rated **Medium High (0.6)**.

### Quality of Border Controls

Malawi has 5 main land border crossings with neighbouring countries (1 with Tanzania, 3 with Mozambique and 1 with Zambia) and smaller border posts which are mostly unmanned. Some spots of unmanned border line, whose re-affirmation exercise is on-going, makes the country's land borders porous. There have been a number of arrests of illegal immigrants who are believed to be smuggled by syndicates. Most of the illegal immigrants are from the Horn of Africa and beyond (countries like Somalia, Egypt, Ethiopia, Eritrea including Pakistanis, Bangladeshi). It is believed that they use unchartered routes to enter Malawi. There are efforts for effective border control to the extent that travel documents are issued to eligible persons by Department of Immigration and Citizenship Services and establishment of border posts in all main and smaller border points to curb smuggling.

Nevertheless, at international level, there are bilateral and multilateral arrangements with INTERPOL and with platforms such as a Joint Permanent Commission on Defence and Security (JPCDS), Southern Africa Development Cooperation (SADC) trade agreements and MOUs with neighbouring countries to curb the challenges associated with trans-border criminal activities.

While legal trade usually follows authorised entries and exits, cases of illegal border passes are found amongst traders. Lack of national ID makes manual tracing of suspected criminals difficult. In addition, the underlying language and cultural connections between Malawians living in border districts and people from neighbouring countries due to intermarriages makes following up of suspected criminals hard for law enforcers.

Some of the country's borders are known as routes for smuggling trade goods, people, drugs and can also be abused for smuggling cash. This is largely in smaller borders that are not in the spotlight and not adequately manned. Observably, Chisinga in Kasungu is prone to illegal wildlife trade, Marka-Nyathando in Nsanje is known for smuggling of stolen motor vehicles especially from the Republic of South Africa, while there have been cases of rampant smuggling of manufactured food products between Malawi and Zambia through Mchinji border post. Maize is predominantly smuggled out of Malawi through Mbilima border post in Chitipa while timber is smuggled through Nayuchi border post.

Uncharted routes such as in Mwanza have been used for human trafficking. There have been cases of human trafficking involving persons disguised as refugees, asylum seekers or immigrants transiting through Malawi into Mozambique then onward to the Republic of South Africa. In 2016,

over 50 children who had been trafficked from Malawi were apprehended in the Republic of South Africa.

There have also been cases of drug trafficking recorded in 2015 and 2016. Foreign nationals were arrested at Kamuzu International Airport for possession of cocaine coming from Asia and South America and wildlife trophies heading to Europe and Asia. There have also been cases of medical drug proliferation along the border and currency externalisation by locals and foreigners.

Overall, financial and human resource constraints affect the effectiveness of suspicious activity monitoring and reporting along the borders. The need for community policing teams in villages, effective security patrols, actionable intelligence gathering and sharing with the defence and security sector at local and international levels is compromised due to lack of such resources.

This variable is rated **Medium Low (0.4)**.

#### **Comprehensiveness of Customs Regime on Cash and Similar Instruments**

Malawi has a declaration system whereby travellers are required to declare the amount of currency they are bringing in or taking out of the country (Section 55 of FCA). The system is administered by MRA, MPS and Immigration. These agencies draw their powers from the FCA. Where the authorised officer has reasonable grounds to believe that currency or BNIs found in the course of an examination or search may afford evidence as to the commission of an offence under the FCA, the officer has the powers to seize the currency or BNIs. The currency may be confiscated if it is established that it is proceeds of crime, upon conviction.

The FCA provides that a person who fails to declare or makes a false declaration commits an offence and is liable, on conviction, to a fine of K5,000,000 and ten percent of non-declared amount. False declaration or non-declaration is also an offence under section 55 (5) of the FCA.

Based on the above facts, this variable is therefore rated **Medium High (0.7)**.

#### **Effectiveness of Customs Controls on Cash and Similar Instruments**

Malawi has 2 airports and 7 land border posts. Travelers are required to make declarations such as on goods and currency at these places. However, there is irregular or no provision of declaration cards at such places. In instances where the declarations are provided, both the officers and travellers do not take the declarations seriously.

There are inadequate laid down procedures to govern the screening of travellers and their luggage. In addition, there are no facilities at the border posts for such specific purposes. There are scanners

at some major border posts but they are focused on determining the correctness of the importer's declaration in respect of quantity and nature of goods.

There is no recorded case by Customs/MRA of seizure or prosecution on unauthorised transportation of cash. Precious metal and stones are restricted by relevant regulatory bodies. The existing controls are inadequate and therefore not efficient.

Rating for this variable is **Low (0.3)** as there is no effectiveness of customs controls on cash and similar instruments.

### **Effectiveness of Domestic Cooperation**

At a national level Malawi has a national AML/CFT Committee which has recently been formally recognised and constituted. Its members include the heads of public institutions including but not limited to MRA, ACB, DPP, RBM, MGB, FIA, MPS, NIB, MoJCA, MoFEPD. According to its terms of reference the Committee is chaired by the Secretary to the Treasury, and the FIA is the Secretariat, it has the option of co-opting other ministries and agencies as it deems necessary. In the past the committees operated in a vacuum without terms of reference as stipulated by international standards. The committee is responsible for coordinating AML/CFT issues including making recommendation on AML/CFT policy in Malawi and they form part of the Malawi task force of senior officials in the ESAAMLG.

At institutional level the FIA signed MoUs with the RBM, ACB, MRA, MPS and the Department of Immigration. The MoUs have the purpose of enhancing information sharing among the parties. The ACB also has an MoU with MRA to share information. The FIA has a standing calendar where they schedule meetings with LEAs to get feedback on what the LEA have done with the intelligence disseminated to them. On major cases that have a common interest, sometimes the LEAs form taskforces to share information.

The RBM also established a Committee on Exchange Control and Trade Issues that exchanges information and intelligence. This committee comprises members from the RBM, FIA, MRA, MPS, Ministry of Trade and Industry and Immigration and ACB. This committee meets quarterly and has worked together to resolve cases involving violations of the Exchange Control act and other trade related statute.

There is also an Inter-Agency Committee on Wildlife Crime whose members are Department of National Parks and Wildlife (DNPW), FIA, MRA, ACB, Police. The committee also has observers from development partner agencies. This Committee is responsible for resolving wildlife cases involving flora and fauna.



With regard to reporting institutions, the FIA and RBM meet compliance officers from financial institution to discuss matters of common interest. This forum offers a platform for guidance and communication of initiatives to improve reporting and compliance in general. Compliance officers are also encouraged to call or email on officers of the FIA directly when they have queries or challenges regarding their work or compliance with the FCA.

Despite having cooperation instruments in place, there are instances where the institutions disagree on how to proceed with certain cases. This challenge is not unique to Malawi where agencies differ in opinion on how to proceed in certain instances.

This variable is rated **Medium High (0.6)**.

### **Effectiveness of International Cooperation**

Malawi is a signatory to a number of regional and International accords on cooperation for instance the United Nations Convention Against Corruption (UNCAC) and the African Union Convention on Prevention and Combating Corruption which have provisions pertaining to AML/CFT. Besides these instruments, the country has signed a number of Mutual Legal Assistance Treaties with other jurisdictions pursuant to the Mutual Legal Assistance in Criminal Matters Act (Cap 8:04).

Competent and supervisory authorities such as the RBM, FIA, MRA and Police have formal and informal arrangements in international arena in the respective areas of expertise. The FIA has been a member of the Egmont Group since 2009. Egmont Group of FIUs offers a platform that enables members to securely share information on the Egmont Secure Web (ESW). Further to this, the FIA has signed information sharing MOUs with the FIUs of, among others, the United States of America, Namibia, France, United Arab Emirates, South Africa, Mauritius, Tanzania, Philippines, Japan, Madagascar and Sierra Leone. Pursuant to its Egmont membership and its international obligation the FIA has requested information or shared information either on request or spontaneously on a bilateral basis with other FIUs. The information provided by the FIA includes information on beneficial ownership. FIA always gives priority to financial investigations with an international angle.

RBM has MOUs with central banks of several countries including, Zimbabwe, Botswana, Mauritius and South Africa. These MOUs provide for information sharing, consolidated supervision and monitoring where shareholders of financial institutions are from foreign countries. For example, RBM and the South Africa Reserve Bank conducted a joint inspection on a bank in Malawi which has ties with a bank in by South Africans.

Malawi has a robust Mutual Legal Assistance Regime that is provided under the Mutual Legal Assistance in Criminal Matters Act and the Extradition Act (Cap 8:03) of the Laws of Malawi. The

Attorney General's office handles all MLA issues in Malawi. The general view is that when a requesting jurisdiction is making its representations, usually a court process will have ensued and hence the matters are handled urgently. The Attorney General's office has adequate staff to handle MLA matters.

In 2013/14, there was one major case that involved money laundering and which also targeted asset forfeiture. There were however, some technical challenges after the suspect was deceased. The asset forfeiture provisions under the ML legislation which was in force at the time were conviction-based. The FCA has covered all the envisaged scenarios including where the person of interest is deceased or has absconded.

Apart from the FIA's interaction with other FIUs, the country has not had a high number of international cooperation on supervisory authorities' exchanges and cases for extradition. The police and ACB usually make use of INTERPOL platforms to pursue cases that have international dimension. The ACB has a network of similar agencies that the institution interacts with on regional and global level. MRA also has its own network with counterpart tax authorities across the globe.

There are a number of challenges under international cooperation; one significant one is delay caused by bureaucratic processes. Once a request is made to a foreign jurisdiction, experience has shown that it can take up to a few years before getting a response. For instance, in 2014 the FIA made a request which was not responded to until the jurisdiction made a spontaneous disclosure on the subject in 2017, at which point reference was made to the 2014 request. Other agencies have indicated that it can take up to 2 years for an extradition case to be concluded.

The other challenge is the minimal cooperation and coordination among the local stakeholders. Some cases are usually singlehandedly investigated by one agency where collaborative efforts would have achieved better results if another agency leveraged its international links.

This variable is rated medium with a score of **0.50 (Medium)**. This is because the challenges are overshadowing the efforts made in signing of MoUs and other forms of collaboration.

### **Availability of Independent Audits**

The accountancy profession in Malawi is regulated by the Malawi Accounting Board (MAB) established under the Public Accountants and Auditors Act (PAAA) No. 5 of 2013. The objectives of MAB are; promoting high quality reporting of financial and non-financial information by entities, promoting highest professional standards among auditors and accountants, enhancing the credibility of financial reporting, improving the integrity, competence and transparency of professional activities in accounting and auditing and improving the quality of accounting and

auditing services, among others. It works closely with the Institute of Chartered Accountants in Malawi (ICAM) which is mandated to set accounting standards by the PAAA. The PAAA makes it mandatory that every person offering services as or holding himself out to be a public accountant, chartered accountant or diplomate accountant in Malawi should be registered with MAB and therefore are regulated.

Financial reporting and auditing in the country are conducted in accordance with generally accepted auditing standards as adopted by ICAM: these are the International Accounting Standards (IAS), International Financial Reporting Standard (IFRS) and International Standards of Auditing (ISA). There are also compliance gaps by small and medium enterprises (SMEs) due to the fact that IFRS are too onerous for them. Reporting entities are required to rotate their independent auditors or audit firms every 5–7 years. For example, RBM's directive on Annual Audit of Banks requires independent auditors of banks to be changed every 5 years; the audit firm can remain the same but the partner has to be changed. For non-financial public institutions and listed companies, the requirement is to change auditors every 7 years. For other private companies, auditors/partners are supposed to assess themselves for their independence.

According to MAB there have been no reported integrity breaches by independent auditors / audit firms the past few years. However, some small and medium enterprises (SMEs) have been known to keep two sets of records on sales with the aim of evading value added tax.

It is mandatory for reporting entities to evaluate the independent auditor's/audit firm's performance. It is common practice in the country for reporting entities to periodically evaluate their independent auditors' performance; for example, most parastatals evaluate their auditors every three years. However, it is not mandatory for reporting entities to disclose professional fees paid for audit and non-audit services.

Effective engagement and communication between independent auditors and audit committees of organisations happens before, during and after the audits. Regular communication between reporting entities' supervisory authorities, audit firms and the accounting profession as a whole on key risks and systemic issues, as well as a continuous exchange of views on accounting and auditing issues do take place. ICAM regularly organises conferences, publishes magazines and on its website updates on industry issues concerning accounting and auditing for all these stakeholders. On the other hand, dialogue between reporting entities' supervisory authorities and relevant audit oversight body takes place when need arises.

Potential or existing independent auditors are required to disclose any independence issues and confirm their independence to MAB when carrying out their duties. In addition, audit rules also require the prospective independent auditor's internal control procedures to guarantee the uniform quality of the audit and compliance with auditor independence requirements.

This variable is rated **High (0.7)**.

### **Level of Financial Integrity**

Companies are obligated under the Companies Act, 2013, to submit audited financial statements to the Registrar of Companies. However, there is lack of enforcement on the part of the Registrar in cases where companies do not file the returns. This may be due to technology challenges which are currently being addressed as well as attributed to the small fines imposed for non-compliance. The Act also demands companies to have a board of directors with at least three directors that regularly meet and hold annual general meetings to review and report on the company's performance to the shareholders. There is commitment to good corporate governance and compliance by listed/licensed companies as it is a requirement by their respective regulators such as the Malawi Stock Exchange, the Registrar of Financial Institutions, etc. For example, the Registrar of Financial Institutions has issued various directives on corporate governance for its licensed financial institutions. Likewise, private companies are committed to good corporate governance as this leads to high ratings when accessing financing and striking significant business deals.

Most companies are complying with the tax laws, as the MRA has been aggressive in ensuring compliance. In addition, the Office of the Director of Public Procurement demands a tax clearance certificate for a company to be registered as vendor to supply goods and services to public institutions.

The MRA conducts comprehensive taxpayer education programmes for taxpayers to comply with tax changes as well as various provisions of tax laws. These programmes have enabled taxpayers to understand their rights and obligations under the tax laws and subsequently have promoted compliance. The tax laws require tax payers to provide comprehensive information about their income and assets to MRA. However, it is easier for MRA to enforce this requirement with legal persons than individuals. Pay As You Earn (PAYE) tax information for individuals who are in formal employment is made available to MRA by their employers. Information on sources of income other than formal employment is a challenge.

There are innumerable instances where non-compliance with tax legislation has elicited imposition of sanctions. Just to mention a few notable instances – motor vehicles are seized for non-payment

of duty almost every week; administrative penalties are routinely imposed for recalcitrant tax payment defaulters or those with intentions to deliberately defraud.

This variable is thus rated **Medium (0.5)**.

### **Effectiveness of Tax Enforcement**

The tax legislation of Malawi includes the MRA Act, Taxation Act, the Value Added Tax (VAT) Act and the Customs and Excise Act. These empower the MRA to access and obtain information that is relevant to revenue collection. For instance, sections 86 of the Taxation Act allows the Commissioner General of MRA to access all public records deemed necessary to assess, demand or enforce revenue collection. Taxpayers are obligated to comply with notices from MRA requiring the production of information – section 88 of the Taxation Act and section 58 of the VAT Act.

To ensure compliance with the dictates of tax legislation, sanctions have been provided for to penalise and deter non-compliance. The sanctions comprise: Administrative penalties – section 112 of the Taxation Act, section 143B of the Customs and Excise Act; forfeitures, seizures, embargoes under Part XVIII of the Customs and Excise Act; civil claims and liens- section 107 and 107A of the Taxation Act respectively; distraint –section 40 of the VAT Act; and prosecution of tax offences- Part XII of the VAT Act and Part XVII of the Customs and Excise Act.

Notably, both conviction based and non-conviction-based forfeiture are provided for in the tax legislation. Under the Customs and Excise Act, goods or conveyances that have been seized for contravening customs laws are liable to forfeiture –sections 145 and 146. If such goods or conveyances are not successfully claimed by the owner they are forfeited to the government of Malawi and are either sold, destroyed or otherwise dealt with as deemed fit by MRA.

Tax audits are a critical tool and an integral part of a compliance management programme in MRA. They provide the tax administrations with significant leverage across the business community and not only impacting on taxpayers selected for audit. The impact of tax audit is felt through corrective measures where instances of non-compliance to the laws are detected and the deterrent effect where they influence the behavior of the selected taxpayer and potential non-compliant taxpayers.

Malawi Revenue Authority achieves a balanced audit programme through implementation of a risk-based audit programme, covering a wide range of audit types. For example, in fiscal year ending June 2017, the audit function concluded 170 comprehensive audits, 318 issue-oriented audits, 65 desk audits and 34 representing other audits such as refund. The programme also includes carrying out quality assurance checks on concluded audits in various audit functions to ensure achievement of quality conduct of audits and application of appropriate regime of penalties to deter non-

compliance. with tax laws. For instance, sections 112 (3) of the Taxation Act and 38 of the VAT Act deals with penalties and interest to deter non-compliance

Tax audit programmes have adequate financial resources both at Head office level for carrying out planning and monitoring activities and in operational offices for delivery of the audit programme but human resources are not adequate. The audit function is headed by the Deputy Commissioner responsible for audit who reports to the Commissioner for Domestic Taxes. Under the Deputy Commissioner – audit there are 2 Managers at Head office level and also 2 Managers managing the audit function at Large Taxpayer Office (LTO).

In respect of numbers of staff, LTO has 38 auditors whilst the rest of the other stations including Blantyre, Lilongwe, Mzuzu and Zomba, are allocated an aggregate of 45 auditors. The number of auditors is not adequate considering the number of registered Taxpayers hence low coverage ratio especially for other than LTO. There are intentions to increase the number of auditors but shall depend on other factors especially availability of financial resources. Auditors stay at the function for adequate periods of time to encourage specialisation to address specific risks to particular segments or sectors but movements do also happen to match the technical capability of auditors to maintain a balanced audit programme.

The audit function at the MRA is usually staffed with tax auditors with accounting and economics background. Most auditors have a minimum of a degree and are qualified accountants or pursuing professional courses especially Association of Chartered Certified Accountants (ACCA). They have to be trained in Taxation, VAT and Domestic Excise laws at the MRA Institute of Tax Administration before being deployed on audits. They are also continuously exposed to various international trainings in auditing and transfer pricing.

Safeguards are in place to preserve the integrity of tax officials through provision of manuals such as audit manual that stipulate the procedures and processes that auditors need to follow. If they happen to make mistakes whilst on duty, they are given opportunities to be heard through appropriate mechanisms such as disciplinary hearings.

The institution has lagged behind in implementing audit measures much as intentions have been there. Though a survey was once implemented to establish perception of taxpayers towards the institution but not specifically on tax audits. The statistics of integrity breaches by tax audit staff in MRA is fairly low. From February 2013 to November 2017, there have been four (4) cases of alleged integrity breaches by tax audit staff involving a total of seven (7) officers. Out of the 7 officers only

two were proved to be in serious breaches and dismissed from employment while five (5) were cleared of the alleged breaches

There has been no specific survey that has been conducted on the level of corruption/integrity of MRA. However, the Governance and Corruption Surveys of 2013 which was sanctioned by the Anti-Corruption Bureau revealed a mixed picture about the state of corruption in MRA. Whilst the perception of staff showed low prevalence of corruption, the perception of the public, business and other public officials on the other hand gave a different picture. For instance, payment of bribes to avoid taxes was considered as having the most significant impact on the economy amongst the factors that were listed. The 2013 survey indicated that the MRA had improved in ranking in terms of institutions that the public considered to be most corrupt. For example, while in 2010 a similar survey established that MRA officer received the highest number of gratification payments at 43%, the 2013 survey on the other hand showed that the cabinet ministers and MPs had displaced MRA officials at the number one positions having received 81 % of gratifications.

MRA has a Corporate Affairs Division which conducts annual comprehensive taxpayer education programmes to mobilise taxpayers to comply with tax changes as well as various provisions of Customs and Domestic Taxes laws. The programmes comprising print, electronic and outreach campaigns have enabled taxpayers to understand their rights and obligations under the tax laws and subsequently comply. Taxpayers now demand fiscal receipts as a result of a robust Lisiti Langa EFD campaign. Taxpayers have also migrated to paying taxes online through ASCUDA World and E-payment system as a result of vigorous awareness campaigns. Local communities are also reporting cases of smuggling, tax evasion and fraud as a result of continuous awareness.

There are innumerable instances where non-compliance with tax legislation has elicited imposition of sanctions. Just to mention a few notable instances – motor vehicles are seized for non-payment of duty almost every week; administrative penalties are routinely imposed for recalcitrant tax payment defaulters or those with intentions to deliberately defraud. In terms of forfeiture, the High Court of Malawi in 2013 forfeited to the government of Malawi a consignment of alcoholic beverages worth circa MK20, 000,000 that was smuggled into Malawi: Thom Njilika vs. Malawi Revenue Authority (2013) Civil Cause Number 320 (HC) (PR).

In view of the foregoing, this variable is rated **Very High (0.8)**.

### **Level of Formalisation of the Economy**

Data on the size of the informal sector in Malawi is not readily available. The National Statistical Office (NSO) has never conducted an economic census to establish the size of the informal sector

and the national accounts do not provide an estimate of the size of the informal economy. However, according to a 2017 International Monetary Fund Working Paper<sup>23</sup> Malawi's informal economy is estimated at 34 percent of GDP. Most payments in the country are made in cash in terms of both value (25%) and volume (0.3).

There is no law or regulation that requires formalisation of economic activities in the country, however the Ministry of Industry, Trade and Tourism (MoITT) is drafting a legislation to this effect. However, there is the Micro, Small and Medium Enterprises (MSME) Policy whose objective is to encourage formalisation of enterprises. There are incentives prompting the transition from informal to formal economic activity such as the requirement of 60% of government procurement contracts to be made to local companies, 30% of which goes to small formal enterprises. There are also other incentives in terms of business support to SMEs by the MoITT and the Small and Medium Enterprises Development Institute (SMEDI) that target registered entities only.

This variable is therefore rated **Medium Low (0.4)** because a significant proportion of Malawi's GDP is informal where there is no regulation.

#### **Availability of Reliable Identification Infrastructure**

The national identification system is fairly new. As such, frequently used identification documents are passport and driver's licence. These are, however, only possessed by less than 10 percent of the population making proper identification of individuals a difficult exercise.

Under the current legal regulatory framework, financial institutions are obliged to undertake Know Your Customer measures but considering the above it is hard to identify an individual with sufficient particularity. This has resulted in banks using other unreliable source documents such as voter registration cards (which have since been discarded by some banks due to rampant fraud using the voter IDs), letters from employers, traditional/religious leaders, etc. to ID their clients. Further, phone numbers that individuals provide when opening accounts cannot be used to identify an individual as one can easily purchase a sim card without any registration at all rendering it difficult to clearly identify an individual. Furthermore, even the physical addresses that individuals provide do not provide much help as most areas cannot be identified with sufficient particularity owing to rapid development of unplanned urban settlements and the lack of zip codes in Malawi.

---

<sup>23</sup> L. Medina, A. Jonelis, and M. Cangul (2017) *The Informal Economy in Sub-Saharan Africa: Size and Determinants*, IMF, Washington DC



It is against this background that the National Registration Act was enacted in 2010 creating the National Registration Bureau (NRB) whose mandate, inter alia, is to issue national identity cards for all citizens above 16 years of age. The NRB engaged in a pilot registration exercise that saw most public servants and some private sector employees registered and issued with national IDs. The NRB then rolled out a national registration exercise requiring all persons to be registered and their IDs will be issued shortly. The total number of persons above 16 years of age registered is currently at just over 9 million. For those below the age of 16, their biometric details have also been captured and their ID will be produced upon their turning 16. The total number of those below 16 years of age captured is just over 4 million. In the meantime, they can apply for a birth certificate and to date the NRB has so far issued about 140,000 certificates since August 2015. It is also worth noting that all babies being born in hospitals are being registered at birth. With the total population projected at around 17 million it means about 4 million people are yet to be registered. In short, the NRB has embarked on a serious Civil Registration and Vital Statistics exercise that will see civil events like birth, adoption, marriage and death being captured at occurrence with attendant fines for late or failure to report.

In light of this the variable has a score of **Medium (0.5)** as individuals have just been captured into the database but are yet to be identified with sufficient particularity without their ID cards.

#### **Availability of Independent Information Sources**

Listed companies and financial institutions licensed by RBM keep records for a specified period as required under various legislations. However, it is challenging to access information for private companies after a considerable lapse of time because most of the information is kept manually and to create room, older information is destroyed. Most financial institutions verify information provided by clients on a risk-based approach. The higher the net-worth of an individual the more the need for verification (i.e. high-net worth person and PEPs pose a high ML risk).

The Government enacted the Credit Reference Bureau Act in 2010 to help with information on credit worthiness and general CDD of individuals and companies. Banks are under obligation to provide information on clients on their credit books and in turn obtain information on potential credit clients from credit reference bureau at a fee. However, the uptake has been very slow. One of the credit reference bureaus in the country, Credit Data had been complaining that financial institutions especially banks were shunning its services.<sup>24</sup> Recently five banks lost over US\$20 million that was provided as seasonal loan facility to a company that was involved in false

---

<sup>24</sup> <https://www.nyasatimes.com/parliament-gets-tough-on-malawi-banks-amends-crb-act/>

accounting and fraudulent activities. This theft could have been avoided if there was proper use of the services of credit reference bureau.

In Malawi there is no central repository for information, however verification can be done through relevant institutions that collect the information. For instance, banks verify company existence with Registrar General's Department (RGD) and physical addresses using utility bills. However, there are challenges with the utility bills as not all Malawians have water and electricity accounts in their names.

The vulnerability for this variable is rated medium low at **Medium Low (0.4)**.

### **Availability and Access to Beneficial Ownership Information**

Malawi does not have registered Trusts and Company Service Providers (TCSPs). Legal persons and arrangements can however be registered or administered by lawyers and accountants.

The RGD is responsible for registration of legal persons and arrangements. This Department collects basic information on legal persons and arrangements at registration and requires any changes to be registered within 28 days. However, the Registrar of Companies does not collect information on beneficial ownership of legal persons and arrangements. Currently the MoJCA is working on draft regulations to be issued under the Companies Act to mandate the Registrar of Companies to obtain and require companies to provide information on beneficial owners. The information kept by the Registrar General is accessible to LEAs free of charge and at fee to the public including the reporting institutions. The searches are manual and it takes a maximum of 72 hours to get the information.

Apart from this, the FCA requires reporting institutions to collect and keep beneficial ownership information of their customers and clients. Although the reporting institution collect such information, it is difficult for them to verify the information as the Register of Companies does not collect this information.

This variable is rated medium low at **Medium (0.5)**.

## **Banking Sector Vulnerability**

### **Background**

The banking sector in Malawi comprises 9 commercial banks and 1 leasing and finance company. The leasing and finance company is considered under this sector for the sole reason that its main transactions are deposits and withdrawals as such during assessments which the country does from time to time, as required by the World Bank or International Monetary Fund, the entity is considered under the banking sector.

The banking sector is the most significant sector with a total asset value of MK1.3-trillion as of April 2017, which is the highest among the financial sectors in Malawi and this is a significant jump for the sector which had an asset value of K531-billion in 2013. Furthermore, the sector's significance extends to the fact that it is vulnerable to both money laundering and terrorist financing since transactions in the sector are huge, swift and attract all kinds of customers carrying various money laundering and terrorist financing risk levels.

Between August 2014 and December 2017, the country recorded 16 convictions on money laundering from the 2013 public sector theft and fraud scheme commonly known as *cash-gate* scandal in which the country lost over K20-billion. Further, the courts convicted 2 individuals (a police officer and businessman) on money laundering charges in a K45-million fraud case which took place at the National Police headquarters for transactions whose services were not delivered by the businessman. Another police officer related to this case was convicted of negligence by a public officer. Information on the 2013 *cash-gate* and 2011 fraud case was mainly obtained through the banks as most cases involved funds that were cashed through the banking sector.

In terms of the legal framework, the sector is governed by the Financial Crimes Act 2017; Terrorist Financing and Proliferation Regulations 2017; and Money Laundering, Proceeds of Serious Crimes and Terrorist Financing Regulations 2011 on implementation of AML/CFT obligations as well as the Banking Act 2010, Financial Services Act 2010, and various Directives issued by the Reserve Bank of Malawi on implementation of prudential obligations and some AML/CFT obligations.

During the 2013 NRA, the sector's vulnerability to ML was rated medium high with a score of 0.71 due to poor quality of AML controls rated low medium contributed by quality of operations rated low medium and quality of policies and procedures rated medium. The most vulnerable products/services of the sector were trade finance, retail and corporate deposits, international funds transfers, private banking and SME credit products which had Medium-High vulnerability.

In this NRA, the banking sector's vulnerability is at medium high with a score of 0.62. The drop in the vulnerability score, as compared to the 2013 rate, is due to sector's improved quality of general AML controls. which is at 0.6 (i.e. quality of internal AML policies and procedures rated 0.66, quality of AML supervision rated 0.67, and quality of banks' operations rated 0.6).

The sector's vulnerability to TF is low. This is based on the fact that while some products are vulnerable to TF, there has been no TF case in the country and searches by the banking sector on international sanction lists have not resulted in any positive or true match.

## Overall Vulnerability

The banking sector's vulnerability is at 0.62 (Medium High) and is a result of the quality of the general AML controls rated 0.6 and this is derived from the quality of internal AML policies and procedures rated 0.66, quality of AML Supervision rated 0.67, and quality of Banks' Operations rated 0.6.

The vulnerability of the banking sector to ML has been highlighted in a number of ML investigations done and trials concluded or in progress. For instance, the Baker Tilly Report on *cash-gate* scandal of 2013 stated that *a total of 104 'cash-gate' cheques were paid into at least ten different commercial banks throughout Malawi with 22 cheques, linked to 10 different businesses, being banked at one bank.* The report recommended that *the relevant regulatory authorities should investigate the role of the banks in the cases where large sums of money were being deposited and then withdrawn to assess whether it would have been reasonable to expect the banks to raise concerns.*

## Assessment of Variables

The assessment of variables was in two categories, namely; General Input Variables and Products/Services variables. On the assessment of the general input variables, the banking sector scored relatively well, featuring several strong factors, such as a comprehensive legal framework including strong entry controls and a specific and ML risk-based supervision. There are, however, some areas of improvement, particularly in the detection of suspicious transactions and in the effectiveness of the compliance functions and availability and enforcement of administrative and criminal sanctions, as shown by the analysis below.

### Assessment of General Input Variables

#### *Comprehensiveness of AML Legal Framework*

The FCA is generally a comprehensive AML/CFT legislation, albeit with some deficiencies which include regulations on KYC, to enhance implementation of this law. Currently there are TF & Proliferations Regulations 2017 and Money Laundering, Proceeds of Serious Crimes and Terrorist Financing Regulations 2011 which are facilitating implementation of the law. The latter will be in force until replaced by regulations to be issued under the FCA as provided for under S.141(3) of the FCA. Based on this information, the variable is rated High (0.7).

#### *Effectiveness of Supervision Procedures and Practices*

The Reserve Bank of Malawi and the Financial Intelligence Authority have been conducting comprehensive risk-based AML/CFT supervision for the banking sector until February 2017 as mandated by the old ML Act and the MoU that was in place. Currently both FIA and RBM conduct

AML/CFT offsite and onsite supervision and ensure that all issues identified are addressed within specified timelines

The FCA mandates the FIA to supervise all reporting institutions under the Act, However, the FIA has limited financial and human resources to adequately supervise all the sectors. The FCA provides that the FIA may delegate to supervisory authorities to conduct AML/CFT supervision, however the FIA is yet to delegate the supervision powers for the banking sector to the Reserve Bank of Malawi. As such the Reserve Bank of Malawi is conducting the AML/CFT supervision based on Section 36(1) of the FSA.

AML supervision procedures and practices for the banking sector are effective save for the absence of the delegation of the supervisory powers by the FIA to the Reserve Bank of Malawi and absence of the MOU stipulating supervision roles for each authority.

Both FIA and RBM have comprehensive supervisory frameworks including clear supervision policies, procedures, manuals, tools and systems. Further, FIA and RBM officers are adequately trained and experienced to understand and appreciate ML risks within the sector and to carry out AML compliance examinations.

The Reserve Bank of Malawi has sufficient number of staff and financial resources to ensure AML compliance. The RBM received technical capacity assistance from the IMF for offsite risk assessment tool in 2014 and 2015. The Reserve bank is yet to have another technical capacity assistance for transaction monitoring tools from the World Bank in January 2018.

In particular RBM has developed an AML/CFT risk assessment tool for banks, which is fed by both qualitative and quantitative information (on, inter alia, products, customers, delivery channels, geographical factors and risk management and mitigation measures<sup>25</sup>), which are validated.

*Table 7: Banking sector supervision*

Year	Institutions Inspected	Supervisory Authority
2017	Ecobank	FIA
	CDH Bank	FIA
	FMB	RBM
	Standard Bank	RBM

---

<sup>25</sup> Such as the effectiveness of compliance governance, risk management, AML/CFT policies and procedures, internal audit and training and human resources)

	National Bank	RBM
	FDH	RBM
	CDH	RBM
<b>2016</b>	NFB	FIA
	FMB	RBM
	National Bank	RBM
	NBS Bank	RBM
<b>2015</b>	Inde Bank	FIA
	FMB	FIA
	Opportunity Bank	RBM
	FDH	RBM
	Standard Bank	RBM
	Nedbank	RBM & FIA
<b>2014</b>	Malawi Savings Bank	FIA
	Standard Bank	FIA
	FDH Bank	FIA
	NBS Bank	FIA
	CDH Bank	RBM
	FMB	RBM
<b>2013</b>	National Bank	FIA
	NBS Bank	RBM
	National Bank	RBM

Based on this analysis, the variable is rated High (0.7).

***Availability and Enforcement of Administrative Sanctions***

Section 34 of the FCA mandates the FIA to impose administrative sanctions on non-compliant reporting institutions. To operationalise this, regulations are being developed to cater for

application of monetary penalties. In the meantime, the RBM imposes sanctions on non-compliant banks based on the FSA, and the Financial Services (Customer Due Diligence Requirements for Banks, Leasing Companies or Discount House) Directive 2016. The sanctions have in form of monetary penalties and directive to do a specified action. The FIA has only sanctioned 1 bank by directing it in August 2017 to comply with reporting a specific suspicious transaction.

*Table 8: Administrative sanctions imposed on banks*

YEAR	NATURE OF VIOLATION BY THE BANK	TYPE OF SANCTION
2016	Non-compliance on-site examination and AML/CFT requirements	Warning letter
2017	Failure to implement most of the AML/CFT on-site examination recommendation	Monetary penalty of K30-million
2017	Failure to submit an action plan for the implementation of AML/CFT on-site examination recommendations within the stipulated deadlines	Monetary penalty of K25-million
2017	Failure to implement some of the AML/CFT on-site examination recommendations	First and final warning
2017	Resistance to file a suspicious transaction to FIA	Directive to file the suspicious transaction

The on-site examination reports on the banks conducted by the FIA and RBM have revealed significant deficiencies among the banks relating to compliance with various obligations including CDD, transaction monitoring, suspicious transaction reporting, and independent testing of the AML/CFT procedures and systems, which have not been sanctioned. This brings into doubt the effectiveness of the sanctioning regime. The variable is therefore rated Medium High (0.6).

#### ***Availability and Enforcement of Criminal Sanctions***

The country has effective, proportionate and dissuasive criminal sanctions. However, these criminal sanctions have not yet been enforced on the banks, their directors or senior management.

While there could be some investigations by law enforcement, there has never been a court trial in the local courts for AML non-compliance in the banking sector. Further, there have never been instances of criminal enforcement actions that have been carried out by foreign law agencies against the local banks and their staff. Based on this analysis, the variable is rated Medium (0.5).

### *Availability and Effectiveness of Entry Controls*

The regulatory requirements for establishing a banking institution are quite stringent. Sections 4 and 5 of the Banking Act provides for the licencing procedures and conditions. Part III of the FSA provides for licencing and registration of financial institutions.

The FSA grants the Registrar of financial institutions powers to assess fitness and propriety of a controlling party of a bank including beneficial owners. The threshold for controlling party is 10% shareholding, however; any person with power to exert significant influence even if they do not own 10 % or more of the share is considered a beneficial owner.

The provisions in the Banking Act and FSA highlighted above are in line with Principle 5 on Licensing Criteria contained in the Basel Core Principles for Effective Banking Supervision which provide guidance on Licensing the Financial Services (Fit and Proper Requirements for Shareholders, Directors and Senior Management Officials of Banks) Directive of 2014 also provides detailed requirements for entry into the banking sector with the aim of preventing criminals from operating in the sector thereby promoting financial integrity and stability in Malawi.

The RBM uses a questionnaire derived from Financial Services (Licensing of Banks) Directive, 2012 and this is filled by an applicant requiring a banking license. RBM conducts due diligence processes for all applicants for banking licence to determine if they are fit and proper. Further, for foreign investors which are corporates, meetings are held with their bankers, auditors as well as the FIU of the particular country in which the business is registered and this is aimed at collecting information including details of the shareholders, their financial statements and source of funds. For regulated investors, meetings are held with their home country supervisor. No shell banks are permitted to invest in Malawi. In instances where the investor is an individual, the FIU for a country in which the business is registered is also required to provide information that would be relevant to the application. In addition, a clean report is obtained from previous employers as well as a clean report from the police. The supervisors also assess the source of funds through analysis of financial statements and bank accounts of the prospective shareholders and beneficial owners to determine that the funds being invested are legitimate.

In addition to vetting of shareholders, the Licensing of Banks Directive requires that all Directors, executive officers and senior management officials not to assume their respective roles without prior approval from the Registrar. Further, the Financial Services (Fit and Proper Requirements for Shareholders, Directors and Senior Management Officials of Banks) Directive of 2014 has provided specifications for the position of head of finance, head of internal audit and compliance officer. Further, Section 27 of the FCA provides for appointment of a compliance officer, setting up of a



compliance management programme, and the policies, procedures and systems required for the function.

From 2013, the country has received one Banking license application and it was approved. No license application has ever been denied or revoked for failure to meet AML controls. Based on this information, this variable is rated Close to Excellent (0.9).

### *Integrity of Bank Staff*

Most bank staff discharge their duties with integrity. The banks have clear policies and procedures including on staff recruitment process which involves police screening and background checks with relevant authorities. Further, senior management staff, of banks are vetted by the RBM.

However, there has been isolated instances of fraud perpetrated by bank staff. These incidences are reported to Fiscal Police for prosecution and also internally sanctioned including termination of employment. The banking industry had 4,494 employees as at 31<sup>st</sup> December 2017 of which 27 were involved in fraud in the year 2016 representing 0.6 percent. Based on this analysis, this variable is rated Medium High (0.6).

### *AML Knowledge of Bank Staff*

Banks have internal policies on ongoing AML/CFT training for all staff as required under Section 27(1)(c) of the FCA. In addition, both FIA and RBM provide training to the sector especially to the Board members, Chief Executive Officers and Compliance Officers. The RBM and FIA have trained 646 bank staff since 2011 as follows:

*Table 9: Statistics of training for bank staff*

Year	No. of bank staff trained by FIA/RBM
2013	296 (8 of them Board members)
2014	69 (20 of them Board members)
2015	4 (Board members)
2016	231 (7 of them Board members)
2017	46

AML/CFT training to staff is delivered in two forms; through workshops/seminars and computer-based training. Further to that, some banks administer tests to staff to gauge their understanding of AML/CFT requirements aft the training. The training is extended to senior management and in some banks the board members are also trained.

Interviews with staff during onsite examinations by RBM and FIA have shown that senior management and the compliance staff are more knowledgeable on AML/CFT issues while in most banks the Board is not adequately aware of AML/CFT compliance issues. Knowledge levels are low amongst front line staff despite being trained on AML/CFT issues.

However, some banks do not comply with their own policies and do not conduct AML/CFT trainings on an annual basis. The variable is therefore rated Medium High (0.6).

### *Effectiveness of Compliance Function*

Most banks have an effective independent compliance function that is comprehensive and risk-based. Based on onsite examination reports and RBM's offsite returns data, only five players of the sector have well-resourced compliance functions; the other five bank's compliance functions are understaffed in comparison with their size and volume of transactions they handle.

Based on the onsite examination reports and December 2017 annual returns submitted by the banks to the RBM, the banks have a minimum of 2 and maximum of 4 officers dedicated to the compliance function commensurate with their size and volume of transactions. The December 2017 returns submitted to RBM also indicate that compliance programmes of most banks are commensurate with the level of risk, considering factors such as the volume and nature of the products provided, the client base profiles, the transaction patterns, and the cross-border nature of transactions. Three banks are still in the process of developing a comprehensive risk assessment taking into account all the core ML/TF risk categories of customers, products/services, delivery channels and geographical locations. Further to this, all banks have been advised to update their risks assessment after results of this NRA report are issued. All banks have appointed a qualified and independent AML/CFT compliance officer at a senior management level, who reports to the Board on AML/CFT compliance issues. In addition, in most banks the roles of the compliance officer outlined in the officer's job descriptions are in line with provisions of Section 27 of the FCA, 2017. However, in most banks, the compliance officers have multiple roles e.g. legal/company secretary hence AML compliance responsibilities are not allocated adequate time and the functions are not adequately executed.

On the other hand, all banks are subjected to both internal and external audits; however, the internal and/or external AML audits scope focuses on KYC/CDD issues and not the assessment of the whole compliance programme. So far only three banks have been exposed to specialised AML/CFT compliance audits.

Based on the analysis provided, the variable is rated Medium High (0.6).

### *Effectiveness of Suspicious Activity Monitoring and Reporting*

Most banks have automated systems for transaction monitoring these have helped the banks to identify suspicious transactions. However, some banks underutilise the automated systems to monitor transactions aimed at identifying every suspicious transaction and this has resulted in missing out of certain suspicious transactions. This is compounded by inadequate staff to analyze alerts generated by the systems, and low knowledge levels among front line staff despite being trained on AML/CFT issues. Furthermore, knowledge levels are low amongst front line staff issues as such these may have problems in identifying suspicious transactions.

For banks that have no automated systems, the likelihood of missing out the suspicious transactions is high. This is reflected by the number of STRs filed by such banks. This variable is therefore given the rating of Medium (0.5).

The number of STRs filed by the banks since 2011 is as follows:

*Table 10: Statistics of STRs filed by banks*

	Year (January - December)							Total
	2011	2012	2013	2014	2015	2016	2017	
No. of STRs received from banks	18	59	65	80	89	129	120	560
STRs extracted by FIA from LCTRs	17	22	0	1	0	0	0	40
No. of STRs resulting in ML investigations & prosecution	28	73	37	19	38	37	33	265
No. of STRs resulting in ML convictions	1	0	3	0	0	0	1	5

### *Level of Market Pressure*

AML standards demanded by correspondent banks have increased pressure in the sector to ensure that local banks are compliant with international AML standards. For instance, in 2015 the FATF carried out a Terrorist Financing Fact Finding Initiative (TFFFI) survey on how countries are implementing United Nations Security Council Resolutions (UNSCRs) 1267 (requiring states to freeze funds belonging to terrorist involved with the Taliban and Al-Qaeda, and 1373 (requiring states to identify their own terrorist and take actions against them). Malawi was picked as one of 26 countries with significant deficiencies and risked being designated as non-cooperative. This

attracted the interest of correspondent banks who even though Malawi succeeded in passing the FCA and the TF regulations to address the deficiency still monitor the performance of this sector.

Furthermore, there has been peer pressure created by compliance officers during their meetings held as members of Bankers Association of Malawi (BAM). Further, the FIA produces an analysis of reporting trends bi-annually and sends the results to Chief Executive Officers of the banks, this has further increased the pressure on compliance officers who do not want to be left behind or exposed for not meeting their reporting obligations.

This variable is therefore rated Medium High (0.6).

#### *Availability and Access to Beneficial Ownership Information*

The FCA has addressed the issue of beneficial ownership and banks have access to beneficial ownership information, mainly for transactions or relationships involving natural persons. While banks can easily access information held with the Registrar General, it is not currently a requirement for legal persons and arrangement to provide details of the ultimate beneficial owners to the Registrar General. In turn, this makes it difficult for banks to verify declarations on beneficial ownership on legal persons and arrangements. This variable is therefore given the rating of Medium High (0.6).

#### *Availability of Reliable Identification Infrastructure*

Section 16(1) of the FCA requires banks to identify customers or beneficial owners using verifiable official documentation. The introduction of the national identification document will help many people to have the IDs especially those that 18 years and above. The National Registration Bureau was issuing birth certificates to people below the age of 18. According to Malawi News Agency online ([manaonline.gov.mw](http://manaonline.gov.mw)) article of 30 November 2017, a total of 9,000, 514 people had registered for national identification cards in the country and most of them had collected their IDs by December 2017. However, some people were yet to receive the IDs. Currently, most customers do not have official identifications like passport and driver's licence, they instead present voter registration cards and letters from District Councils or local chiefs while pupils were using school IDs as their primary identification documents. In addition, banks were yet to update customer files with the issued National IDs. This variable is rated Medium (0.5).

#### *Availability of Independent Information Sources*

Section 16(1) of the FCA requires banks to verify customer and beneficial owner identification through reliable and independent source documents, data or information. In practice, the banks verify customer information through documentation or information from the Registrar of Companies/ Registrar General, National Registration Bureau, Department of Road Traffic, Malawi

Revenue Authority, District Commissioner, Immigration Department, Water Boards, and ESCOM. This variable is rated High (0.7).

### Assessment of Product Variables

The products offered by the banking sector in Malawi were classified for purposes of this assessment and were twelve in total as follows: Private Banking, Deposit Products - Corporate, Deposit Products - SME, Deposit Products – Retail, Credit Products - Corporate, Credit Products - SME, Credit Products – Retail, Funds Transfer – International, Funds Transfer – Domestic, Negotiable Instrument – Telegraphic Transfers, Trade Finance, and Correspondent Accounts.

The most vulnerable top 5 products/services are Trade Finance, Deposit Product SME, Funds Transfer (International), Private Banking, and Deposit Product Retail with inherent vulnerabilities ranging from Medium High to Medium.

The vulnerability of the sector’s product is presented in the table below:

Table 11: Banking products vulnerability to ML

PRODUCT/SERVICE VULNERABILITY		
	INHERENT VULNERABILITY	FINAL VULNERABILITY
1. Private Banking	0.63	0.51
2. Deposit Products – Corporate	0.56	0.47
3. Deposit Products – SMEs	0.82	0.62
4. Deposit Products – Retail	0.55	0.50
5. Credit Products – Corporate	0.47	0.44
6. Credit Products – SMEs	0.48	0.45
7. Credit Products – Retail	0.34	0.34
8. Funds Transfers – International	0.76	0.59
9. Funds Transfers – Domestic (MITAS)	0.60	0.49
10. Negotiable Instruments: Telegraphic Transfer	0.08	0.08
11. Trade Finance	0.85	0.64
12. Correspondent Accounts	0.58	0.42
<b>Average Vulnerability</b>	<b>0.56</b>	<b>0.46</b>

### Private Banking

The product had an asset size of MK14.9-billion as of December 2017, this is rated Medium Low compared to the sectoral total deposits transaction value of K2.9 trillion.

The average transaction size of the product is MK4-million and this is rated High.

The client base of the product is considered Very High risk on the basis that it is mostly accessed by high-net worth individuals, politically exposed persons, corporates and SMEs and this makes the product vulnerable to both ML and TF. Generally, there are few customers (8,776 customers against a total estimated figure of 1,663,249 customers for all banks as of December 2017) accessing this product because there are charges for transactions above various thresholds set by the banks and additional charges for accessing private banking services. The charges for private banking have resulted in few customers accessing the product/service. The individual customers for this product can either be Malawian citizens or non-Malawians resident in the country and the customers are mostly well known to the banks since they are few.

The usage of cash is High, and this involves both deposits and withdrawals; however, the amounts involved are Low. In addition, there is Medium Low level of international transactions and the product does not allow for anonymous use. There have been limited existence of ML and fraud cases relating to private banking customers since some of them engage in small and medium-scale businesses.

Apart from the general AML/CFT controls, transactions by private banking customers undergo enhanced due diligence. Banks consider these customers as high risk because of either their wealth, political (PEPs) or celebrity status.

With regard to PEPs, some banks keep their own list of PEPs to help them in setting system alerts for enhanced transaction monitoring. Banking institution's customer relationships with PEPs are approved by senior management prior to commencement. This helps to deal with customer familiarity and influence issues. This procedure is confirmed through independent checks and balances done by internal audit staff of the banks as well as targeted compliance audits carried out by compliance officers of banks. In addition, compliance with AML/CFT procedures have been embedded in performance appraisal of staff of relevant departments of most banks.

Over and above that, in monitoring dormant accounts or activation of such accounts, the banks pay close attention to account of customers accessing high risk products of which private banking is one. The banks identify the dormant accounts as well as newly opened accounts and such information is provided to FIA on quarterly basis to help them with their analyses.

While the product's vulnerability to TF is rated **Medium Low** because of the profile of the customers with some of them involved in ML, there has never been any transaction linked to TF.

Based on the factors above, this product has inherent vulnerability of 0.63 (Medium High) with final vulnerability of 0.51 (Medium).

### **Deposit Products – Corporate**

The product had an asset size of MK378.8-billion as of December 2017, this is rated Medium High compared to the sectoral total deposits transaction value of K2.9 trillion. The average transaction size of the product is MK17-million and this is rated Medium High. While corporates make cash transactions, most of the transactions are done through cheques or inter-bank electronic transfers.

The client base of the product is considered Medium risk on the basis that it is accessed by corporates. Their transactions are mostly by cheque. However, where cash deposits are made they tend to be of high volumes. The investment feature is limited. Most corporates rely on trade finance and credit for investment. Frequency of the international transactions is High as most corporates make deposits for purposes of meetings costs of both domestic and international transactions. There have been limited existence of fraud cases relating to corporates.

Apart from general AML/CFT controls, opening of bank accounts for corporate customers is approved by the senior management of Board of Directors of the bank. Corporate businesses are well established and are required by law to be audited and submit their audited financials to the Registrar of Companies as required by the Companies Act. The audited financials are accessed by the banks and the banks further demand a board resolution to open an account for a corporate business.

The product's vulnerability to TF is rated **Very Low** and there has never been any transaction being linked to TF.

This product has an inherent vulnerability of 0.56 (Medium High) with final vulnerability of 0.47 (Medium).

#### **Deposit Products – SMEs**

The product had an asset size of MK107.5-billion as of December 2017, this is rated Medium compared to the sectoral total deposits transaction value of K2.9 trillion.

The average transaction size of the product is MK2-million and this is rated Medium. SMEs are rated Very High risk because of their involvement in fraud and money laundering cases. Most businesses involved in the *cash-gate* scandal were in the SMEs category. The level of cash transactions High. Most deposits are done in form of cash and some customers withdraw huge cash amounts to make business payments which include payment for casual labour and other overheads costs.

Frequency of the international transactions is Medium High as some SMEs make deposits for purposes of imports of goods mostly from neighbouring notably South Africa. The product has a limited non-face-to-face feature.

There is existence of ML typologies on the abuse of the product/service and use of the product/service in fraud or tax evasion schemes. According to the 2016 Money Laundering Typologies Report produced by the FIA, there exists public sector fraud in which SMEs and individuals are paid cheques for goods and services not rendered. The SMEs and individuals involved usually have direct links with the perpetrators at the public office making out the payments. Bank accounts of companies and individuals are used to place illegitimate funds after which the money is then withdrawn. In some cases, some front companies are being used to create distance between the real criminal elements and the illicit proceeds.

Further to the FIA typologies report, The Baker Tilly report which presented an audit done after the *cash-gate* scandal was uncovered, revealed that there was one individual linked to at least 18

businesses which were SMEs with two of these businesses receiving a total of MK4.4-billion in 17 cheques.

Apart from the general AML/CFT controls, banks categorise the SMEs in terms of risks they pose to the bank. Most banks have alert systems to flag out suspicious transactions or listed individuals. For high risk SMEs, the banks escalate their transactions to senior management at branch level for approval and also apply enhanced due diligence. Since *cash-gate* was uncovered banks take extra care when dealing with construction companies and related high risk businesses as these played a major role in *cash-gate*. When establishing relationships with such customers, the banks request for their registration with the National Construction Industry Council (NCIC). In addition, banks monitor media articles and where such customers are allegedly connected to criminal activities the banks notify the FIA or file an STR and continue close monitoring of the customer's transactions.

Furthermore, most banks provide Cash –in – Transit services to customers as part of enhanced Know Your Customer. Bank officials visit business premises of SMEs to appreciate and understand their businesses and collect their cash for deposit at the bank.

The product's vulnerability to TF is **Low** and there has never been any transaction being linked to TF.

The product has an inherent vulnerability of 0.82 (Very High) with final vulnerability of 0.62 (Medium High).

#### **Deposit Products – Retail**

The product had an asset size of MK212.7-billion as of December 2017, this is rated Medium compared to the sectoral total deposits transaction value of K2.9 trillion. The average transaction size of the product is MK200,000 and this is rated Low. The product is accessed by individuals of varying profiles including civil servants some of whom were involved in *cash-gate*. The rating for the customers is Medium risk.

Being a cash-based economy, most individual customers transact in cash (i.e. make cash deposits and withdrawals) as such level of cash transactions is High. For some customers, they use funds for this product for investments. Frequency of the international transactions is Medium Low. Most customers for this product are low income earners and do not engage in international transactions.

In view of the above stated issues, AML/CFT controls applied on this product are general in nature. The product's vulnerability to TF is rated **Very Low** and there has never been any transaction being linked to TF.

This product has an inherent vulnerability of 0.55 (Medium High) with final vulnerability of 0.50 (Medium).

#### **Credit Products – Corporate**

The product had an asset size of MK230.3-billion as of December 2017, this is rated Medium compared to the sectoral total deposits transaction value of K2.9 trillion. The average transaction size of the product is MK70-million and this is rated High.



The client base of the product is considered Medium risk on the basis that it is accessed by corporates. There is Low cash usage due to minimal usage of cash on credits to corporates, and the product has a limited investment aspect. Frequency of the international transactions is Medium as most corporates make deposits for purposes of meetings costs of both domestic and international transactions.

Most corporates in Malawi get loans for financing of business imports and other projects. There is limited existence of fraud cases relating to corporates. A case involving fraud and ML happened in 2017 where a corporate company swindled various banks by way of obtaining loans to finance business amounting to K20,903,508,825. The suspect, a foreign national, was arrested in September 2017 by the Malawi Police Service and was charged with fraud and money laundering charges. The suspect was on the run for some months.

There are general AML/CFT controls implemented by banks and monitored by RBM and FIA in line with AML/CFT legislations.

While the product's vulnerability to TF is rated **Medium Low** because of the profile of the customers with some of them allegedly involved in fraud and ML.

The product's inherent vulnerability of 0.47 (Medium) with final vulnerability of 0.44 (Medium Low).

#### **Credit Products – SMEs**

The product had an asset size of MK45.02-billion as of December 2017, this is rated Medium compared to the sectoral total deposits transaction value of K2.9 trillion.

The average transaction size of the product is MK100-million and this is rated Medium.

Because SME involvement in fraud and ML they have been rated Very High risk. Usage of cash by SMEs is rated Medium High. The product is used by some SMEs for business investments, though this is limited. Further, frequency of international transactions is Medium as most SMEs make deposits for purposes of meetings costs of both domestic and international transactions. There have been cases of fraud and ML relating to SMEs and credit.

There are general AML/CFT controls implemented by banks and monitored by RBM and FIA in line with AML/CFT legislations.

While the product's vulnerability to TF is rated **Medium Low** because of the profile of the customers with some of them involved in ML, there has never been any transaction linked to TF.

The product's inherent vulnerability is rated 0.48 (Medium) with final vulnerability of 0.45 (Medium).

#### **Credit Products – Retail**

The product had an asset size of MK67.3-billion as of December 2017, this is rated Low compared to the sectoral total deposits transaction value of K2.9 trillion. The average transaction size of the product is MK2-million and this is rated Medium.

The product is accessed by individuals of varying profiles including civil servants some of whom were involved in the *cash-gate*. Therefore, the customers were rated Medium risk. The usage of cash is high but the amounts involved are low hence the rating given is Medium High. There is limited aspect of investment for this product. Frequency of the international transactions is Medium Low. There are limited cases of fraud and ML relating to customers of this product who aim at disguising the source of funds.

There are general AML/CFT controls implemented by banks and monitored by RBM and FIA in line with AML/CFT legislations.

The product's vulnerability to TF is **Very Low** and there has never been any transaction being linked to TF.

Based on the factors above, the product's inherent vulnerability is rated 0.34 (Low) with final vulnerability of 0.34 (Low).

### ***Funds Transfer – International***

The product had an asset size of MK199.5-billion as of December 2017, this is rated Medium compared to the sectoral total deposits transaction value of K2.9 trillion. The average transaction size of the product is MK10-million and this is rated High.

The product is accessed by Corporates, SMEs, individuals and NGOs and these were rated Very High risk. Some corporates and SMEs use this product to procure equipment, machinery or other goods for further investment.

Frequency of the international funds transfer is High. There exists cases of fraud and ML relating to customers of this product. In 2014, FIA disseminated one report to Law Enforcement on one NGO operated by foreign nationals whose origins of funds was a foreign organisation suspected to be financed by individuals one of whom was on an UN sanctions list (refer to NGO sector vulnerability). In addition, analysis by the FIA in 2017 established that transactions of total value of USD16.9 million (approximately K12-billion) were found to have been supported by fake MRA Form 12 (form used to clear imports). It was further established that twenty-two foreign-owned businesses were involved in illegal foreign exchange transactions at some banks.

In addition to General AML/CFT controls, under advance payments, customers are required to provide invoice documentation for the transfer to the bank before effecting the funds transfer. After the arrival of the imported goods, the customer provides customs documents for purposes of reconciliation with the bank on the received goods. The RBM verifies the authenticity of the importation documents.

For other imports, the MRA prepares documentation for purposes of payment of duty at the point of entry into the country (i.e. border post). Customers are required to pay duty after assessment of the goods by the MRA. Meanwhile, the country has started implementing a new system on funds transfer to link the RBM, MRA, banks and foreign exchange bureaus so that they access transactions being made timely. This system started working from July 2017. This system is known as Customs Foreign Exchange Reconciliation System (CFERS).

Furthermore, banks are required to maintain accurate originator and beneficiary information on all wire transfer transactions for easy tracking of customer transactions which may be necessary for investigation purposes. The banks verify import documents with MRA prior to effecting import payment.

The product's vulnerability to TF is **Medium High** because of the nature of the product and profile of the customers as some of them have been involved in ML and fraud.

Based on the factors above, the product's inherent vulnerability is rated 0.76 (Very High) with a final vulnerability of 0.59 (Medium High).

### ***Funds Transfer – Domestic***

The product had an asset size of MK1.5-trillion as of December 2017, this is rated High compared to the sectoral total deposits transaction value of K2.9-trillion. The average transaction size of the product is MK100-million and this is rated High.

The product is accessed by Corporates, SMEs, and individuals and NGOs and these were rated High risk. The level of investment using this product is low. Frequency of the international transactions is High. There are limited cases of fraud.

Over and above general controls, banks have additional controls in place which include verification of transfer instruction from the source, verification of signatures on transfer instruction, sending Short Message Service (SMS) alerts to account-holders for any transaction to the account.

Banks are required to maintain accurate originator and beneficiary information on all wire transfer transactions for easy tracking of customer transactions which may be necessary for investigation purposes. In addition, most banks have alert systems to flag out suspicious transactions or listed individuals.

The product's vulnerability to TF is **Very Low** and there has never been any transaction being linked to TF

Based on the factors above, the product's inherent vulnerability is rated 0.60 (Medium High) with final vulnerability of 0.49 (Medium).

### ***Negotiable Instruments - Telegraphic Transfers***

The product had an asset size of MK24.9-billion as of December 2017, this is rated Low compared to the sectoral total deposits transaction value of K2.9 trillion. The average transaction size of the product is MK130-million and this is rated Low

The product is accessed by Corporates, SMEs, and individuals and these were rated High risk. Frequency of the international transactions is Very Low, and there exist no fraud or ML typologies for this product. The product is subject to general AML/CFT controls.

The product's vulnerability to TF is **Very Low** and there has never been any transaction being linked to TF.

Based on the factors above, the product's inherent vulnerability is rated 0.08 (Close to Nothing) with final vulnerability of 0.08 (Close to Nothing).

### **Trade Finance**

The product had an asset size of MK10-billion as of December 2017, this is rated High compared to the sectoral total deposits transaction value of K2.9 trillion. The average transaction size of the product is MK344-million and this is rated High.

The product is accessed by Corporates, SMEs, and individuals and these were rated High risk. The product is used for further investment by some corporates and SMEs. There is minimal usage of cash as most trade finance transactions involve bank transfers, hence frequency of international transactions is High.

There exist some fraud or ML typologies for this product, an example of which has been explained under Credit Corporate.

Apart from general AML/CFT controls, for trade finance that involves wire transfer transactions, banks are required to have similar controls as those discussed above for wire transfer transactions as a product.

While the product's vulnerability to TF is rated **Medium Low** because of the profile of the customers with some of them involved in ML and fraud, there has never been any transaction linked to TF.

Based on the factors above, the product's inherent vulnerability is rated 0.85 (High) with final vulnerability of 0.64 (Medium High).

### **Correspondent Accounts**

The product had an asset size of MK69.5-billion as of December 2017, this is rated High compared to the sectoral total deposits transaction value of K2.9 trillion. The average transaction size of the product is MK4.7-billion and this is rated High.

The product is accessed by banks and these were rated Low risk. There is no usage of cash, and frequency of international transactions is High. There are no fraud or ML typologies for the product.

The product's vulnerability to TF is **Very Low** and there has never been any transaction being linked to TF.

Based on the factors above, the product's inherent vulnerability is rated 0.58 (Medium High) with final vulnerability of 0.42 (Medium Low).

### **Recommendations for the Sector**

The following are recommendations for the banking sector:

- a) Amendments to the FCA to address AML/CFT deficiencies identified after the law was passed
- b) Issuance of the Financial Crimes Regulations to facilitate implementation of monetary sanctions

- c) Supervisory authorities and LEAs should commence enforcement of criminal sanctions against the banking sector especially where the case is grave or there is repeated non-compliance even after meting out administrative sanctions
- d) Banks should enhance internal controls to prevent fraud.
- e) Banks should ensure that all fraud or attempted fraud perpetrated by staff is reported to RBM and FIA.
- f) Banks should conduct targeted AML /CFT training for frontline staff who interact with customers to enable them to easily identify suspicious transactions and activities.
- g) The board members of banks should be adequately trained so that they provide proper oversight role for AML/CFT programmes.
- h) Banks should enhance the frequency of training and implement measures to assess the effectiveness of the training programmes.
- i) The Ministry of Education and institutions of higher learning should be approached to consider introducing AML/CFT courses in the education system.
- j) Banks should develop and continuously update ML/TF risk assessments on all the core categories of customers, products/services, delivery channels and geographical locations.
- k) Holders of compliance functions in banks should not be required to conduct other functions.
- l) Bank's compliance functions must be adequately resourced to be able to execute all compliance responsibilities as provided for under Section 27 of the FCA.
- m) Both the internal and external audits scope of banks must be enhanced to include the assessment of the whole AML compliance programme.

## Insurance Sector Vulnerability

### Background

The insurance sector in Malawi is regulated and supervised by the Reserve Bank of Malawi. Insurance entities (insurance companies, insurance brokers, insurance agents and loss assessors / adjusters) are licensed under the Financial Services Act (FSA), No. 26 of 2010, CAP 44:05 of the Laws of Malawi. The FSA provides the relevant legal framework for the regulation and supervision of the insurance entities. The insurance industry was previously excluded as a financial institution and therefore as a reporting entity under the Money Laundering, Proceeds of Serious Crimes and Terrorist Financing Act of 2006. It was however incorporated by notice of a gazette published by the Minister of Finance, on 26<sup>th</sup> October 2012. In the same year, the sector was assessed for its ML and TF vulnerabilities and the results showed that ML/TF vulnerabilities were *Medium* for life insurance and *Low* for non-life (general) insurance. Many changes took place in the sector since 2012, including introduction of new players and products as well as more ML/TF awareness by stakeholders. The 2017 assessment of the insurance and pensions sectors looked at the various insurance and pensions products offered by market players in the sector.

The insurance sector is categorised into two sub-sectors, namely: life insurance and general insurance. Meanwhile, as at 31<sup>st</sup> December 2017, the insurance sector comprised the following entities:

- a) **Insurance companies:** There are a total of thirteen (13) insurance companies, with eight (8), dealing in general insurance business and five (5) dealing in life insurance business;
- b) **Re-insurance companies:** There is only one (1) re-insurance company in Malawi;
- c) **Insurance brokers:** There are 16 insurance brokers in the industry, one of which is a re-insurance broker. These conduct insurance businesses on behalf of the insurance companies and can represent multiple insurance companies;
- d) **Agents:** There are 33 insurance agents. However, these can only operate under one principal insurance company and the insurance company is responsible for ensuring that the agent has proper AML/CFT measures in place;
- e) **Agents for brokers:** There are 5 agents for brokers. These are banks providing bancassurance services; and
- f) **Insurance loss adjusters / assessors:** There are 15 Loss adjusters/ assessors in the insurance industry.

The total assets in the industry as at 31<sup>st</sup> December 2016 were MK371.0 billion, of which 89 percent (MK332.7 billion) belonged to the Life insurance sector. Gross total premium for both sub-sectors stood at MK55.0 billion, of which 64 percent belonged to the general insurance sector.

### Overall Vulnerability

The insurance sector's vulnerability is dependent on the strength of the AML general controls and product specific variables. The assessment looked at both life and general insurance and focused on five products, namely; motor, fire, personal accidents, endowment and group pension.

The overall ML vulnerability of the sector in Malawi was found to be Medium High (0.61). This rating took into consideration the AML general controls, which were rated Medium (0.40) as represented below. The AML general controls looked at the quality of insurance company operations (Medium low – 0.40), quality of internal AML policies and procedures (Medium – 0.59), commitment and leadership of insurance companies' management (Medium – 0.57), compliance of insurance companies staff Medium Low – 0.40), quality of CDD framework (Medium – 0.50) and quality of AML supervision (Medium – 0.60). These ratings took into consideration various variables.

### Assessment of Variables<sup>26</sup>

#### Comprehensiveness of AML Legal Framework

This variable is rated High (0.7) on the basis that the FCA, No. 14 of 2017, conforms to international standards on combating ML as it covers all areas of KYC/CDD/EDD, reliance on CDD by third parties, record keeping, suspicious transaction reporting, tipping-off and confidentiality, internal controls, foreign branches and subsidiaries, regulation and supervision of financial institutions, supervisory powers and sanctions and administrative penalties (*See FCA sections 16 to 34*). The existing subsidiary legislation (regulations) was based on the repealed Money Laundering, Proceeds of Serious Crimes and Terrorist Financing Act. Even though these regulations are still applicable, they were drafted in 2011 and few of the issues covered in the FCA are not taken into account, such as

---

<sup>26</sup> See Insurance sector analysis of variables report for detailed information

administrative sanctions and beneficial ownership, among others. The Financial Crimes Regulations are expected to be concluded by March 2018.

### *Effectiveness of Supervision Procedures and Practices*

Between 2013 and January 2017, the RBM was the direct supervisor of the insurance sector on AML issues. The introduction of the FCA changed this as it mandates the FIA to be the supreme authority regarding AML matters. The FCA further gives powers to the FIA to delegate AML supervision to other supervisory authorities or self-regulatory bodies (*See FCA s35 to 38*). While previously both RBM and FIA were conducting either separate or joint supervisions, the two are now in the process of coming up with a MoU and delegation instrument on supervision. The MoU and delegation instruments are expected to be concluded by March 2018.

Both FIA and RBM carry out their supervisory activities within a comprehensive supervisory framework which includes clear supervision policies, procedures and manuals. Both RBM and FIA have to some extent supervised the insurance sector using a risk-based approach. However, while the FIA has conducted some desk reviews on the sector, it has not fully utilised its findings to implement a proper risk-based approach to its supervision as the previous law did not focus a risk-based approach. RBM on the other hand took into consideration the findings of the 2015 NRA report and focused its supervision on the life insurance providers as these were rated as posing a higher risk. RBM has therefore conducted on-sites at all the life insurance companies, some of these jointly with FIA. FIA has also conducted on-site examinations at all the general insurance companies. FIA and RBM statistics show that between 2015 and 2017, on-site inspections were conducted at 11 of the 13 insurance companies (84.6 percent), the Re-insurance company and 1 out of the 16 insurance brokers (6.25 percent). FIA also conducts desk reviews and has helped the insurance companies in compiling AML/CFT policies and procedures and generally setting up of the compliance functions.

Both FIA and RBM have well trained staff. While RBM has sufficient staff, FIA has experienced staff shortages, which has impacted on the supervision. The number of reporting entities requiring supervision is many, therefore requiring adequate staff to competently and adequately supervise them.

Based on the above, the effectiveness of supervision procedures and practices is rated Medium High (0.6).

### *Availability and Enforcement of Administrative Sanctions*

This variable is rated Medium Low (0.4). on the basis that the repealed ML Act did not provide for administrative sanctions and the RBM does not have administrative sanctions for the sector on AML issues or AML related issues.

While the FCA has provided for administrative sanctions, these are currently in draft form and are yet to be issued and tested. The administrative sanctions include provisions for warnings, monetary penalties and recommendations for closure of business. Both FIA and RBM are working together in finalizing these as stated above.

### *Availability and Enforcement of Criminal Sanctions*

Criminal sanctions are provided both under the FCA and the repealed ML Act. However, there have been no ML criminal cases in the sector yet. There have been several fraud cases in the sector, with many institutions opting to take administrative actions and not criminal actions<sup>27</sup> against the involved persons. On this basis, the rating for this variable is Medium (0.5).

### *Availability and Effectiveness of Entry Controls*

The Insurance Act and subsidiary legislation (licensing guidelines and directives) provide for the entry requirements for those interested in investing in the insurance sector. Despite such entry requirements not being specifically aligned to the FCA, they address some of the AML/CFT issues such as requiring fit and proper testing for directors and senior management to prevent criminals or their associates from being licensed, vetting and appropriate educational and professional qualifications for key directors and senior management. RBM further conducts intensive screening / conducts due diligence on the new entrants and their seed capital even though this is not reflected in the licensing guidelines for the insurance sector. For instance, between 2013 and 2014, RBM conducted CDD on a potential investor for Charter Insurance Company Limited by engaging the FIA (then FIU). Like in the case of the banking sector, RBM screens seed capital/ source of funds to determine that the funds being invested are legitimate. In the case of foreign investors which are corporates, meetings are held with their bankers, auditors as well as the FIU (of the country where the company is registered) aimed at collecting information including details of the shareholders, their financial statements and source of funds. For regulated investors, meetings are held with their home country supervisor. The FCA (S.27 (3)(a)) also compliments this by specifying key requirements for staff holding compliance officers' positions.

There are also requirements to demonstrate the source of funds for the paid-up capitals of insurance (typically in the form of audited financial statements from banks where the funds are held). The information which is gathered is not systematically subject to verification.

On the basis of the above information, this variable is rated Medium High (0.6).

### *Integrity of Staff in Insurance Companies*

This variable is rated Medium Low (0.4). on the basis that insurance entities are required to screen or vet their staff by checking with past employers and conducting police checks. However, this is usually done during recruitment and not as an ongoing activity. As a result, during the course of their employment, some employees have engaged in criminal activities. Furthermore, when such activities are detected, the employers sometimes opt to deal with the matter quietly by taking internal disciplinary action such as dismissal. For instance, between 2013 and 2017 there were 15 cases involving fraud and other malpractices in the insurance sector. Information gathered from LIPAM, IAM and IBAM during the assessment revealed that 6 of the 15 cases (40%) involved insurance staff. Of the 6 cases involving the staff, 3 were dealt with internally and 3 were taken to court.

---

<sup>27</sup> Summary of fraud cases in the insurance sector as compiled by LIPAM, IAM and IBAM for the period 2013 to 2017



### *AML Knowledge of Staff in Insurance Sector*

The AML knowledge of insurance staff is rated Medium Low (0.4). It is a requirement under the law for insurance entities to train their staff in AML/CFT issues. However, only a few entities have complied. Most insurance staff are therefore found not to have adequate AML/CFT knowledge. Statistics show that between 2013 and 2017, the FIA and RBM trained compliance officers of all 30 insurance entities, that is, excluding the Agents. Both the FCA and repealed ML law clearly place(d) the responsibility of training Agents on the insurance companies. Only 6 out of the 13 (46 percent) insurance companies and one out of 16 (6 percent) insurance brokers have provided AML/CFT training to their staff. 75 percent of the Insurance business is through insurance brokers and yet only 6 percent of the brokers have received AML/CFT training.

Verification of training documents during on-site examinations showed that staff working in insurance companies were more knowledgeable about AML issues than insurance brokers. In addition, insurance companies had adequate training programmes in place.

### *Effectiveness of Compliance Function (Organisation)*

This variable is rated Medium Low (0.4). The insurance entities generally do not have robust compliance functions, particularly insurance brokers. While about 70 percent of the insurance companies have appropriate AML policies and procedures in place and an active AML function, only 6 percent of the brokers have done the same. The insurance companies generally have more dedicated and knowledgeable staff and adequate resources than the Brokers. However, in most cases, the compliance officers do not hold senior positions and as such may not be involved in decision making processes concerning the compliance function.

The insurance brokers generally do not have adequate resources for the compliance function as seen by their low attendance during compliance officers' meetings that have been organised by the FIA. This is also reflected in the number of threshold and suspicious transactions reported from the sector to the FIA.

There has been no disciplinary action on any compliance staff by either the insurance companies or Brokers and most have not conducted audits of the compliance functions.

### *Effectiveness of Suspicious Activity Monitoring and Reporting*

This variable is rated Low (0.3). The FIA installed the encryption software at all the insurance entities, however, despite 73 percent of the insurance entities submitting threshold reports (Large currency transaction reports) to the FIA, between 2013 and November 2017, the FIA received less than 5 STRs from the insurance sector in the same period.

Transactions in the sector are mostly monitored manually, making it difficult for suspicious criminal activity to be detected. Most entities do not have mechanism in place to identify or conduct PEP screening. In addition, most of the staff are lacking in AML knowledge and therefore unable to detect suspicious activity.

### *Level of Market Pressure to meet AML Standards*

Most insurance institutions with international ties (about 10% of the sector) or seeking international ties were seen to have high AML/CFT standards and understood the need to have robust AML/CFT functions. However, those without international ties (about 70% of the sector) were seen to be less proactive. On this basis, the rating has been Medium Low (0.4).

### *Availability and Access to Beneficial Ownership Information*

The rating for this aspect is Medium (0.5) on the basis that the FCA has addressed the issue of beneficial ownership. However, this is a fairly new concept for the insurance sector more so that many are not aware or have not been adequately equipped of their AML/CFT obligations such as identification of clients or conducting proper KYC/CDD/ECDD.

### *Availability of Reliable Identification Infrastructure*

Malawi currently does not have a reliable national identification system as the system is currently being put in place and has not been fully implemented. While the passport and drivers' license are used as official identification documentations, they have been prone to abuse and forgery.

Furthermore, although there are institutions that can provide verification channels, such as the Registrar of Companies or Department of Immigration the services are not easily accessible and there are fees attached to these services which deter institutions from using them. Based on the above, the rating is Medium (0.5).

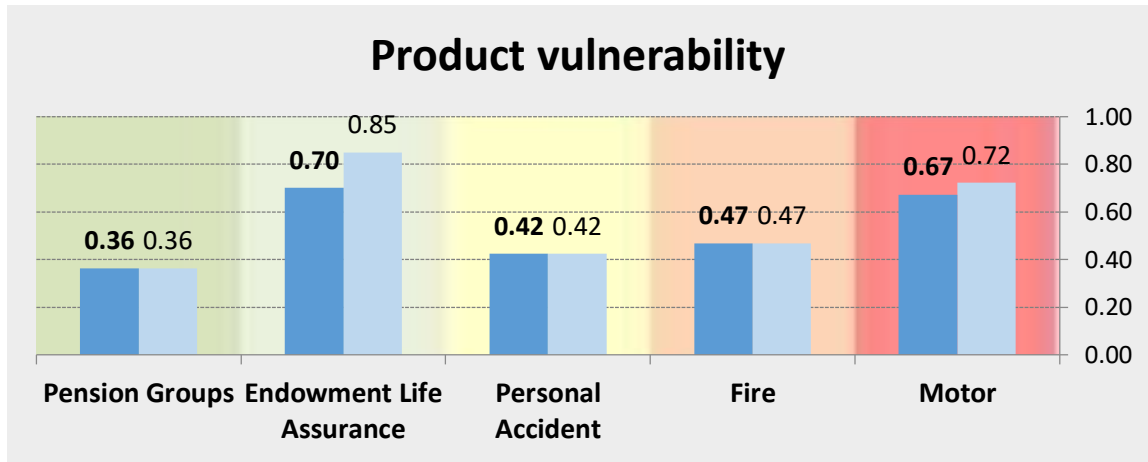
### *Availability of Independent Information Sources*

The availability of Credit Bureau provides channels for independent information on financial information. However, such services attract certain fees which deter institutions from using them. In addition, this Credit Bureau is fairly new and therefore may not have adequate information. This variable is rated Medium High (0.6).

### *Product-Specific Input*

The assessment focused on five (5) products; motor, fire, personal accidents, endowment and group pension. The analysis revealed that Endowment products were the riskiest while group pension products were the least risky products. The results are represented by the graph below, with the following ratings; Endowment - Medium High (0.70), Motor - Medium High (0.67), Fire - Medium (0.47), Personal accident - Medium (0.42) and Group Pension – Medium Low (0.36). Further, the analysis revealed that all the products for the insurance sector posed Low TF threat and that none of them was linked to TF issues.

Figure 2: Insurance products vulnerability to ML



**Key:**

- Final product/service vulnerability
- Inherent product/service vulnerability

The table below is a summary of the assessment:

Table 12: Insurance products ML assessment

	Motor	Fire	Personal accident	Endowment Life Assurance	Pension groups
Total Value/size	High – 21.5 billion	Low – 6.2 billion	High – 4.0 billion	High	High
Use of agents	Very High	Medium	High	High	Low
Client base profile	Very High risk	High risk	Low risk	High risk	Medium risk
Investment type policy	Not available	Not available	Not available	Available	Available but limited
Level of cash activity	High	High	Medium Low	Medium	Low
Cross border use	Does not exist	Does not exist	Does not exist	Medium high	Does not exist
Possible anonymous use of the product	Available	Not available	Not available	Not available	Not available
Use of product in fraud/tax evasion schemes	Exists and significant	Exists and significant	Exists and significant	Exists	Exists but limited
Existence of ML typology on abuse of the product	Does not exist	Does not exist	Does not exist	Does not exist	Does not exist

<i>Difficulty in tracing the transaction records of the product</i>	Easy to trace	Easy to trace	Easy to trace	Easy to trace	Easy to trace
<i>Non-face-to-face use of the product</i>	Not Available	Not Available	Available but limited	Available and prominent	Available but minimal
<i>Other – Fraudulent activities by insurance staff</i>	Medium	Does not exist	Medium Low	Low	Low
<i>Availability of product Specific AML controls</i>	Only General AML controls	Only General AML controls	Only General AML controls	Available and comprehensive	Available and comprehensive

**Endowment**

This variable is rated Medium High (0.70). Endowment products are life insurance policies that pay the assured sum (face amount) on a fixed date or upon death of the insured, whichever comes earlier. These policies carry premiums higher than those on conventional whole life policies and term insurance, and are useful in meeting special lump sum needs such as buying a home<sup>28</sup>.

Total assets and volume turnover for the Life insurance products are lumped as one. As such, it was difficult to isolate those for Endowment. As at 31<sup>st</sup>December 2016, the assets for all life insurance products were at K332.7 billion and the profits after tax were at K9.2 billion. This is rated as being High compared to other products offered by the sector.

The business set up of this product is that it is sold through tied agents i.e. agents working for life insurance companies on commission basis. Most of the insurance companies do not train their agents in AML issues and therefore, many of them are not equipped to conduct adequate CDD measures.

The product is rated as being used by high risk customers in that it is used by people with disposable income and therefore high net-worth individuals and some of these include PEPs. Since most entities have not categorised their customers according to the risks they pose and do not have systems in place to identify PEPs, the product could be used by people with connections in high risk jurisdictions, clients with criminal records and all sorts of business entities.

The product structure allows for investment of money into the financial system. Further, a customer is allowed to access a loan with the policy as collateral.

<sup>28</sup> Business dictionary – <https://www.businessdictionary.com>

There is Medium usage of cash in this product. Most premiums are paid through standing orders with pay-outs being mostly through cheques or bank transfers. There are no third-party payments in this product.

The product cannot be used anonymously, however, it can be accessed by customers based in other jurisdictions, with the beneficiaries based in Malawi thereby allowing for cross-border use of the product. The product has been used in fraud / tax evasion schemes, for example, there have been fake deaths reported of insured persons and there have been exaggerated amounts on the issued sums. In one case, a teacher in Thyolo wanted to claim on his Family Funeral Insurance Policy by falsely indicating that his child, who was covered by the policy, had died. Investigations revealed this was false and the policy was cancelled.

Despite there being no ML typologies from Malawi, there are typologies from other countries which could also be applicable in Malawi as per the examples below.

#### **Typology 1:**

**offence:** Money Laundering, Tax evasion    **Insurance related offence:** N/A

**Jurisdiction:** Poland    **Subject:** Individual and Legal Person

**Instruments methods and techniques:** Life insurance policy

**Indicators:** Small initial deposit followed by large deposit by third party legal person; Additional payments from company in geographically different location; Policy cancelled with full reimbursement of contributions shortly after inception; Reimbursement paid to third parties all, natural persons.

**Case description:** Mrs. T (teacher) from the South of Poland, entered into a life insurance policy with a small initial premium being paid. The transaction was arranged by Mr. B who was the agent of insurance company C and a cousin of Mrs. T. Two days later, Company C from the North of Poland made a payment of an additional premium, in excess of 2.1m PLN (€540,000), on behalf of Mrs. T. After one month, Mrs. T cancelled her policy and transferred the refund of contributions to three different accounts: - Mr. MD (Managing Director of Company C) –950,000 PLN (€240,000); - Mrs. N (niece of Mr. MD) –600,000 PLN (€150,000); and - Mr. U 600,000 PLN (€150,000). All of them subsequently transferred the money onwards to other accounts in different banks. Investigations revealed that the money being laundered was linked to fuel smuggling. The accounts were blocked by the FIU and the case was forwarded to the public prosecutor<sup>29</sup>.

#### **Typology 2:**

**Jurisdiction:** Bulgaria                      **Subject:** Individual and Legal Person

**Instruments methods and techniques:** Pension/savings

**Indicators:** Large deposit by third party; Prompt withdrawal by policyholder

---

<sup>29</sup>Moneyval. "Typology Research", 2010

**Case description:** A single premium on a life policy, totalling more than €500,000 was paid on behalf of Mr. A by Mr. A's employer, who was a related person. Half of the amount was withdrawn by Mr. A within a month of paying the premium. A request for withdrawing the balance of the amount was filed at the same time. Subsequent action Following a report to the FIU subsequent checks revealed that Mr. A had a criminal record and was involved in pending legal proceedings. It also appeared that Mr. A was allegedly involved in drug dealing and assassinations. Following further investigation and collection of information, including tax records, CTRs, and movements of funds on Mr. A's accounts the relevant information was forwarded to law enforcement agencies<sup>30</sup>.

Tracing of transactions involving this product is easy as it involves future benefits and therefore insurers make sure that records are available. The product does not require complex record keeping so they are fairly easy to trace. The RBM also requires all entities to keep customer files and records on all pay-in and pay-outs

The product allows for non-face-to-face use and this is prominent. Malawians in the diaspora or foreigners based outside the country can acquire the policy for beneficiaries without the insurance company having face-to-face interactions with them. This can be done using brokers or via emails or using the internet to complete forms available on the insurance company's website.

There have been cases involving insurance staff engaging in fraudulent activities. For instance,

- i) In 2014, a MK13.7 million claimed cheque for death benefits was deposited with fraudulent payees.
- ii) In 2015, An employee credited his/her account with lump sum contributions amounting to MK1.7 million.
- iii) In 2016, an employee re-activated an annuitant's account which was dormant for two years and created a fictitious annuitants account using the same initials and surname, but different bank account and continued to receive the annuities, amounting to MK0.8 million, for the next four years.

The FCA has provided for specific AML controls for this product. Section 18 specifically alludes to products related to life insurance and the need for identification and verification of beneficiaries.

### **Motor**

This variable is rated Medium High (0.67). Annual turnover statistics for this product as at 31<sup>st</sup> December 2016 were K25.5 billion (in gross premium earned), of which K19.0 billion were Motor products representing 74.3 percent of the industry.

There is very high use of insurance brokers and insurance agents in Motor products as they are mostly sold through intermediaries i.e. Agents and Insurance Brokers. The product is used by very high-risk customers since it is mandatory that every motor vehicle driving on the roads of Malawi should be insured. The client base for this product therefore includes high risk individuals, PEPs,

---

<sup>30</sup>Moneyval. "Research typologies", 2010

regular individuals and entities from or with connections in high risk jurisdictions, high net-worth individuals, clients with criminal records and all sorts of business entities.

There are no investment type policies linked to this product. However, most premiums are paid through cash but claim pay-outs are through cheques or bank transfers. There are no third-party payments in this product. Further, there is no cross-border use of the product.

There is a possibility of anonymous use of this product as one can insure a vehicle on behalf of someone. For example, one company may pay premiums on behalf of another company and the insurer may not know the owners of the company i.e. the ultimate beneficiary may not be adequately identified and proper CDD measures may not be applied.

There have been instances of fraud involving the product. For instance, there are cases whereby Insurance staff have received premiums and issued fake receipts (by having forged receipt books), thereby defrauding the insurance entity. In other cases, customers have staged accidents so that they get paid through claims and staff have colluded with customers to inflate the values of vehicles so that they get high compensation.

Although there are no ML typologies for Malawi, typologies from other countries exist and are very significant. For example:

**Typology 1:**

**Offence:** Suspected terrorist financing.      **Insurance related offence:** N/A

**Jurisdiction:** United Kingdom.      **Subject:** Natural person

**Instruments methods and techniques:** Cancellation of motor insurance policies

**Indicators:** Early cancellation of policy; Prompt closure of account from which premium paid; Request for cheque rather than wire transfer to originating account; Cheque presented to “cash converter”

**Case description:** In October a motor insurance policy was purchased by Mr. X to cover a Nissan Micra. The premium was £772 based on 4 years no claims bonus. The premium was paid by way of debit/credit card via the internet. Mr. X cancelled cover on the 5th November and asked for the refund of premium to be paid by personal cheque as he had lost the relevant debit/credit card. On 3rd December Mr. X contacted the insurer’s call centre and took out cover on a different vehicle, a Vauxhall Corsa. This time he attempted to pay via a debit/credit card and initially the transaction was declined. The premium was paid in full by debit card the following day. Mr. X now claimed that he had no claims bonus and bought every possible “added on” product and subsequently the premium was £3,483. Once again Mr. X requested that this policy be cancelled. He requested that the refund of premium should not be paid via the original debit card as that particular bank account had been closed. Consequently, he asked for a personal cheque to be sent to him. This was refused with the insurer insisting that the refund should be paid via the original debit card. The insurer has subsequently established that the first refunded cheque

was presented to cash converters. The series of transactions was reported to the FIU. Subsequent investigations indicated that the individual concerned appeared to be linked to a terrorist network<sup>31</sup>.

**Typology 2:**

**Offence:** Money laundering.      **Insurance related offence:** N/A.      **Jurisdiction:** Bulgaria

**Subject:** Legal Person.      **Instruments methods and techniques:** Motor insurance

**Indicators:** False or inconsistent declarations; Refusal to provide information on source of funds

**Case description:** Numerous motor vehicles owned by a number of companies were insured. As part of the process for setting up the insurance policies various company documents were reviewed by the insurer. The companies had been incorporated during 1994-1995 when Mr. X was 24 years old. The registered business activities of the companies set out significant investments that did not correspond to the age and status of Mr. X. The companies appeared to be linked to other persons related to the Mr. X and were incorporated with the same address. Subsequently Mr. X refused to provide information on the origin of the funds used to acquire the motor vehicles<sup>32</sup>.

Transaction records can easily be traced as the product involves future benefits and therefore insurers make sure that records are available. The product does not require complex record keeping and the RBM also requires all entities to keep customer files and records on all pay-in and pay-outs.

There is no non-face-to-face use of the product and there are no specific AML controls for this product

**Fire**

This variable is rated Medium High (0.47). The annual turnover for the product is low compared to other products in the sector. The annual turnover statistics for products in the sector as at 31<sup>st</sup> December 2016 were K25.5 billion, with Fire products registering K2.3 billion in gross premiums earned, representing 9.0 percent.

There is medium use of agents in this product, as this only happens when a bank acts as an agent. This happens when individuals or entities obtain loans, the bank or lending institution would ensure that the fire insurance premiums are paid on time. There are currently 9 banks in Malawi, therefore limited use of such agents.

. The product is quite expensive and utilised mostly by an elite group of customers who are mainly high net-worth individuals, PEPs and high-risk individuals and entities/individuals with high risk jurisdiction links, this poses a high risk. The fact that most entities have not conducted ML risk assessments and have not categorised their customers according to the risks they pose and that

---

<sup>31</sup>Moneyval. "Research Typologies", 2010

<sup>32</sup>Moneyval. "Research Typologies", 2010



most entities do not have systems in place to identify PEPs and therefore hardly apply enhanced due diligence measures, increases the risks.

There are no investment type policies linked to this product and there is high usage of cash in this product as some premiums are paid through cash. However, pay-outs are through cheques or bank transfers. There are no third-party payments in this product.

There is no cross-border use of this product and there is no non-face-to-face use. The product has been used for fraud in that there are cases whereby customers have committed arson so that they get paid through claims. However, there have been no known cases of insurance staff being involved in fraudulent activities using this product. Even though there are no ML typologies for Malawi, typologies from other countries exist and are very significant. For example:

**FATF Typology:**

Clients in several countries used the services of an intermediary to purchase insurance policies. Identification was taken from the client by way of an ID card, but these details were unable to be clarified by the providing institution locally, which was reliant on the intermediary doing due diligence checks. The policy was put in place and the relevant payments were made by the intermediary to the local institution. Then, after a couple of months had elapsed, the institution would receive notification from the client stating that there was now a change in circumstances, and they would have to close the policy suffering the losses but coming away with a clean cheque from the institution. On other occasions the policy would be left to run for a couple of years before being closed with the request that the payment be made to a third party. This was often paid with the receiving institution, if local, not querying the payment as it had come from another reputable local institution<sup>33</sup>.

Transaction records are easy to trace as the product involves future benefits and therefore insurers make sure that records are available. The product does not require complex record keeping so they are fairly easy to trace. The RBM also requires all entities to keep customer files and records on all pay-in and pay-outs.

The product cannot be used without face-to-face interactions and there are no specific AML controls for this product

***Personal Accident***

This variable is rated Medium High (0.42). Annual turnover statistics for products in the sector as at 31<sup>st</sup> December 2016 were K25.5 billion, of which K2.0 billion were personal accident products, representing 7.8 percent of the turnover

There is high use of agents and insurance brokers for this product. The client base consists of low risk customers as the product is used mostly by entities, for their employees. This can include PEPs and high net worth customers however; the source of funds is known.

---

<sup>33</sup>FATF Report on Money Laundering and Terrorist Financing Typologies, 2003 – 2004

There are no investment type policies linked to this product and the use of cash is medium low. Cash is not often used for this product as the customers are entities that are covering their employees and therefore choose to use traceable methods such as cheques and wire transfers. Pay-outs are also through cheques or bank transfers. There may be third-party payments as payments may be made to the victim's beneficiaries in the case of death.

There is no cross-border use of this product and there are no possibilities for anonymous use. The product has been used in fraud and tax evasion schemes as there have been cases whereby lawyers, police and medical personnel have connived to claim compensation on this product or they exaggerate the nature of injuries so as to claim higher pay-outs. In other cases, employers have used "ghost workers" to claim on this product. Money laundering typologies are not available in Malawi however; they do exist in other countries. For example:

**IAIS Typology:**

An individual purchased an expensive new car. The individual obtains a loan to pay for the vehicle. At the time of purchase, the buyer also enters into a medical insurance policy that will cover the loan payments if he were to suffer a medical disability that would prevent repayment. A month or two later, the individual is purportedly involved in an "accident" with the vehicle, and an injury (as included in the insurance policy) is reported. A doctor, working in collusion with the individual, confirms injury. The insurance company then honours the claim on the policy by paying off the loan on the vehicle. Thereafter, the organisation running the operation sells the motor vehicle and pockets the profit from its sale. In one instance, an insurance company suffered losses in excess of \$2 million from similar fraud schemes carried out by terrorist groups<sup>34</sup>.

There are specific cases that were reported to the Insurance Associations involving staff engaging in fraudulent activities. For instance, in 2017, an employee was reviving policies, which had lapsed or had been paid up and was raising fictitious receipts in the system, which resulted in incorrect payments, being made. He was also making changes to the bank account details for policyholders resulting in the proceeds going to his/her accomplices' bank accounts. This case involved MK40 million.

Transaction records are easy to trace in that the product involves future benefits and therefore insurers make sure that records are available. The product does not require complex record keeping so they are fairly easy to trace. The RBM also requires all entities to keep customer files and records on all pay-in and pay-outs for a minimum period of 7 years, as per government requirement, which is also in line with the FCA.

There is limited non-face-to-face use of the product as legal entities obtain cover for their employees hence the insurers have direct contact with the employer and not the employee, except when there is a pay-out. There are no specific AML controls for this product.

---

<sup>34</sup> IAIS – Examples of money laundering and suspicious transactions involving insurance, 2004

### Group Pension

This variable is rated Medium Low (0.36). The asset size of the product as at 31<sup>st</sup> December 2016 was at K380.8 billion. The sector does not provide detailed statistics, apart from the assets of the pension funds and pension contributions.

There is low use of agents in this product as its nature requires a lot of bureaucracy and paperwork. Insurance entities therefore interface with their clients directly. Were agents are used, it is tied agents that would be used in many instances as opposed to the brokers.

The client base for this product is considered medium risk as the clients are mainly well-known entities. The product is used mostly by companies and since the insurance entities deal with these directly, then CDD measures are conducted comprehensively.

The product offers investment opportunities; however, these are limited. The pension funds are heavily invested and the returns thereof are apportioned to individual members' accounts. There is low usage of cash in this product as the users are mostly companies / entities and many choose to pay using company cheques or electronic transfers. Pay-outs are also done through cheques or bank transfers. In addition, there are no third-party payments in this product. There is no cross-border use of the product and it does not allow for anonymous use.

There have been few instances of fraud involving the product. These have involved fake death claims and ghost workers. In one known case an employee credited his/her account with lump sum contributions amounting to MK1.7 million, some of this money included pensions group contributions.

Money laundering typologies from other countries include the following cases:

#### Typology 1:

**Offence:** Insurance fraud/money laundering

**Insurance related offence:** Insurance claims fraud

**Jurisdiction:** Moldova

**Subject:** Individual/Legal Person Money laundering through private pension funds and the insurance sector – October 2010 46

**Instruments methods and techniques:** Health and personal injury

**Insurance Indicators:** Dummy persons; Premium rate that did not equate to the underlying risk; False claims supported by false documents; Abnormal internal practices (accelerated claims payments)

**Case description:** An insurer in collusion with an insured person attempted to launder money through insurance transactions. The manager of an insurance company sold health and personal injury insurance policies insuring against the liability from accidents to dummy persons, normally in the names of friends and relatives. These persons paid a low premium rate. Subsequently claims were received, supported by false documentation and medical certificates to substantiate the losses and the insurer paid the claims promptly. The claims for damages were considerable. The manager then sought to legalise this scheme and recover the damages paid out. Under subrogation rights, the insurance company took legal action against all businesses where the alleged accidents had occurred. The businesses involved (restaurants,

clubs etc.) responded that they had not been aware of the alleged accidents and that no such accidents had occurred at the times stated. Subsequent action Details were subsequently passed to law enforcement agencies. It was also considered that the scheme could have been designed to avoid payment of taxation<sup>35</sup>.

#### **Typology 2:**

**Offence:** Money laundering

**Insurance related offence:** N/A

**Jurisdiction:** Bulgaria

**Subject:** Individual and Legal Person

**Instruments methods and techniques:** Pension/savings

**Indicators:** Large deposit by third party; Prompt withdrawal by policyholder

**Case description:** A single premium on a life policy, totalling more than €500,000 was paid on behalf of Mr. A by Mr. A's employer, who was a related person. Half of the amount was withdrawn by Mr. A within a month of paying the premium. A request for withdrawing the balance of the amount was filed at the same time. Subsequent action Following a report to the FIU subsequent checks revealed that Mr. A had a criminal record and was involved in pending legal proceedings. It also appeared that Mr. A was allegedly involved in drug dealing and assassinations. Following further investigation and collection of information, including tax records, CTRs, and movements of funds on Mr. A's accounts the relevant information was forwarded to law enforcement agencies.

Tracing of transaction records is easy as the product involves future benefits and therefore insurers make sure that records are available. The product does not require complex record keeping so they are fairly easy to trace. The RBM also requires all entities to keep customer files and records on all pay-in and pay-outs

There is limited non-face-to-face use of the product as it is used by companies on behalf of their staff. The insurer therefore interfaces with the company more than the beneficiaries

Apart from the general AML controls, the FCA has provided for special controls in that section 18 specifically addresses AML measures regarding life insurance products and the need to identify beneficiaries.

#### **Deficiencies / Gaps Identified and Proposed Actions to Rectify the Issues**

The insurance sector is rated as posing a Medium High risk to ML and TF. While the previous assessment (*refer NRA of 2013*) revealed life insurance as posing Medium risk and general insurance as posing Low risk, this assessment has established that both general and life insurance have products that pose Medium High risks i.e. Endowment and Motor. The supervisors therefore need to look at both life and general insurance and to fully adopt and implement a risk-based approach to their supervision. As identified, there is need to increase the AML knowledge of staff in the sector so that they are aware of their roles and obligations in combating ML/TF in the sector. The increase in AML knowledge will assist in ensuring that entities have effective compliance functions.

---

<sup>35</sup>Moneyval – Insurance typologies 2010

It is also essential that the FIA and RBM finalise their MoU and the Financial Crimes Regulations so that the supervisory roles are clear and that administrative sanctions are available and enforced. The enforcement of administrative sanctions should help compel entities to fulfil their obligations particularly suspicious activity monitoring and reporting. The lack of enforceable sanctions has contributed to the laxity in the sector.

The areas of focus to address the identified deficiencies as per the analysis of the insurance sector are represented in the following table:

*Table 13: Prioritisation of general AML controls for insurance sector*

PRIORITY RANKING - LAST CASE/SCENARIO	PRIORITY RANKING**
Comprehensiveness of AML Legal Framework	
Effectiveness of Supervision Procedures and Practices	
Availability and Enforcement of Administrative Sanctions	2
Availability and Enforcement of Criminal Sanctions	7
Availability and Effectiveness of Entry Controls	
Integrity of Staff in Insurance Companies	6
AML Knowledge of Staff in Insurance Companies	1
Effectiveness of Compliance Function (Organisation)	2
Effectiveness of Suspicious Activity Monitoring and Reporting	4
Level of Market Pressure to Meet AML Standards	5
Availability and Access to Beneficial Ownership Information	9
Availability of Reliable Identification Infrastructure	7
Availability of Independent Information Sources	10

## Securities Sector Vulnerability

### Background

The securities sector in Malawi is regulated by the Registrar of Financial Institutions. The sector has 23 players: stock exchange (1), portfolio managers (5), investment advisors (7), stock brokers (3), collective investment schemes (2) and transfer secretaries (5).

The stock market had a capitalisation of K956.7-billion with 698.9 million shares traded in 2017 at a turnover of K13.5-billion. Total funds under management by portfolio managers amounted to K827.3-billion<sup>36</sup> while stock brokers had K1,458.5-million and collective investment schemes were

<sup>36</sup> Life insurance funds account for 55% of the funds while pension funds account for 23% of the funds

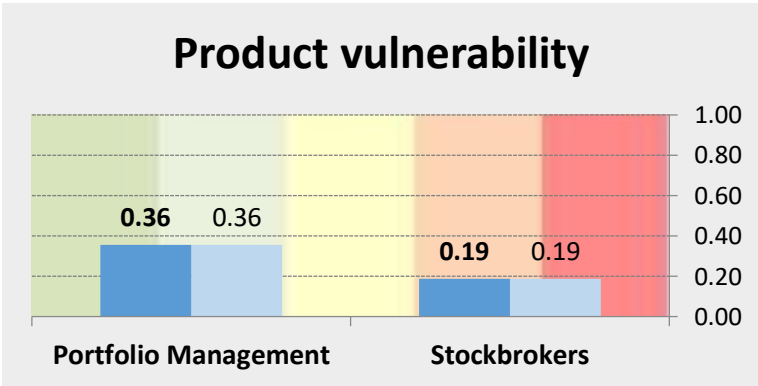
at K7, 263.1-million as at 31<sup>st</sup> December 2017. Transactions in the securities sector are done through cheques and bank transfers and are in the local currency.

The most common types of transactions in the securities sector are: equity issuance by companies and secondary trading on the stock exchange, rights issues on a stock market, debt issuance by government, investment management and collective investments. Investment management is the professional asset management of various securities (shares, bonds and other securities) and other assets (e.g., real estate) to meet specified investment goals for the benefit of the investors. A collective investment scheme (CIS) is an investment product that allows many different investors to pool their money into a portfolio comprising stocks, bonds or property.

**Overall ML Risk Assessment**

The securities sector’s overall ML risk level is rated Medium Low with an overall score of 0.33. Product specific variables were not considered in the analysis as the securities sector in the country predominantly consists of equity products. Therefore, the analysis focused on portfolio management and stockbrokerage firms trading on behalf of two different investor types; institutional investors and retail investors. However, considering the quality of AML controls existing in the two securities institution types<sup>37</sup>, Portfolio Management is assessed as being riskier with final and inherent vulnerability scores of 0.36 while those of Stock brokerage are 0.19.

*Figure 3: Securities product vulnerability to ML*



**Key:**

Final product/service vulnerability

Inherent product/service vulnerability

<sup>37</sup> Portfolio management and stock brokerage firms

## Sub-Sectors Assessment

### *Stock Brokerage Vulnerability Assessment*

#### a. **Comprehensiveness of AML Legal Framework**

The FCA has comprehensively covered AML/CFT issues by addressing KYC/CDD/EDD, reliance on CDD by third parties, record keeping, suspicious transaction reporting, tipping-off and confidentiality, internal controls, foreign branches and subsidiaries, regulation and supervision of financial institutions, supervisory powers and sanctions and administrative penalties. Money Laundering regulations are in place, but need to be revised to incorporate the changes in the FCA.

This variable is rated High (0.7).

#### b. **Effectiveness of Supervision Procedures and Practices**

As part of ongoing supervision process the RBM and FIA conducted regular AML/CFT onsite inspections of stock brokers. To date, RBM conducted 3 AML onsite inspections at 3 stockbrokerage firms between 2015 and 2017). The inspections also included AML/CFT issues such as risk-based approach and ML/TF Risk Assessment, AML/CFT Compliance Program, Internal/External Audit, Customer Identification Program, Customer Due Diligence and Suspicious Transaction Reporting. Reports were shared with the FIA. However, although the FIA and RBM have experienced, qualified personnel and relatively enough financial resources for inspections, the staff compliment needs to be increased to ensure wider coverage of the sector.

This variable is rated Medium (0.5).

#### c. **Availability and Enforcement of Administrative Sanctions**

The previous ML law had no provisions for Administrative sanctions. However, these have been provided for by the FCA and are yet to be implemented. Regulations governing enforcement of these sanctions are yet to be drafted and approved.

This variable is rated Medium (0.5).

#### d. **Availability and Enforcement of Criminal Sanctions**

Criminal sanctions provisions available under the FCA. However, implementation has not yet started as there is no conviction record and no case presented before a court of law yet.

This variable is rated Medium (0.5).

#### e. **Availability of Effective Entry Controls**

The RBM is mandated by law to license all stock brokerage firms in the securities sector. The licensing process involves assessment of ML risk by administering a fit and proper test for shareholders, beneficial owners, board of directors and management of prospective entrants into

the securities brokerage industry. The Registrar of Financial Institutions conducts fit and proper tests for all shareholders and management of brokerage institutions and vet sources of capital funds during licensing process. Besides, all brokerage firms are required by law to have an AML compliance function and designate a senior officer to handle AML compliance issues. Furthermore, securities' sector players do conduct KYC/CDD procedures both at on-boarding stage and whenever transacting with clients.

This variable is rated Very High (0.8).

**f. Integrity of Staff in Security Firms**

So far, there is no record of staff from the securities sector aiding or colluding with criminals in order to undermine AML controls. There is one record of a member of staff from a brokerage firm who was involved in matters bordering on misconduct and lack of integrity, in which an employee of a stockbrokerage firm was trading in stolen shares. The matter is currently in court. In addition, the brokerage firm involved was sanctioned by the regulator (RBM) to pay for the losses incurred by the clients. Other than that, most firms vet their staff for criminal records before engaging them.

This variable is rated Medium High (0.6).

**g. AML Knowledge of Staff in Security**

AML knowledge in brokerage securities sector has improved greatly (compared to 2013 when the first NRA was carried out) following the RBM and FIA's efforts to enforce AML compliance. All brokerage firms have incorporated AML compliance into their business functions and conduct periodic training for their staff members, which is further enhanced with training provided by the RBM in conjunction with the FIA on their obligations under the FCA. Staff members in most brokerage firms are aware of their reporting obligations and have knowledge of ML typologies. Interviews with members of staff revealed that front officers responsible for account opening and dealing have general knowledge of AML/CFT issues.

This variable is rated Medium High (0.6)

**h. Effectiveness of Suspicious Activity Monitoring and Reporting**

Institutions monitor transactions and submit large currency transaction reports to FIA. However, the levels of STR reporting remain very low. Only one (1) STR was filed from the sector between 2014 and 2017. One of the reasons for irregular reporting of STRs is the institutions focus on the LCTRs and submit reports on attempted cases or cases which have been resolved administratively, case in reference is the case where a member of staff facilitated the sale of stolen shares.

This variable is rated Medium Low (0.4).

**i. Effectiveness of Compliance Function**



All brokerage firms have a compliance function in place and have designated an independent compliance officer at a senior management level for AML. Their compliance function is proportionate to the size of the institution, risk level, volume and nature of transactions and client profiles. In addition, all brokerage firms have AML policies and procedures, conduct KYC procedures both at on-boarding stage and whenever transacting with clients as part of their AML compliance programme. This variable is rated Medium (0.5).

**j. Availability and Access to Beneficial Ownership Information**

The FCA under section 16 has addressed the issue of beneficial ownership and securities obtain the information through KYC/CDD during on-boarding and in the course of the business relationship. However, it is difficult to obtain such information when the customer is a legal person. Verification of such information with the Registrar of Companies also poses challenges as the information may sometimes not be available. This variable is rated Medium (0.5).

**k. Availability of Reliable Identification Infrastructure**

Malawi's system for identifying its citizens, in the form of the National ID, has recently been introduced and not fully implemented. Currently, the main forms of identification for the sector are the passports and driver's licenses issued by the Department of Immigration and the RTD, respectively. All brokerage firms verify identities using these government departments. However, these documents have been subjected to abuse and forgery. This variable is rated Medium (0.5).

**l. Availability of Independent Information Sources**

The RBM and the Malawi Stock Exchange (MSE) are the main sources of information for the brokerage sector. The stock brokerage firm also obtains supporting customer information through utility bills issued by the Malawi Water Board and the Electricity Supply Commission of Malawi (ESCOM). This variable is rated High (0.7)

**m. Stock brokerage Inherent Vulnerability Assessment**

The inherent vulnerability for stock brokerage firms is dependent on a number of variable. Stock brokerage has a low asset size (MK1.5 billion in value of funds under management), low risk client base, no deposit features and the lack of cash transactions or activity. There is also low frequency of international transactions. For non-resident customers and other high-net wealth individuals and PEPs, the ML risk would arise mostly during Initial Public Offers (IPOs) when the source of funds used to acquire is not directly vetted by brokers. Stock brokerage firms rely on receiving banks to conduct due diligence on walk-in clients during IPOs. Thus, potential ML vulnerability for the sector arising from walk-in clients' transactions that are cash-based during the IPO are mitigated by banks.

***Portfolio Management Vulnerability Assessment***

**a. Comprehensiveness of AML Legal Framework**

The FCA has comprehensively covered AML/CTF issues by addressing KYC/CDD/EDD, reliance on third parties, record keeping, suspicious transaction reporting, tipping-off and confidentiality, internal controls, foreign branches and subsidiaries, regulation and supervision of financial institutions, supervisory powers and sanctions and administrative penalties. Money Laundering regulations are in place, but need to be revised to incorporate the changes from the FCA.

This variable is rated High (0.7).

**b. Effectiveness of Supervision Procedures and Practices**

Both the RBM and FIA conduct regular AML/CFT onsite inspections of portfolio managers. However, during the assessment period only one institution out of five (20%) was inspected. This was done by RBM in 2016. The inspection covered AML/CFT issues such as ML/TF Risk Assessment, AML/CFT Compliance Program, Internal/External Audit, Customer Identification Program, Customer Due Diligence and Suspicious Transaction Reporting. The report was duly shared with the FIA.

Although the FIA and RBM have experienced and qualified personnel and relatively sufficient financial resources for inspections, the staff compliment needs to be increased to ensure wider coverage of the sector.

This variable is rated Medium (0.5).

**c. Availability and Enforcement of Administrative Sanctions**

The repealed ML Act did not provide for administrative sanctions and the RBM did not and does not have administrative sanctions for portfolio managers on AML issues or AML related issues. While the FCA has provided for administrative sanctions, these are currently in draft form and are yet to be concluded and tested. The administrative sanctions include provisions for warnings, monetary penalties and recommendations for closure of business. Both FIA and RBM are working together in finalizing these as stated above.

This variable is rated Medium (0.5).

**d. Availability and Enforcement of Criminal Sanctions**

Criminal sanctions provisions for non-compliance are available under the FCA. However, no portfolio managers have been sanctioned for non-compliance during the assessment period.

This variable is rated Medium (0.5).

**e. Availability of Effective Entry Controls**

The RBM is mandated by law to license all portfolio management in the securities sector. The licensing process involves assessment of ML risk by administering a fit and proper test for shareholders, beneficial owners, board of directors and management of prospective entrants into the securities brokerage industry. RBM conducts fit and proper tests for all shareholders and

management of portfolio managers and vets sources of capital funds during the licensing process to ensure that the applicant indeed has the required finances to operate the business.

This variable is rated High (0.7).

**f. Integrity of Staff in Security Firms**

So far, there is no record of staff from the portfolio management engaging in fraud, aiding or colluding with criminals to undermine AML controls. There is one record of a member of staff from the sector who was sanctioned for lack of integrity or other forms of misconduct. Other than that, portfolio management firms vet their staff for criminal records before engaging them.

This variable is rated High (0.7).

**g. AML Knowledge of Staff in Security**

AML knowledge in portfolio management sector has improved greatly (compared to 2013 when the first NRA was carried out) following the RBM and FIA's efforts to enforce AML compliance. Most institutions have incorporated AML compliance into their business functions and conduct periodic training for their staff members which is enhanced with training provided by the RBM in conjunction with RBM on the FCA. Staff members in most brokerage firms are aware of their reporting obligations and have knowledge of ML typologies. Interviews with members of staff revealed that front officers responsible for account opening and dealing have general knowledge of AML/CFT issues.

This variable is rated Medium (0.5).

**h. Effectiveness of Suspicious Activity Monitoring and Reporting**

Institutions monitor transactions and submit large currency transaction reports to FIA. However, the levels of STR reporting remain very low. Between 2014 and 2017 no STR was filed with the FIA from portfolio managers. One of the reasons for irregular reporting of STRs is that most of the institutions focus on the LCTRs.

This variable is rated Medium (0.5).

**i. Effectiveness of Compliance Function**

All portfolio management firms have a compliance function in place and have designated an independent compliance officer at a senior management level for AML. Their compliance function is proportionate to the size of the institution, risk level, volume and nature of transactions and client profiles. In addition, all firms conduct KYC/CDD procedures both at on-boarding stage and during the course of the business relationship. Further, all institutions except one, have documented AML policies and procedures.

This variable is rated Medium (0.5).

**j. Availability and Access to Beneficial Ownership Information**

The FCA under section 16 has addressed the issue of beneficial ownership and securities obtain the information through KYC/CDD during on-boarding and in the course of the business relationship. However, it is difficult to obtain such information when the customer is a legal person. Verification of such information with the Registrar of Companies also poses challenges as the information may sometimes not be available. This variable is rated Medium (0.5).

**k. Availability of Reliable Identification Infrastructure**

Malawi's system for identifying its citizens, in the form of the National ID, has recently been introduced and not fully implemented. Currently, the main acceptable and reliable forms of identification for the sector are the passports and, driver's licenses and the voter's registration cards issued by the Department of Immigration and the RTD, respectively. Portfolio managers verify identities using these government departments. However, these documents have been subjected to abuse and forgery. This variable is rated Medium (0.5).

**l. Availability of Independent Information Sources**

The RBM and the Malawi Stock Exchange (MSE) are the main sources of information for portfolio managers, who are mandated by law to periodically submit information to the regulator. Portfolio managers obtains supporting customer information through utility bills issued by the Malawi Water Board and the Electricity Supply Commission of Malawi (ESCOM) This variable is rated High (0.7).

**m. Portfolio Management Inherent Vulnerability**

Portfolio management has more inherent vulnerability to ML risk given its asset size (MK827.3 billion in value of funds under management) and client base. High net-worth individuals and PEPs pose an ML threat or risk to the sector. However, securities sector laws help to mitigate the risk by mandating portfolio management firm to obtain information regarding the identity of beneficial owners before entering into contracts and verify sources of funds for investment.

Besides the level of cash activities is low as most transactions are through checks and bank transfers the due diligence of which is done by their respective banks. There is also existence of investment or deposit features especially for institutional investors who are mostly life insurance companies and pension funds.

***Deficiencies / Gaps Identified and Proposed Actions to Rectify the Issues***

The securities sector is rated as posing a Medium Low risk of ML/TF, however, there are a number of gaps that need to be addressed as revealed by the assessment.

The FIA and RBM need to intensify AML training for the sector and enhance supervision while implementing a risk-based approach to their supervision. The training will ensure that entities are aware of their AML obligations and that AML compliance functions are instituted.

Apart from that, it is essential that the FIA and RBM finalise the Financial Crimes Regulations so that the supervisory roles are clear. There is also a need to enhance staff compliment for the FIA and the RBM to strengthen AML regulation and supervision.

Further, administrative sanctions need to be enforced. The enforcement of administrative sanctions would help improve compliance especially relating to suspicious activity reporting. The absence of enforceable sanctions has contributed to the laxity in the sector.

The FIA, in collaboration with the sector regulator, should intensify enforcement of STR reporting by the sector.

In addition, there is also a need to enhance staff compliment for the FIA and the RBM in order to strengthen AML regulation and supervision.

The following table summarises areas that needs priority to address the identified deficiencies of the securities sector:

*Table 14: Prioritisation of general AML controls for securities sector*

<b>PRIORITY RANKING – Securities</b>	<b>Priority Ranking - Stockbrokers</b>	<b>Priority Ranking - Portfolio Managers</b>
Comprehensiveness of AML Legal Framework		
Effectiveness of Supervision Procedures and Practices	1	1
Availability and Enforcement of Administrative Sanctions	3	3
Availability and Enforcement of Criminal Sanctions	6	6
Availability and Effectiveness of Entry Controls		
Integrity of Staff in Securities Firms	8	
AML Knowledge of Staff in Securities Firms	1	1
Effectiveness of Compliance Function (Organisation)	3	3
Effectiveness of Suspicious Activity Monitoring and Reporting	3	5
Level of Market Pressure to Meet AML Standards		
Availability and Access to Beneficial Ownership Information	9	8
Availability of Reliable Identification Infrastructure	7	7
Availability of Independent Information Sources		

## Other Financial Institutions Vulnerability

### Background

Other financial institutions refer to those sectors that are financial in nature other than commercial banks, insurance and securities. These can be categorised as regulated (legally operating) and unregulated (illegally operating). The key players in the regulated category include foreign exchange bureaus (FEBs), money transfer operators (MTOs), microfinance institutions (MFIs) and mobile payment service providers or mobile money Operators (MMOs). On the other hand, the unregulated category consists of individuals and entities which operate illegally, and their operations include *hawala*, black market foreign exchange and loan sharking (*katapila*). This assessment covered both ML and TF risks posed by the sector.

The OFIs are reporting institutions (for AML/CFT purposes) under the FCA, however, they are regulated by the RBM under various legislations as indicated in the table below:

Table 15: Regulation of other financial institutions

Sector	Legislation / Regulations / Directives
Mobile Payments Services	<ul style="list-style-type: none"> <li>- Mobile payments Act;</li> <li>- Interoperability of Retail Payment Systems Directive, 2017; and</li> <li>- RBM guidelines</li> </ul>
Microfinance	<ul style="list-style-type: none"> <li>- Financial Services Act 2010;</li> <li>- Microfinance Act, 2010;</li> <li>- Financial Cooperatives, 2011; and</li> <li>- the directives issued under FSA.</li> </ul>
Foreign Exchange Bureaus	<ul style="list-style-type: none"> <li>- Exchange Control Act of 1989 and</li> <li>- Exchange Control Regulations of 2007.</li> </ul>

The table below gives a summary of the OFI sector:

Table 16: Profile of regulated OFIs

SUB-SECTOR	NUMBER OF PLAYERS	STATISTICS	
Mobile Payments	3	Value	US\$821.5 Million
		Volume	US\$195,000

<b>Microfinance Institutions</b> (including microcredit agencies, MFIs and SACCOs)	79	Total assets	US\$64.4 million
		Total loans	US\$39.5 million
<b>Forex Bureaus</b>	15	Total Sales:	US\$1.2 million
		Total purchases	US\$78.9 million
<b>Money Remittances</b>	11	Inward remittances	US\$37.8 million
		Outward remittances	US\$ 903,000

The assessment revealed that out of the four regulated OFIs, the highest ML risk is posed by Money Transfer Operators – rated **Medium High (0.70)**, then Foreign Exchange Bureaus – rated **Medium High (0.63)**, Mobile Money Operators – rated **Medium (0.56)** and Microfinance Institutions – rated **Medium Low (0.40)**.

Detailed sector analysis is as explained below:

**Money Transfer Operators (MTOs)**

*Introduction*

In the 2013 NRA, this sector was rated 0.70 (Medium High). Since then Malawi has made great strides, including registering more money remittance service providers. In March 2015, RBM introduced guidelines for operating money transfer agents in Malawi, which permit operators to be agents for more than one remittance institution. This resulted in registration of operators and agents to ensure compliance to ML/TF. The number of MTOs has increased from two (2) to eleven (11) since 2013 Statistics for the asset size and annual turnover of the MTOs could not be obtained. However, as at December 2016, total trading volumes for inward remittances were US\$37,784,744.00 while outward remittances totalled US\$902,966.57. The MTOs are MoneyGram, Western Union, Mukuru, Rapid Transfer, Hello Paisa, RIA Financial Services, Amerit Operations, Airtel Cross Border Transfers, Exchange4Free, International Financial Systems and Express Link. All these operate through agents in banks, foreign exchange bureaux, post offices and other financial institutions. Only four operators are licensed to make cross-border remittances while the rest only conduct domestic transaction

*Assessment of Variables*

The assessment took into consideration various variables, as explained below:

- a. **Comprehensiveness of AML Legal Framework**

MTOs are reporting institutions under the FCA and as such, the FIA is their AML supervisor. However, the FCA has also granted the FIA powers to delegate their AML supervisory role. FIA and RBM are currently working on delegation of this role. The FCA has mandated the FIA to supervise all financial institutions including money transfer agents on compliance with the FCA. However, while the AML law is in place, the accompanying regulation are not available. The current regulations do not address some of the issues appearing in the FCA. The 2011 AML Regulations are still in force but yet to be revised. This variable is rated therefore High (0.7).

**b. Effectiveness of Supervision/Oversight Activities**

The FCA gives the FIA powers to supervise the sector and the FIA works with RBM to supervise the sector using the available laws including Exchange Control Act and regulations and guidelines for licensing and operating money transfer agents. The supervision by RBM is mainly prudential as RBM's Banking Supervision's AML operations has not extended to the MTOs. The FIA conducts AML/CTF examinations on reporting institutions. However, between 2013 and 2017 none were conducted on the MTOs. The RBM has relatively adequate number of staff for supervisory assignment, however, they have not extended their work to include AML/CFT. The FIA has capable and knowledgeable staff to conduct AML/CFT supervision. However, the number of staff is limited. There is a working relationship between the FIA and the RBM and a draft MoU between the two authorities on delegation of supervisory authority is yet to be finalised.

The rating for the variable is therefore Medium (0.5).

**c. Availability and Enforcement of Administrative Sanctions**

Section 34 of the FCA gives powers to the FIA to impose administrative sanctions on non-compliant institutions. In addition, the Exchange Control Act and regulations provide administrative sanction for non-compliance with exchange control regulations which are mostly related to ML cases. In terms of licensing, the RBM has powers to revoke licenses of non-compliant operators on prudential matters. There has been a challenge to administer the available administrative sanctions despite the reported offences resulting in laxity by most operators. Currently there are no AML administrative sanction implemented on this sector. This variable is rated Medium (0.5).

**d. Availability and Enforcement of Criminal Sanctions**

The FCA provides for criminal sanctions for all reporting entities. However, these sanctions have not been meted out on any operator of this sector. This variable is rated Medium (0.5).

**e. Availability and Effectiveness of Entry Controls**

The Reserve Bank of Malawi registers/licenses all MTOs, using the various laws, regulations and guidelines for licensing and operation of MTOs in the country. RBM assesses all service agreements before entering into a contract with the MTO. RBM ensures that the agreement is in line with the current exchange control requirements and operating procedures. The sector is regulated as one



of the Authorized Foreign Exchange Dealers (AFED) under the Foreign Exchange Act and as such, the RBM conducts regular on-site inspections of the sector. The operators submit weekly and monthly returns to RBM for off-site inspections. In March 2015, RBM introduced guidelines for licensing and operating money transfer agents in Malawi under the Exchange Control Regulations. Most of the operators are agents of international money transfer organisations such as Western Union, which are also subjected to international ML regulations. A “fit and proper” test is conducted to prevent criminals (or their associates) from obtaining a business license. The RBM assesses educational and professional certification requirements for key directors and senior management in the Fit and Proper Test. This variable is rated High (0.7).

**f. Integrity of Business/Institution Staff**

The RBM scrutinises entrants into the sector to prevent all possible money launderers or their associates to the business. Some MTOs screen their staff during the hiring phase with the Malawi Police if the individuals have any criminal records while others run a background check with the individual’s previous employers. This variable is rated Medium (0.5).

**g. AML Knowledge of Business/Institution Staff**

There is basic understanding of the ML/TF requirements. The RBM and FIA conduct training for foreign MTOs front office staff on ML/TF laws and regulations, domestic and transnational money laundering schemes and typologies, including actual and potential misuse of the businesses and specialised knowledge and skills of their professionals and their products and services; and legal consequences for non-compliance. The training is however inadequate, as not all MTOs have been trained. There is poor staff retention and this affects staff knowledge as the new staff come with little AML/CFT knowledge. This variable is rated Medium (0.5).

**h. Effectiveness of Compliance Function (Organisation)**

Some operators have a well-structured and effective compliance function while others seem not to understand their obligations. It has also been noted that foreign investors and MTOs that are operating in Banks have a sufficiently-resourced, independent AML compliance officer appointed at senior management level. However, most of the local operators which are also small or medium in size appoint compliance officers but they have little or no independence as they are not at senior management level. Some operators carry out regular internal AML inspections while others wait for FIA to conduct AML inspection. Most organisations do not understand the national risk associated with non-compliance to AML/CTF laws. This variable is rated Medium (0.5).

**i. Effectiveness of Suspicious Transactions Reporting Monitoring**

Some MTOs have automated systems that can enable and facilitate the monitoring of client transactions and comparing them against the clients’ profiles before concluding a transaction. However, most MTOs manually file transaction records making it difficult to screen and monitor possible AML trends. During the assessment period, none of the MTOs submitted any STRs to the

FIA. Large currency transaction reports were however submitted to the FIA. This variable is rated Medium Low (0.4).

**j. Availability and Access to Beneficial Ownership Information**

The issue of access to beneficial ownership information has been addressed in the FCA. MTOs are able to access beneficial ownership information from their customers for a particular transaction.

This variable is rated High (0.7).

**k. Availability of Independent Information Sources**

There are two licensed Credit Reference Bureaux which are still in their infancy hence there is inadequate information to facilitate decision making or verification of concrete information. In addition to this, MTOs also use utility bills such as electricity and water bill to verify customer information. However, the problem with utility bills is that sometimes they are not in the customer's name. This variable is rated Medium (0.5).

**l. Availability of Reliable Identification Infrastructure**

The identification infrastructure in Malawi include Passports, Driver's Licence and National Identification. However, the National ID which was recently introduced has only registered about nine million citizens by December 2017 and some people were yet to receive their IDs. Some customers use identification documents under simplified CDD such as voter registration card, student ID, letters from the District Commissioner and local chiefs. This variable is rated Medium High (0.6).

**m. Inherent Vulnerability**

The inherent vulnerability of MTOs is assessed as High (0.82). This rating has been based on several variables such as size, use of agents, client base profile, frequency of international transactions, anonymous use of the product, tracing of the transactions, existence of ML typologies and use of the product in fraud or tax evasion, non-face to face use of the product and the existence of informal MTOs.

The size of the sector is rated Medium. There are 11 licensed money transfer platforms operating through 17 institutions in the country. Three of the eleven platforms have business establishments in the country while the rest operate through various agents like banks, bureaux, post offices, courier agents and other businesses. Some of the MTOs agents are accessible even in the remote place of the country through Malawi Post Office and mobile phone operator agents. It was difficult to obtain data on asset size of MTOs from the operators. However, data on trading volumes indicate that as at 31<sup>st</sup> September 2017, total value of transactions for inward remittances was \$37.7 Million and \$902, 966.57 for outward remittances.

The client base of MTOs includes domestic Politically Exposed Persons (PEPs), low to medium-net-worth individuals and both resident and non-resident clients who pose Medium Risk.

There is High use of agents by MTOs compared with the use of agents in other FIs. There are 11 money transfer platforms operating in 17 financial institutions with 2 of the operators using various forms of agents including road side kiosks and mobile money agents to operate the MTO services. There is High use of cash, with an exception of mobile money and commercial bank agents where funds are transferred through the clients' account. For bureaux and other businesses that are not mandated to open an account for a client, one has to deposit cash for outward remittances or be given cash for inward remittances.

The frequency of international transactions is High in MTOs that are established for international remittances as opposed to local money remitters. International wire transfers and other international transactions are high with this product. The value of the transactions is generally low however some of the jurisdictions MTOs deal with are regarded as high risk jurisdictions for both inward and outward transactions. Anonymous use of the product is not available and non-face-to-face use of the product is also not available. It is easy to trace the transaction records as most operators use electronic transaction systems.

Money laundering typologies through MTOs exist and the use of the product in fraud, or tax evasion schemes also exists but is limited as evidenced by reports of illegal externalisation of forex. In recent years, fake MRA documents were used to support transactions of import payment for goods that were alleged to have been registered for custom and cleared with MRA<sup>38</sup>.

The existence of informal money remitters systems such as *hawala* is High. However, there is no data to quantify the informal money remitters. There is significant activity in the informal sector where people send and receive money to other countries through relations and friends to avoid transaction charges required by the formal service providers. The *hawala* method of transferring funds is mostly used by Malawians living abroad or those with children studying abroad. It is also a common practice among Malawians of Asian origins and operates on trust and secrecy.

#### n. Other Vulnerable Factors of the MTOs

There is an existence of illegal money remittance services; in the form of *hawala*. *Hawala* is an alternative or parallel remittance system that exists and operates outside of, or parallel to "traditional" banking or financial channels<sup>39</sup>, It works by transferring money without actually moving it. Its dealings are done underground with no formal records being kept and the practice

---

<sup>38</sup> Typologies report 2015/2017, Financial Intelligence Authority (<https://www.fia.gov.mw>)

<sup>39</sup> FINCEN

relies on trust and extensive use of connections such as family relationships or regional affiliations. In Malawi, this market is unregulated.

The asset size of this market is not known. However, there has been movement of huge sums of money outside the formal financial system through this system and it is a potential breeding ground for ML/TF as source of the funds cannot be established. The system is swift, attracts little to no commissions and there are no restrictions on how much can be remitted.

In Malawi, *hawala* comes in different forms, the most common being; Malawians living in the diaspora deposit foreign currency in a designated account outside Malawi to the credit of a colleague residing in Malawi. This Malawi resident will in turn either deposit the equivalent amount in Malawi Kwacha locally to the credit of the Malawian living abroad or pay directly to the supplier on behalf of the Malawian. In such cases transfers attract an “interest rate” agreed upon by the two parties, or; A Malawian resident in a foreign country visiting Malawi buys goods or services in Malawi but pays for them in the country of residence, denying Malawi of foreign currency.

The existence of this parallel market in Malawi has served the interests of a small group of people; mainly PEPs, business people, the Asian community and Malawians living abroad. There is a huge likelihood that ML activities are facilitated through this practice. It is believed that some of the finances used in constructing houses by Malawians living abroad are remitted using *hawala*. The assessment could not establish whether the *hawala* system is used for TF.

## Foreign Exchange Bureaus (FEBs)

### *Background*

As at 30 October 2017, the RBM had licensed 15 foreign exchange bureaus with 45 branches across the country. Of the 15, three bureaus namely FDH Money Bureau, Standard Bank Bureau De Change and NFB Forex Bureaus are subsidiaries of Commercial banks while the rest are stand-alone operators. In March 2015, the RBM issued a new regulation which allows foreign exchange bureaus to operate through agents. Only one bureau, Midland Forex Bureau has a branch and 4 agents.

As at 31 December 2016, total foreign exchange sales were at \$94,884,703.00 while total purchases were \$78,884,703.00. In 2015, the RBM issued a directive for bureaus to renew their licenses every three years. This has resulted in laxity for bureaus to submit the audited financial reports annually. This also created a challenge in collecting data on total asset size for exchange bureaus for the purposes of this assessment. Only 6 of the 15 bureaus (40%) responded to the request for audited financial statements and the total asset value for these six as at 31 December 2015 was MK901,510,543.00 (US\$1,226,544.96)

### **Vulnerability Assessment**

The sector has a final vulnerability of 0.63 (Medium High) and inherent vulnerability of 0.65 (Medium High). The final vulnerability was based on a number of variables, such as comprehensiveness of AML legal framework, availability of criminal and administrative sanctions, effectiveness of supervision, AML knowledge of staff and many more. Detailed analysis of the variables is as explained below:

#### **a. Comprehensiveness of AML Legal Framework**

The FCA mandates the FIA to supervise all financial institutions including FEBs on compliance with the existing AML laws. The FCA adequately addressed AML issues such as KYC, CDD/ECDD, beneficial ownership, record keeping, internal controls, tipping off and confidentiality and suspicious transaction reporting. However, while the AML law is in place, the accompanying regulation are not available. The current regulations do not address some of the issues appearing in the FCA. The 2011 AML Regulations are still in force but are yet to be revised. This variable is rated High (0.7).

#### **b. Effectiveness of Supervision/Oversight Activities**

The FCA gives the FIA powers to supervise the sector on AML matters and the FIA works with RBM to supervise the sector. The RBM's banking and supervision division has relatively adequate number of staff for AML/CFT supervisory assignment. However, the supervision of FEBs by RBM has mainly been for prudential purposes and not focused on AML/CFT. The FIA has well knowledgeable staff to carry out AML/CFT supervision however it has limited number of staff. There are 15 registered FEBs during the period under review. However, since 2013, there have been only 4 AML/CFT inspections conducted by the FIA, representing 26%. There is a working relationship between the FIA and the RBM and a draft MoU between the two authorities on delegation of authority to RBM awaits signing.

The rating for the variable is therefore Medium (0.5).

#### **c. Availability and Enforcement of Administrative Sanctions**

The FCA under section 34 has made provisions for administrative sanctions in the form of warnings, monetary penalties and recommendations for closure of business. While the FCA has provided for the administrative sanctions, the regulations governing their implementation are currently in draft form and are yet to be concluded and enforced on the sector.

This variable is rated Medium (0.5).

#### **d. Availability and Enforcement of Criminal Sanctions**

The FCA provides for criminal sanctions for non-compliance with ML requirements, however; they have not been applied on any operator of this sector. This variable is rated Medium (0.5).

#### **e. Availability and Effectiveness of Entry Controls**

The RBM registers/licenses FEBs. Licensing of the sector is governed by the Exchange Control Act, regulations and guidelines for licensing and operating Foreign Exchange Bureaus. A “fit and proper” test is conducted to prevent criminals (or their associates) from being granted a business license. This includes the RBM assessing educational and professional certification requirements for key directors and senior management. The FCA provides for all financial institutions to have adequate AML compliance controls in place, including compliance policies and procedures and the appointment of well-qualified compliance officer who is supported by other compliance staff. This variable is rated High (0.7).

**f. Integrity of Business/Institution’s staff**

Most staff in FEBs perform their duties with integrity. Before recruitment, some FEBs vet their staff with the police while others verify staff integrity with the staff’s previous employers. There have not been any reported integrity breaches by staff. This variable is rated Medium (0.5).

**g. AML Knowledge of Business/Institution staff**

The RBM and FIA conduct training for foreign exchange bureaus compliance staff on AML/CFT. It is then the responsibility of the institution to ensure that relevant staff are also trained. While most FEBs that operate under banks would have knowledgeable staff, the same does not apply to those FEB operating independently. Not all the independent FEBs have conducted AML training for their key staff. Considering that the independent FEBs constitute 80% of the sector, this means that most of the staff are not fully aware of AML issues. In addition, the high staff turn-over in the sector affects institutional knowledge as trained staff leave the industry. This variable is rated Medium (0.5).

**h. Effectiveness of Compliance Function (Organisation)**

Some operators have a well-structured and effective compliance function while others do not. FEBs that are operating in Banks have a sufficiently resourced, independent AML compliance officer appointed at senior management level while the stand alone FEBs which are mostly family businesses appoint compliance officers who have little or no independence. Though the FCA gives opportunity to financial institutions that have less than 5 employees to appoint the chief executive officer as compliance officer, standalone FEBs appoint another officer to be compliance officer even though this person will have no independence. Some operators carry out regular internal AML inspections especially those affiliated to banks while others wait for FIA to conduct AML inspection. This variable is rated Medium Low (0.4).

**i. Effectiveness of Suspicious Transactions Reporting Monitoring**

Forex bureaus usually report Large Currency Transactions. However, there has been no STR filed to the FIA between 2013 and 2017. This variable is rated Very Low (0.2).

**j. Availability and Access to Beneficial Ownership Information**

The issue of access to beneficial ownership information has been addressed in the FCA. FEBs are able to access beneficial ownership information from their customers using the available CDD measures. This variable is rated Medium High (0.6).

**k. Availability of Independent Information Sources**

FEBs verify information through independent sources such as the credit reference bureau, the Immigration Department and Road Traffic Directorate. They also verify information with employers where necessary. For instance, in cases where foreign currency is being purchased for official purposes. This variable is rated Medium (0.5).

**l. Availability of Reliable Identification Infrastructure**

This variable is rated Medium (0.5). FEBs are able to identify customers using IDs such as passports, driving licences. The introduction of national ID will help mitigate the problem of customers without proper identification.

**m. Inherent Vulnerability of Forex Bureaus**

The inherent vulnerability of forex bureaus is assessed as Medium High (0.65). This has been based on a number of variables such as size, use of agents, client base profile, frequency of international transactions, anonymous use of the product, tracing of the transactions, existence of ML typologies and use of the product in fraud or tax evasion, non-face to face use of the product and the existence of informal or parallel systems.

The size of the forex bureau sector is medium. There are 15 registered foreign exchange bureaus in the country operating through 45 outlets and 3 agents. Three of the 15 are subsidiaries of commercial banks while the rest are stand-alone bureaus.

The client base of FEBs range from domestic Politically Exposed Persons (PEPs); low to high-net-worth individuals; both resident and non-resident clients and business persons. This entails that the sector's client base profile has medium risk.

Use of agents by FEBs is significantly low compared with the use of agents in other FIs. It is one forex bureau that has 3 agent outlets.

FEBs are spot cash-based transactions. Bureaus are not allowed to open accounts for clients and transactions are cash based. This means FEBs are highly cash intensive.

Foreign Currency obtained in FEBs is international transaction when one travels out since it is illegal to trade or hold foreign currency in Malawi. Frequency of international transactions in the forex bureau sector is high.

The value of the transactions is generally high and client's destinations include some jurisdictions that are considered to be high risk jurisdictions.

There are is existence of ML typologies trends on abuse of the product. For example, in recent years, there has been an increase in use of fake bus and air tickets to access the allowable maximum travel allowance limit of \$10,000. Further, there has been an increase in the number of customers who access the allowable maximum limit from different bureaus. Usually the abusers use the same bus or air ticket service providers.

There are some factors that are prevalent in the informal market such as anonymity use of the product, difficulty is tracing the transaction records. Anonymous use of the product is not available on the market.

Use of the product in fraud, or tax evasion schemes exists as evidenced by reports of illegal externalisation of forex by business people who export cash for importation or just to externalise to avoid taxes. For instance, in recent years, there has been an increase in use of fake bus and air tickets to access the allowable maximum travel allowance limit of \$10,000. Further, there has been an increase in the number of customers who access the allowable maximum limit from different bureaus. Usually the abusers use same bus or air ticket service providers. Lack of KYC or CDD and a real-time electronic monitoring system also poses ML risk. There are several cases where people have been found with large sums of foreign currency in their homes or at the airport trying to externalise the funds.

In tracing the transaction records, it is Difficult and Time consuming to trace records because documents are manually filed with and there is no proper filing system in more operators.

- Non face to face use of the foreign exchange bureaus sector is not available.
- Anonymous use of foreign exchange bureaus is also not available.
- Existence of informal players in the sector is high. These are parallel black market forex dealers.

#### n. **Other Vulnerable Factors**

An informal and unregulated illegal market whose dealings are done underground, without official records also exists. The rates applicable are usually higher than the official bank rates. People often utilise this service because it is faster, there are no limits as to how much one can buy or sell, no questions are asked on the purpose for the purchase of the foreign currency and identification documents are not required, and through this, the rigorous process under Exchange Control Regulations is avoided.

The main players in this business are:

- Vendors/dealers who are usually stationed near shopping malls or at border posts. Some business persons, both local and international also engage in this practice. Those who do



cross-border trade may buy or sell foreign currency among themselves. Their exchange rates are usually based on the dominating bank rates.

- Some prominent business people of the Asian community in Malawi buy and sell foreign currency informally amongst themselves outside the formal financial systems. These Asians usually do not sell to any person but rather secretly to those they know or are connected to fellow Asian business associates.

This practice poses a ML/TF risk because there are huge amounts of money involved and there is no audit trail since there are no records such as sources of funds. The money being exchanged could be from illegal economic activities and hence promote ML/TF.

## **Mobile Payment Services**

### ***Background***

Mobile payment services are mobile phone-based financial services that allow subscribers (both banked and unbanked) to send and receive money, pay bills, and buy goods and services. They also allow for bulk payments, such as payment of salaries and loans. There are currently three registered service providers in Malawi; Airtel Limited and Telekom Networks Malawi (TNM) and Zoon Transactions Limited. These are hereinafter referred to as Mobile Money Operators (MMOs).

Airtel Money and TNM Mpamba mobile money services use a mobile wallet and were launched in March 2012 and May 2013 respectively. In addition to the transactions which customers can do from their mobile phones, their operations comprise a network of agents spread across the country where customers can purchase e-value, send and cash out money; merchants who accept mobile money for payment for goods and services; and banks which facilitate funds transfers between subscriber's bank accounts and their mobile wallets

Zoon Transaction limited, on the other hand, introduced their product in October 2015. The Zoon product is different from the product offered by Airtel and TNM as it is agent-based and customers do not use a mobile wallet for their transactions. Instead, customers conduct their transactions (sending and receiving money only) at agents' points established across the country, using the Airtel and TNM mobile networks.

### ***ML/TF Vulnerability***

There have been various changes in the sector since the last assessment, among them, change in AML law, introduction of new players and products and AML/CFT training. As a result, this assessment has established the sector as having a final vulnerability rating of Medium (0.56) and inherent vulnerability of Medium (0.56). This rating is higher than that of the previous assessment, which established the sector as posing Medium Low (0.22) risk.

The vulnerability assessment considered the following general variables:

**a. Comprehensiveness of AML Legal Framework**

The FCA has comprehensively covered Mobile Payment Services as reporting institutions under section 2. The FCA conforms to international standards on combating ML as it covers all areas of KYC/CDD/EDD, reliance on CDD by third parties, record keeping, suspicious transaction reporting, tipping-off and confidentiality, internal controls, foreign branches and subsidiaries, regulation and supervision of financial institutions, supervisory powers and sanctions and administrative penalties (See FCA sections 16 to 34). The existing subsidiary legislation (Regulations) was based on the repealed Money Laundering, Proceeds of Serious Crimes and Terrorist Financing Act. Even though these Regulations are still applicable, they were drafted in 2011 and few of the issues covered in the FCA are not reflected such as administrative sanctions and beneficial ownership, among others. This variable is rated High (0.7).

**b. Effectiveness of Supervision/Oversight Activities**

The FIA has been supervising the sector on AML matters. FIA has conducted desk reviews and has helped the sector in compiling AML/CFT policies and procedures and generally setting up of their compliance functions. FIA has conducted one on-site examination; on Airtel Money and TNM Mpamba and this was in 2013. None have been conducted on Zoon since it started its operations. This sector was rated Medium Low risk during the 2013 assessment, therefore the focus was on the riskier sectors. This variable is rated Medium (0.5).

**c. Availability and Enforcement of Administrative Sanctions**

The FCA, section 34, has made provisions for administrative sanctions in the form of warnings, monetary penalties and recommendations for closure of business. While the FCA has provided for the administrative sanctions, the regulations governing their implementation are currently in draft form and are yet to be concluded and enforced on the sector. This variable is rated Medium (0.5).

**d. Availability and Enforcement of Criminal Sanctions**

Criminal sanctions are provided both under the FCA and the repealed ML Act. However, there have been no ML criminal cases in the sector yet. This variable is rated Medium (0.5).

**e. Availability and Effectiveness of Entry Controls**

The Payments System Act 2016 and the Guidelines on Application and Authorisation of Payment Service Providers gives minimum requirements for new entrants. The Guidelines provide for fit and proper assessment of directors and senior management of prospective applicants and they even apply to beneficial owners. The Guidelines provides a list of requirements that must be satisfied by an applicant. Once the requirements are met, the applicant is invited to make a presentation to a taskforce comprising members drawn from various relevant departments of RBM, including foreign flows monitoring, audit, ICT, and other stakeholder institutions such as the FIA and MACRA. After

the presentation the new entrant, where necessary, is given areas they need to work on including, AML/CFT issues. Once this process is completed and depending on the consensus from the assessment of the proposed service a license is either given or denied by the RBM. This variable is rated Medium (0.5).

**f. Integrity of Business/Institution Staff**

The products are mostly provided through agents, some of whom have been involved in integrity breaches such as defrauding customers such as charging the customers amounts outside the MMO's tariffs. Recently there have been reported cases where agents would receive wrong transaction money and misuse the funds and also some agents would deliberately not cooperate with the business rules, such as not recording details of the transaction as required. On the other hand, there have been no reported malpractices among mainstream staff of the service providers. Mainstream staff are bound by code of conducts, which they are required to read, know and also sign off on yearly basis. This variable is rated 0.4 (Medium low).

**g. AML Knowledge of Business/Institution Staff**

MMOs conduct training for their own staff as well as those agents that support delivery of services. Responses from the questionnaires administered show that MMOs conduct periodic training for their staff especially at entry point which is part and parcel of training conducted for new employees. However, refresher courses also sometimes administered periodically. FIA has trained staff and agents of two of the three service providers, with the remaining service provider opting to conduct the training itself. This variable is rated Medium High (0.6).

**h. Effectiveness of Compliance Function (Organisation)**

MMOs have fully fledged compliance functions, with competent and qualified compliance officers. The heads of compliance of all the MMOs are at senior management level and two of the services providers' heads are AML certified. All the MMOs have enough funding to enable them to fulfil their duties. The compliance function provides the necessary support to agents, customers, merchants and billers to ensure risks related to ML/TF are minimised. In addition to this, all the MMOs have AML policies and procedures in place. This variable is rated High (0.7).

**i. Effectiveness of Suspicious Transactions Reporting Monitoring**

All the MMOs report large currency transactions on weekly basis to FIA and also suspicious transactions as and when they occur. However, there has only been one STR reported in 2017, with all the MMOs claiming that there were no further STRs during that period. This variable is rated Medium (0.5).

**j. Availability and Access to Beneficial Ownership Information**

Beneficial ownership information is available and accessible where the customers are registered with the MMOs. However, access to such information is difficult for those customers who are

unregistered. The MMO services are provided to both registered and unregistered customers, meaning that a registered customer can send money to an unregistered customer. Since mobile phone registration is a fairly new concept in Malawi, the unregistered customer poses challenges, especially where the identification documents are unreliable and some customers have to use other people to complete the transactions by using their identification documents. Further to this, issues of beneficial ownership are fairly new, especially among the agents. MMO customers are required to provide a valid identification document as part of the Know Your Customer (KYC) procedures when registering and also when transacting. This variable is rated Medium High (0.6).

**k. Availability of Reliable Identification Infrastructure**

Mobile money service providers can identify customers using IDs such as voter registration identification, passports, driving licenses and other less stringent documentations. However, one of the challenges facing the sector is the lack of reliable identification documents by the majority of Malawians, especially those living in rural areas. This forces service providers to use less stringent and unreliable identification documents such as the voter registration card, letters from the chief/village headman and unverifiable employer IDs. Nonetheless, the Government has introduced the national identification card which is expected to ease identification challenges. However, this is currently being put in place and not all eligible Malawians have registered or received their national identification. This variable is assigned a rating of Medium (0.5).

**l. Availability of Independent Information Sources**

The availability of Credit Bureau provides channels for independent information on financial information. However, such services attract certain fees which help in deterring institutions from using them. In addition, this Credit Bureau is fairly new and therefore may not have adequate information. In some cases, MMOs also use utility bills such as water and electricity bills to verify customer information. However, these bills are sometimes not in the customers' names. This variable is rated Medium (0.5).

**m. Inherent Vulnerability**

The inherent vulnerability is rated 0.62 (Medium High). This rating has been based on a number of variables such as size, use of agents, client base profile, frequency of international transactions, anonymous use of the product, tracing of the transactions, existence of ML typologies and use of the product in fraud or tax evasion, non-face to face use of the product and the existence of informal money remittance providers.

The size of the sector is considered small and is rated Low. The number of mobile money subscribers reached 4.5 million out of which only 1.4 million subscribers (33%) were active as at 31<sup>st</sup> October 2017. The agent network that support the delivery of mobile money services in Malawi was at 30,568 in October 2017 with only 19,625 being active over a 90-day period. The volume of mobile

money transactions averages K11.9 million per month whereas the corresponding value of transactions averages K50.3 billion per month in the year 2017. This trend shows great improvement compared to the 2013 assessment period when mobile money services had just been launched in Malawi.

The mobile money sector is Highly cash intensive as cash in/out dominate the value of mobile money transactions in the country. The sector has a wide range of clients who are considered Medium Risk. These customers include PEPs, regular individuals, SMEs, NGOs, registered and companies.

The sector involves high use of agents which provide the primary interface with customers in the delivery of services. The frequency of international transactions is Low as only one provider, Airtel Money started providing cross-border transactions in 2016 and there is a threshold to the maximum amount of funds one can send or receive. To mitigate against ML/ TF risks, Airtel has instituted several measures, among them:

- One can only send money from South Africa, through Airtel's collaborating partners, who are required to collect KYC/CDD information from the sender;
- Only Airtel Money registered customers in Malawi can receive and send money to Airtel Money sister countries i.e. Zambia, Tanzania and Rwanda; and
- Transactions with the Airtel Money sister countries mentioned above can only happen among registered customers only.

There is no anonymity in the use of the mobile money service as customers are supposed to register first before using the service. Non-face to face use of the product is available especially for fund transfers, bill payments and other services.

It is easy to trace transactions as there is an audit trail for each and every transaction

International ML typologies exist but are limited. However, there are no local typologies. The product has been used in fraud and tax evasions but at a limited level. The fraud is mainly committed by agents.

## Microfinance Institutions Vulnerability

### Background

According to the Finscope Malawi Small, Medium and Micro-Enterprises (SMMEs) survey of 2012<sup>40</sup> it was reported that about 80% of the Malawi population does not have access to financial services. Therefore, the microfinance sector attempts to provide services such as loans, savings, micro-insurance, funds transfers and payment services to those who are unbanked. The products are delivered mostly through face to face and use of agents. The institutions operate in both rural and urban areas.

As at December 2017, the microfinance sector comprised thirty-five (35) registered microcredit agencies, nine (9) licensed non-deposit taking microfinance institutions, one (1) licensed deposit taking microfinance institution whereas the financial cooperatives (SACCOs) sector comprises thirty-four (34) licensed SACCOs.

The assets size for the microfinance sector stood at K35.5 billion in September 2017 while the financial cooperatives reported total assets amounted to K11.8 billion. The volume as measured by gross loans stood at K21.3 billion and K7.7 billion for microfinance and financial cooperatives sectors respectively.

### ML/TF Risk Control Measures

The sector has a final vulnerability of 0.40 (Medium Low) The final vulnerability was based on a number of variables, such as comprehensiveness of AML legal framework, availability of criminal and administrative sanctions, effectiveness of supervision, AML knowledge of staff and many more. Detailed analysis of the variables is as explained below:

#### a. 2.7.5.2.1 Comprehensiveness of AML Legal Framework

The FCA has comprehensively covered MFIs as reporting institutions under section 2. The FCA conforms to international standards on combating ML as it covers all areas of KYC/CDD/EDD, reliance on CDD by third parties, record keeping, suspicious transaction reporting, tipping-off and confidentiality, internal controls, foreign branches and subsidiaries, regulation and supervision of financial institutions, supervisory powers and sanctions and administrative penalties (*See FCA sections 16 to 34*). The existing subsidiary legislation (Regulations) was based on the repealed Money Laundering, Proceeds of Serious Crimes and Terrorist Financing Act. Even though these Regulations are still applicable, they were drafted in 2011 and few of the issues covered in the FCA

---

40 <http://www.finscope.co.za>

are not reflected such as administrative sanctions and beneficial ownership, among others. This variable is rated High (0.7).

**b. Effectiveness of Supervision/Oversight Activities**

The FIA is the supervisory body for AML/TF under the FCA. The FIA may delegate powers to a supervisory authority or a self-regulatory body to regulate and supervise reporting institutions under its purview. The FIA has well qualified staff to conduct AML/CFT supervision but has limited number of staff. The Registrar of Financial Institution under banking supervision department has skilled members of staff to conduct AML/CFT supervisory assignments. Since 2013, there has been one AML/CFT assessment in the sector conducted by RBM. There is a Draft MoU between RBM and FIA on delegation of AML/CFT supervision which is at an advanced stage.

However, loan sharks which are unregulated also operate as part of this sector and it's impossible to supervise these. This variable is rated Medium Low (0.4).

**c. Availability and Enforcement of Administrative Sanctions**

Section 34 of the FCA provides for the FIA to impose administrative sanctions on non-compliant institutions. Furthermore, section 27 of the FSA provides for the Registrar to suspend or revoke a license issued to a financial institution. Two of the grounds on which this action can be taken are where the institution is not operating with integrity, prudence, professional skills or sound business principles or where it is likely to be involved in criminal activity. Meanwhile, no sanctions have been applied for non-compliance with AML requirements on this sector. This variable is rated Medium Low (0.4).

**d. Availability and Enforcement of Criminal Sanctions**

The FCA provides for criminal sanctions for ML/TF, requiring that the FIA recommend to the Director of Public Prosecutions the commencement of criminal proceedings against a reporting institution for non-compliance. These criminal sanctions have not yet been enforced on the microfinance institutions, their directors or senior management and also there are no reported criminal cases in the sector, however there have been incidents involving unregulated players who usually go unpunished. This variable is rated Medium Low (0.4).

**e. Availability and Effectiveness of Entry Controls**

The Registrar of Financial Institutions under the FSA 2010, Microfinance Act 2010, and Financial Cooperatives 2011 provide specific provisions to guide new entrants and for on-going supervision of the microfinance institutions. Furthermore, the Registrar also assesses educational and professional qualification requirements for directors and senior management as part of a "fit and proper" test.

The Registrar of financial institution's Directives require applicants for a microfinance license to provide detailed information on their legal ownership and management structures. Where an

applicant is a part of group, information must be submitted on the group structure clearly showing the applicant's position within the group and outlining lines of authority including reporting lines to the parent institutions. The application must also provide information on the nature of the activity undertaken by all entities within the group. It is also a requirement that applicants provide information on the products and services they plan to offer and for other categories and relevant systems which the institution will employ to manage inherent risks in their operations.

This variable is rated Medium (0.5).

**f. Integrity of Business/institution**

There have been cases of corruption by staff of some staff of the sector. For instance, there have been cases where members of staff of MFIs demand some fees from clients for certain services that do not require such fees. The presence of the informal sector also presents integrity concerns. This variable is rated Medium (0.5).

**g. AML Knowledge of Business/Institution staff**

FIA and RBM conduct AML training programmes, though not adequate for the sector. There is need to conduct trainings on ML issues for the microfinance sector considering that there is poor staff retention in the sector. MFIs are mandated to ensure that their staff are trained in AML/CFT. It was observed during an onsite examination by the RBM in 2016 that AML knowledge among employees in the microfinance sector was inadequate especially for small microfinance service providers. The understanding of ML/TF risks is limited to undertake appropriate risk assessment and design appropriate controls. This variable is rated Medium Low (0.4).

**h. Effectiveness of Compliance Function (Organisation)**

Based on one AML/CFT onsite examination conducted on a licensed microfinance institution in June 2016, most microfinance institutions do not have effective compliance functions and compliance management programme except for prudential purposes. Only 1 institution has a compliance officer. This variable is rated Very Low (0.2).

**i. Effectiveness of Suspicious Transactions Reporting Monitoring**

There is only one microfinance institution which complies with the obligation of reporting large currency transactions and STRs. The institution filed 1 STR to the FIA in November 2017. Considering the size of this sector and reporting trend, this variable is rated Very Low (0.2).

**j. Availability and Access to Beneficiary Owner Information**

Beneficiary information is available and accessible. The issue of access to beneficial ownership information has been addressed in the FCA. MFIs are able to access beneficial ownership information from their customers using the available CDD measures. Customers are required to provide a valid identification document as part of the Know Your Customer (KYC) procedures when registering and also when transacting. This variable is rated Medium High (0.6).



**k. Availability of Independent Information Sources**

There are licensed credit reference bureaus operating in Malawi and MFIs are obliged to report credit information. The credit bureaus also provide independent information which MFIs can source. However, this is often at a cost. Further to this, the National Credit Bureau is still in its infancy hence there is inadequate information to facilitate decision making or verification of concrete information. MFIs also use utility bills to supplement customer details. This variable is rated 0.5 (medium).

**l. Availability of Reliable Identification Infrastructure**

MFIs use reliable identification documents such as passports and driving licenses. However, the majority of customers, especially those living in rural areas, do not have the passports or driving licenses. For such customer, reduced KYC is used instead and the customers are allowed to use other IDs such as Malawi Electoral Commission voter registration card, letters from the chief/village headman and unverifiable employer IDs. Nevertheless, the rolling out of a national identification system is underway and will address the challenge.

In this regard, the variable is rated Medium (0.5).

**m. Inherent Vulnerability of Microfinance Institutions**

The inherent vulnerability of microfinance institutions is assessed **Medium Low (0.40)** with a final vulnerability rating of **0.40 (Medium Low)**. This is based on a number of variables such as size, use of agents, client base profile, frequency of international transactions, anonymous use of the product, tracing of the transactions, existence of ML typologies and use of the product in fraud or tax evasion and non-face to face use of the product.

The size of the microfinance sector is considered medium low. It is categorised into microcredit agencies (MCAs), Non-Deposit Taking Microfinance Institutions (NDTIs), Deposit Taking Microfinance Institutions (DTI) and Financial Savings and Credits Cooperative Societies (SACCOs). There are currently 35 registered MCAs, 9 NDTIs and 1 DTI and 34 licensed SACCOs.

The client base profile of the Microfinance sector is rated low risk. The clients are mainly Malawian nationals. Majority of the clients are women in rural areas. Nevertheless, the sector is also used by PEPs.

The use of agents in the microfinance sector is rated medium low. Agents in the sector are permitted for prudentially regulated microfinance institutions and SACCOs as an extension of the activity of principal financial institution. Institutions obtain approvals from the Registrar of Institutions to operate using agents and the agents are vetted by the principal institution.

The level of cash intensiveness associated with microfinance sector is high. The values for most individual transactions are smalls but the volumes are high.

Frequency in international transactions in the sector is rated low as all the transactions are domestic. However, it should be noted that some MFIs operate in areas that are close to the borders with other countries such that some foreigners may have access to the services offered by the MFIs.

Anonymous use of the product in Microfinance sector is not available. Beneficial owners of the transaction are identified and verified and customers are subjected to due diligence. However, some people can obtain loans on behalf of other people and not disclosed to the MFI. In such cases, it means due diligence is done on the customer who has applied for the loan and not the actual beneficial owner.

Transaction records in this sector can be traced but it is difficult and time consuming. This is because there are some institutions that do not have adequate automated MIS to monitor their transactions. There is unavailability of non-face-to-face initiation of business relationships, with respect to the microfinance (or microfinance products) hence face to face transactions are common. There are no ML typologies on the abuse of the Microfinance sector in Malawi and no typologies were found from outside Malawi. However, the use of the sector for fraud and tax evasion schemes exist but both are limited.

There is existence of un-regulated players (loan sharks). These are individuals and sometimes institutions that operate without requisite licence by loaning money to individuals at an interest rate that is above a maximum lending rate, sometimes collected under blackmail or threats of violence. According to FATF, loan sharks may be financed and supported by organised crime networks who are also involved in money laundering activities. A loan shark usually preys on individuals who are struggling financially or, for some reason, are unwilling to seek credit from legal sources. Persons in debt to loan sharks may be coerced into assisting with money laundering schemes.

In addition to the loan sharks, there are also what is known as “village savings and loans” whose total asset sizes could not be determined. These are usually conducted by people in a group who contribute and lend each other money usually on a monthly basis. The challenge with most of such groups is that sometimes the participants may not be known to the group.

**Priority Ranking for AML Controls**

*Table 17: Priority ranking for AML controls for the Other Financial Institutions sector*

PRIORITY RANKING FOR AML CONTROLS - LAST CASE/SCENARIO	PRIORITY RANKING** MFI	PRIORITY RANKING** MMO	PRIORITY RANKING** MTO	PRIORITY RANKING** FEB
--	------------------------	------------------------	------------------------	------------------------

Comprehensiveness of AML Legal Framework	9			
Effectiveness of Supervision/Oversight Activities	2	1	2	2
Availability and Enforcement of Administrative Sanctions	6	6	7	6
Availability and Enforcement of Criminal Sanctions	8	7	8	5
Availability and Effectiveness of Entry Controls	5	4	5	8
Integrity of Business/Institution Staff	7	3	6	7
AML Knowledge of Business/Institution Staff	1	2	1	1
Effectiveness of Compliance Function (Organisation)	3		3	4
Effectiveness of Suspicious Activity Monitoring and Reporting	4	5	3	3
Availability and Access to Beneficial Ownership information	11	9		10
Availability of Reliable Identification Infrastructure	10	8	9	9
Availability of Independent Information Sources	12	10	10	11

### Recommendations

- The RBM and FIA should provide adequate capacity building to enable enforcement of AML compliance by all OFIs.
- The RBM and FIA should enhance supervision of FEBs, MMOs, MFIs and MTOs.
- Regulators should develop AML / CFT regulations and guidelines for all OFIs
- The FIA should enforce STR reporting by MTOs, FEBs, MMOs and MFIs.
- The FIA and RBM should carry out studies on *hawala*, foreign exchange black market and *katapila* to determine extent of the practices and their impact and see if they can be regulated or how enforcement to end the practice can be done.

## Designated Non-Financial Businesses and Professions Vulnerability

### Background

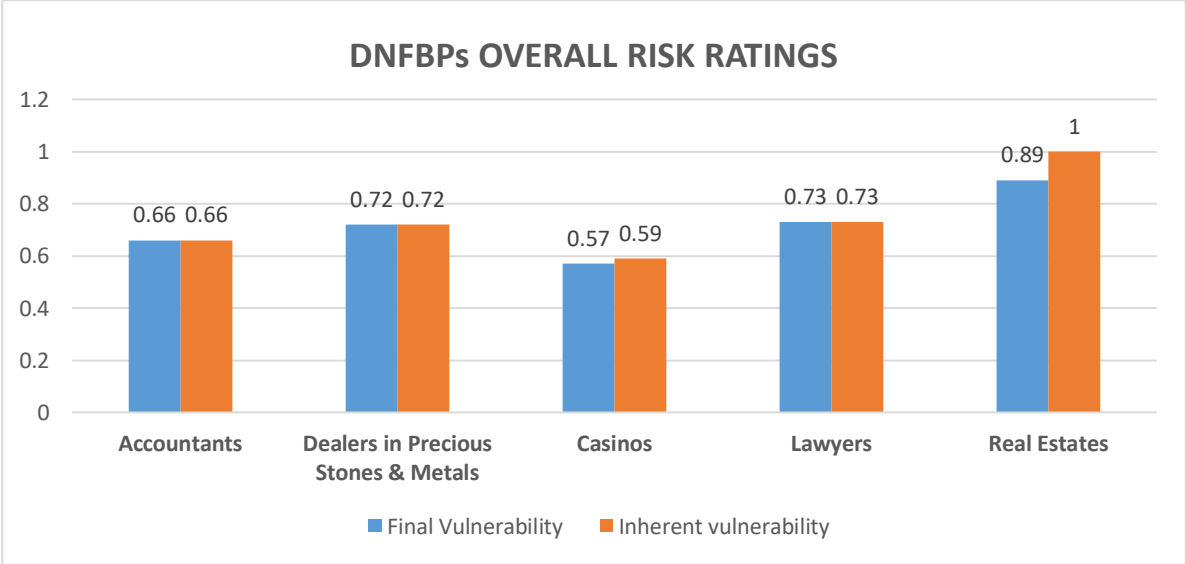
The Designated Non-Financial Businesses and Professions (DNFBPs) which operate in the country are; Casinos, Real Estate, Dealers in Precious Stones and Metals, Lawyers and Accountants. Due to their interface with the financial sector, these professions run the risk of being exploited by criminals

and money launderers who resort to using the non-financial sector to conceal their criminal revenues. In 2013 The DNFBPs were assessed for ML/TF risk and the results revealed that the sectors with the highest ML/TF risks were Real Estates (Very High) and Lawyers (Very High), followed by Accountants (High) then Casinos (Medium) and Dealers in Precious Stones and Metals (Medium). Since the 2013 assessment, FIA has reached out to some of the DNFBPs in terms of raising awareness and sensitisation on AML/CFT requirements and obligations as provided by the FCA.

**DNFBPs Overall Assessment**

The DNFBPs were assessed individually resulting in the following findings; the Real Estates sector has the highest final vulnerability rating of 0.89 (High) followed by Lawyers 0.73 (Medium High) and Dealers in Precious Stones and Metals at 0.72 (Medium High) then Accountants at 0.66 (Medium High) and lastly Casinos at 0.57 (Medium). In terms of inherent vulnerability, the ratings were: real estate at 1.00 (High); lawyers at 0.73 (Medium High); Dealers in precious stones and metals at 0.72 (Medium High); Accountants at 0.66 (Medium High); and Casinos at 0.59 (Medium). The ratings indicate that DNFBPs comprise high risk sector with an average ML/TF final vulnerability rating of 0.71 (Medium High) and inherent vulnerability rating of 0.74 (Medium High).

Figure 4: DNFBPs ML risk



The assessment considered the quality of the AML controls, operations, supervision, policies and procedures and CDD framework, as well as commitment and leadership management and compliance level of staff. The results of the assessment are summarised in the tables below:

Table 18: DNFBP sub-sectors overall assessment

	Accountants	Lawyers and Notary Public	Dealers in precious metals and stones	Casinos	Real Estate Agents
Final vulnerability	0.66	0.67	0.71	0.60	0.89
Inherent Vulnerability	0.66	0.67	0.72	0.65	1.00
Quality of AML Controls	0.29	0.20	0.30	0.46	0.26
Quality of Operations	0.29	0.20	0.30	0.47	0.26
Quality of AML Supervision	0.30	0.10	0.10	0.40	0.20
Quality of policies and procedures	0.42	0.38	0.33	0.46	0.39
Quality of CDD Framework	0.46	0.50	0.54	0.70	0.46
Commitment and Leadership of Management	0.36	0.24	0.30	0.47	0.27
Compliance level of staff	0.30	0.20	0.30	0.50	0.30

Detailed discussions on each sector are reflected below.

## Casinos

### Background

The Casinos and gaming activities in Malawi are regulated by the Malawi Gaming Board (MGB) and the National Lotteries Board (NLB), which are statutory corporations established by The Gaming Act, 1996 and The Lotteries Act, 2003 respectively. Currently, the two organisations operate under merged organisational and operational structure as MGB, even though the law merging them has not been passed. The 2013 NRA established the sector as being Very High risk.

As at 31<sup>st</sup> December 2017, the sector comprised 3 casinos, 2 Wide Area Progressive (WAP) gaming licensees with a total of 29 linked gaming machine sites and 3 standalone gaming machine sites. The gaming industry has a total of 549 gaming machines, 36 gaming tables and over 366 employees. There has been significant growth from 2013 where there were 415 gaming machines, 16 gaming tables and 201 employed in the industry.

Gaming transactions use a combination of both cash and cashless modes. Some machines use cards or tags on which credit for playing machines is loaded. For other machines credit is loaded directly from cash desks. A few have bill acceptors for inputting notes. As for tables, chips can be bought

right at the tables or from cash desks. Casinos also have point of sales devices which are linked to customers' bank accounts, however the bulk of gaming transactions are cash based.

In addition to these gaming outlets, there are also 2 Sports Betting operations with a total of 50 betting shops and over 65 agents countrywide. 461 Malawians have been employed in the sports betting industry. Sports betting was licensed in 2015 and is a relatively new product. Although most of the betting transactions use cash at physical shops or through agents, lately the operators have also introduced an online platform. However, the on-line betting is done at a small scale with payments for the bet and pay-outs being done either through physical shops or through mobile money.

A casino license authorises the holder to operate an unlimited number of slot machines and table games whereas WAP license authorises the holder to operate only slot machines in licensed gaming sites. The machines are linked and run a wide area jackpot. Standalone sites are not linked and do not run wide area jackpots. Gaming machine sites are small operations and are limited to operate a maximum of 10 machines each. A few sites have been given special consideration, due to size of venue, to operate a little more than 10 machines. The WAP license holder may enter into an agreement with a site operator to place machines at the site on a commission basis.

Other lotteries activities available include SMS gaming, raffles and promotional competitions.

Gross Gaming Revenue (GGR) for the 2016/17 financial year for gaming and sports betting was MK4.77 billion (<sup>41</sup>US\$ 6.57 million) representing 15% growth from 2013 (turnover = US\$ 5.72 million). Casinos contributed MK 1.63 billion (US\$ 2.25 million), WAP MK 2.95 billion (US\$ 4.07 million), standalone gaming sites MK 92.6 million (US\$ 127, 661) and sports betting MK 93.3 million (US\$ 128, 641).

### **Casino Vulnerability**

This assessment has established the casinos sector as having a final vulnerability rating of Medium (0.57) and inherent vulnerability rating of Medium (0.59).

The vulnerability assessment considered the following general variables:

#### **a. Comprehensiveness of AML Legal Framework**

The FCA meets most aspects of the assessment criteria in terms of CDD, Record-keeping, EDD for PEPs and high-risk countries, Reliance on third parties for CDD, including introduced business, suspicious transaction reporting, tipping-off and confidentiality, internal controls, foreign branches, and subsidiaries, licensing and supervision for AML compliance. However, subsidiary legislation in the form of regulations are not in place. The existing ML regulations, despite still being in force, are

---

<sup>41</sup> RBM mid-rate as of 8 Dec 2017; 1 US\$ = MK 725.4144

outdated as they were issued in 2011 and do not address some of the changes that have been included in the FCA.

This variable is rated Medium High (0.7).

**b. Effectiveness of Supervision/Oversight Activities**

The FIA has been supervising the sector on AML matters while MGB has supervised on prudential matters. The AML supervision has not been on a risk-based approach as focus has been more on raising AML awareness and ensuring that the sector has established AML compliance functions. To this effect, FIA conducted 2 covert visits at one casino and one gaming house between 2013 and 2016. In 2017 FIA and MGB jointly conducted 12 AML inspections.

While FIA has well trained staff, it has experienced staff shortages which has resulted in inadequate AML supervision of the sector. MGB conducts monthly prudential visits on the sector but does not have staff that are adequately trained in AML matters and therefore has not included AML issues in its supervisions. As such, the FIA and MGB are in the process of signing a Memorandum of Understanding which will ensure proper coordination of AML supervision.

This variable is rated Medium (0.5).

**c. Availability and Enforcement of Administrative Sanctions**

The Financial Crimes Act has provided for administrative sanctions in the form of monetary penalties, warnings and loss of business license which are sufficient to influence change in the gaming industry's management and behaviour. The sanctions have been communicated to operators in the industry during training workshops and feedback attests to sufficiency. For instance, following one sensitisation workshop, WAP licensees requested that gaming sites operating under them be licensed separately so that each gaming site should be responsible for their own shortcomings and penalties. There is no record of administrative enforcement actions taken in the past regarding non-compliance with AML requirements in the sector since the law was revised recently and the regulations on administrative sanctions are yet to be finalised and implemented.

This variable is rated Medium (0.5).

**d. Availability and Enforcement of Criminal Sanctions**

Criminal sanctions are available under the FCA. The sector has been sensitised about criminal sanctions under the FCA through workshops. The criminal sanctions are applicable for the offense of money laundering as well as non-compliance. Most persons working in the sector believe that criminal enforcement action would be initiated in case of non-compliance with AML requirements. Despite there being no enforcement of criminal sanctions on AML issues, four illegal operators (3 cases in 2015 and 1 case in 2016) were taken to court and were found guilty for operating without

a license. Their machines were confiscated and disposed. No other cases apart from the unlicensed operators have been taken to court.

This variable is rated Medium (0.5).

**e. Availability and Effectiveness of Entry Controls**

MGB is empowered by section 5 of the Gaming Act to issue gaming licenses whereas sections 21 and 36 of the Lotteries Act empowers the National Lotteries Board to license the national lottery and other lotteries. The Board carries out a thorough evaluation and selection process when licensing entrants. The first stage is to call for applications (regulation 13). Applicants are required to comply with licensing requirements listed down in a Request for Proposals (RFP) document. The next stage is evaluation and selection where among others, the Board scrutinises the applicants (shareholders, directors and such other personnel are required to fill out Personal Declaration forms and a Company Release Authorisation) and sources of their finances. Audited accounts for previous 5 years are required to establish track record and support declaration of financing arrangements. The last stage is for board of directors to consider recommendations by the evaluating team and award license to the successful applicant.

Section 5 (3) of the Gaming Act empowers the Board to issues licenses where it has satisfied itself that the applicant is a fit and proper person to hold the license. Regulation 15 (1) stipulates that the Board may refuse a license if it is not satisfied that the applicant is not fit and proper, not a person of good character and integrity, not a person of good financial standing, an un-rehabilitated, insolvent, is a minor is of unsound mind, or has within the last seven years been removed from an office of trust on account of misconduct. However, requirements are not comprehensive in terms of criminal tests and beneficial ownership. Regulation 32 (3) requires licensees not to employ key employees until the prospective employees have applied for and been granted registration as key employees by the Board. The registration is extended to directors (Reg. 32 (1) (b)). Employees seeking registration with the Board are required to undergo police screening as a prerequisite to the registration process. The FCA has placed obligations on the sector for all licensees to have adequate AML compliance controls in place. The Board is well resourced in terms of personnel and financial resources to implement entry controls. When evaluating applications, teams involving members from different departments are assembled to handle such projects.

This variable is rated Medium High (0.6).

**f. Integrity of Business/Profession Staff**

Slot machines are connected to a monitoring system which records and monitors the activities on all machines exposed to play (Regulation 55). Conduct of table games, which are viewed to be high risk due to human interaction, is specified in 'casino manuals'. For instance, there are procedures for; surveillance monitoring and recording of all transactions (Regulation 52, 53, 54). Breaches or



suspicious activities are reviewed by surveillance department and concerned staff disciplined accordingly. Rotation of table dealers (normally every 20 minutes) disrupts any staff – customer collusion, as well as floor supervisors (Pit Bosses) that check and verify transactions. There is also a manner of cashiering known as ‘Clean Hands’ cashiering where dealers display chips and money received or paid out for clear view of surveillance cameras as a control mechanism.

Between 2013 and 2017, there were only two reported cases involving staff theft, which were reported to the Police. Such cases are rare and are usually concluded by dismissing staff involved. Regulation 32 (4) stipulates that a licensee shall, within 14 days of termination of the employment of a key employee, notify the Board in writing of such termination and the reasons thereof.

This variable is rated High (0.7).

**g. AML Knowledge of Business/Profession Staff**

Most gaming houses are aware of their obligations. The setback is that most small gaming establishments which account for a significant portion of the industry do not employ officers with prerequisite skills sets to satisfactorily drive AML/CFT programmes. The FIA and MGB have since 2012 conducted several training workshops for the sector. In July 2016 a training workshop was held for Director / Senior Management and their Compliance Officers to guide them in setting up a compliance function within their operations. The training workshops targeted the directors, senior management, and compliance officers with a view that they would pass on the knowledge to relevant staff within their businesses. Involvement of directors and senior management was also to ensure buy-in and eventual support of the AML compliance function.

This variable is rated Medium (0.5).

**h. Effectiveness of Compliance Function (Organisation)**

AML Compliance Programs are in place but not very effective due to capacity challenges of responsible officers. Some operators have just started reporting LCTRs. Most operators have put in place AML compliance programmes, however, most of them (especially small operators) are not properly functional. Further to this, there seems to be some reluctance by some of the operators to comply with AML/CFT requirements. Most small operators appoint junior officers (Cashiers) who are not appropriately qualified and lack independence. This is sometimes due to organisational structures having flat hierarchy whereby from owners of business next are the cashiers who are not senior. No disciplinary action against staff has been reported / registered for breaches of AML related matters. Internal and/or external AML audits have not been performed by any of the sector players.

This variable is rated Low (0.3).

**i. Effectiveness of Suspicious Activity Monitoring and Reporting**

Systems are available for monitoring and reporting transactions. Operators have casino management systems (slots accounting systems) in place most with capabilities to monitor and record client transactions. However, they have not been configured for AML monitoring as such, they are mostly being used to compute gaming revenues. Transactional records are available but not in a format that facilitates AML screening and monitoring, which would require time to process. Casinos use 'day cards' for uploading credit for playing on machines and for cashing out. However, transactions for a particular card cannot be traced to an individual person as they are not personal to holder. Some systems require players to pay or to redeem cash at a Cashier's desk (computer). History logs therefore show transactions per machine per given time and not transactions per individual customer. There are no specific systems in place for determining PEP status of customers. Firms rely on declared information when registering their customers with the house or rely on public information. Payouts in excess of K1 million are usually made by cheque indicating the bearer's name. However, for buy-ins firms rely on cashiers to note large transactions. Due to continued business relations operators tend to personally know their clients. Cashiers have been advised to use such knowledge to update customer registers in view of reluctance by some customers to divulge personal details. With such personal relationships, gaming houses can form suspicion when unusual behaviour is displayed and send STRs. FIA installed the reporting software, TrueCrypt at gaming houses and oriented responsible officers how to use the encrypting software for submitting STRs. Some gaming houses have started sending LCTRs to FIA. The sector has not yet started submitting STRs.

This variable is rated Low (0.5).

**j. Availability and Access to Beneficial Ownership Information**

The issue of access to beneficial ownership information has been addressed in the FCA. Casinos and gaming houses can access beneficial ownership information from their customers using the available CDD measures. However, the challenge is that KYC information is not readily available, let alone beneficial ownership, especially in cases where people play or bet on behalf of others. This variable is rated Medium High (0.6).

**k. Availability of Reliable Identification Infrastructure**

Casinos and gaming houses are able to identify customers using IDs such as passports, driving licences and voter registration card. However, the passports and drivers' license have been prone to forgery and abuse. The national identification system is also currently being implemented and it is expected that the introduction of the national ID will help mitigate the problems posed by the other identification documents. This variable is rated Medium (0.5).

**l. Availability of Independent Information Sources**

Casinos and gaming houses can verify information through independent sources such as the credit reference bureau, the Immigration Department and Road Traffic Directorate. However, the

challenge is that customers transact in secret as they do not want their gambling / betting habits to be known. Therefore, in most cases they do not wish to be identified. This variable is rated Medium (0.5).

### *Inherent Vulnerability*

The number of operators in the industry and revenue generated was deemed low to pose significant ML risk. There are no indications of illegal operators at the moment.

Clients that use casinos and gaming houses were deemed medium risk in terms of money laundering abuse. The casino clients include members of parliament, senior officials, business owners and senior managers. The number of tourists visiting the casinos and gaming houses is insignificant. There is no data on clients with foreign business or personal interests, clients with business links to known high-risk jurisdictions and Clients with criminal records or past administrative and/or supervisory actions against them

Gaming is a high cash intensive business. Use of cash is permitted and level of use is high however winnings in excess of K1 million are usually paid out through cheques as part of internal controls, and in this regard, most venues maintain a limited amount of float.

Use of agents is Low as it is non – existent in casinos and gaming houses, but available in sports betting. ML risk in sports betting was deemed insignificant due to low levels of bets processed. Anonymous use of the product is available but limited to online sports betting only which currently is being used minimally. Other gaming/ betting modes require physical interfacing with customers.

Tracing transactions to individual customers is difficult in most gaming venues, except in few instances like jackpot pay-outs where full details are recorded. For customers with customised cards, casino management systems are also able to keep transaction trails. WAP sites use a system whereby a customer pays the cashier who electronically transfers credit into machines. This system does not connect a transaction to a particular customer.

There are no known cases of the sector having been used for fraud or tax evasion in Malawi and there are no local typologies of money laundering in the sector. However, there are typologies at an international level. For instance<sup>42</sup>:

#### **Case 1. Casino used as preferred method to launder millions**

**Offence:** Money Laundering      **Jurisdiction:** Australia

---

<sup>42</sup> Vulnerabilities of Casinos and Gaming Sector – March 2009

**Technique:** Chip purchase and cash out, claiming credits as jackpot wins, playing games with low return and high win.

**Mechanism:** Casino                      **Instrument:** Casino chips, casino cheques

Information identified alleged money launderers using the casino as a preferred method of laundering millions of dollars accumulated from criminal activities. The methods used to launder the money included purchasing and cashing out chips without playing, putting funds through slot machines and claiming credits as a jackpot win and playing games with low returns but higher chances of winning. The same group were also utilising bank accounts and businesses to launder funds.

### Case 2. Loan-sharking profits laundered at casino

**Offence:** Money laundering                      **Jurisdiction:** Japan, United States

**Technique:** Purchase and cash out with little or no gaming activity

**Mechanism:** Casino                      **Instrument:** Cash, casino chips, casino credit

A boss of a loan-shark business ordered his associates to convert the profits from Yen into US currency using false names. These funds were then distributed to numerous bank accounts around the world. Some of the money was also invested with a foreign agent of a Las Vegas casino, who kept the money in a safety deposit box in the head office of a major Tokyo bank. Against the security of this money, the boss played frequently at Las Vegas casinos as a VIP player. Although he gambled in the VIP room, he would never place big bets and, after minimal play, would frequently cash in his chips for US currency. His associated were also circulated through a number of Las Vegas casinos cashing in chips worth USD 2 000 or less.

There has been some illegal gambling in the sector, however, this has been low. Between 2013 and 2017, some illegal gambling operators were arrested, taken to court and their operations closed down. For instance, in one incident, 3 Chinese nationals were found guilty and fined by the courts for operating sixty – six (66) illegal gambling machines, which were seized and destroyed. In 2016, nine (9) machines were seized and the offender taken to court. It was discovered that in almost all such cases, the machines came from Zambia and belonged to Chinese businessmen who were seeking to expand into new markets. Apparently, there is no autonomous licensing authority for gaming in Zambia as the offenders indicated that they obtain licenses from the Zambian City / Town councils. The illegal machines were small garage-made machines with very low bets / pay-outs which do not pose significant ML threats.

Non – face – to – face interactions are available only with online betting which is not wide spread and viewed to be low risk due to limited accessibility and low betting amounts. For online bets over K20,000 cashiers have to seek authorisation before processing and such bets are not common. Online betting is restricted to live games whose results are not instantaneous.

## Dealers in Precious Metals and Precious Stones

### *Background*

Dealers in Precious Metals and Precious Stones in Malawi are regulated under the Mines and Minerals Act 1981 and the Mines and Minerals Policy 2013. The sector is regulated by the Department of Mines. The Ministry of Natural Resources, Energy and Mining (MNREM) requires all players in the sector to obtain licenses based on different activities they carry out.

The mining sector in Malawi falls under large-scale or small-scale operations. Mining licenses are awarded on a 'first come first served' basis. The sector comprises both registered and unregistered operators and there are 268 mineral license holders registered with the Department of Mines. Artisanal and small-scale miners (ASM) are also engaged in prospecting, gemstone mining, rock aggregate crushing, lime production, ceramics and pottery and salt processing<sup>43</sup>. A study of ASM in 2001 estimated that some 40,000 Malawians are engaged in the sector however, this number has to be treated with caution because the activity is in most cases is seasonal and periodic depending on when gemstone rushes occur<sup>44</sup>. Most of the ASMs fall under either the Malawi Women in Mining Association (MAWIMA) or Gemstones Association of Malawi (GAM)<sup>45</sup>. MAWIMA has about 70 registered members. There are also cooperatives involved in mining, whose number is yet to be established. Apart from those engaged in mining, some are simply 'collectors' who collect precious stones and sell them, whether in raw or processed forms.

### *Importance of the Sector*

Malawi is a smaller producer of uranium, gemstones, limestones, bauxite, bituminous coal, and rock aggregate. The rock aggregate account for 56% of the production in 2015. The Government is promoting investment in the extractive industries to make the sector contribute up to 20% of the country's GDP by 2020. According to Malawi Extractive Industries Transparency Initiative (MWEITI) 2014/15 report, total revenue for the extractive sector was MK5,935-million (USD13.6-million) of which 40% came from solid minerals. Mining sector contributed 0.9% to Malawi's GDP in 2014. In total, the small extractive sector contributed 1% to Government revenue and 0.6 to exports. <sup>46</sup>. Mining is important in Malawi because of its potential to significantly contribute to Malawi's Gross Domestic Product (GDP).

### *Vulnerability Assessment*

Specific findings of the assessment on dealers indicate final vulnerability rating of 0.72 (Medium High) and inherent vulnerability rating of 0.72 (Medium High).

#### **a. Comprehensiveness of AML Legal Framework**

---

<sup>43</sup> Mines and minerals policy, 2013

<sup>44</sup> World Bank, 2009

<sup>45</sup>Tilitonse, 2013

<sup>46</sup> <https://eiti.org/malawi>

The FCA has adequately addressed AML issues related to DPSM. Sections 16-34 of the FCA provide guidance on customer due diligence processes for every reporting institution and require entities to keep records and give guidance on the type or records as well as length of period for keeping the records, identification of PEPs, conducting risk assessment, reliance on third parties for CDD and require supervisory authorities to ensure there are adequate internal controls in reporting institutions. However, subsidiary legislation in the form of FCA Regulations are in draft form. Despite this, the ML Regulations of 2011 are still in force.

This variable is rated High (0.7).

**b. Effectiveness of Supervision/Oversight Activities**

Before the enactment of the FCA, the Ministry of Energy, Mines, and Natural Resources had an AML/CFT supervisory role in accordance with the ML Act, but since there was no formal engagement with the FIA, it was difficult for the Ministry to act accordingly on AML/CFT matters hence there was no supervision. The enactment of the FCA changed the supervisory regime in that it mandates the FIA as the supreme supervisory authority on AML/CFT matters. As the supreme supervisory authority, the FIA can delegate its supervisory authority through a clearly laid out framework, which is currently not in place. While the FIA has well trained and knowledgeable staff, it has few staff and inadequate financial resources to carry out its supervisory work effectively. In addition, the FIA is yet to commence both on-site and off-site risk-based monitoring for the sector.

This variable is rated Close to Nothing (0.1).

**c. Availability and Enforcement of Administrative Sanctions**

The FCA (Section 34) provides for a wide range of administrative sanctions which include; written warnings, monetary penalties and publicising the non-compliance and penalty meted out. The FCA also recommends enforcing of sanctions under respective laws governing the contravening individual. However, FIA is also in the process of drafting regulations to guide the implementation of the administrative sanctions.

This variable is rated Medium (0.5).

**d. Availability and Enforcement of Criminal Sanctions**

The FCA has made provisions for criminal sanctions which are proportionate and dissuasive and are applicable to both natural and legal persons. However, these have not yet been tested.

The assessment established that the MPS has handled cases of people trying to export minerals without export licenses, mixing stones and other illegal items like ivory in an export consignment and people bringing in precious stones from other countries to export through Malawi because the 'borders are considered porous'. However, there has never been a case linked to ML or TF.

This variable is rated Medium (0.5).

**e. Availability and Effectiveness of Entry**

The Department of Mines, which is under the Ministry of Energy, Mining and Natural resources is responsible for registering dealers in precious stones and metals. This Department of Mines has laid

down procedures for processing of applications and granting of mineral right in accordance with the Mines and Minerals Act, 1991. These are categorised as large and small scale mineral license. The Mines and Minerals Act is very old and therefore has not addressed ML/TF issues. The criteria for getting licenses does not guarantee prevention of criminals or their associates from being granted a business or professional license or being the beneficial owner of a significant controlling interest in the business or holding a significant management position.

This variable is rated Medium (0.5).

**f. Integrity of Business/Profession Staff**

The Department of Mines largely regulates how players comply with pieces of legislation and conditions of their licenses – the mandate is limited to this. Staff in the Department is subject to the code of ethics for the public sector. There is however no information at the moment on staff vetting programmes, incidences of disciplinary action for breach of integrity and number of cases against staff members in the sector. Section 10 of the FCA provides a mechanism for protecting those who report suspicious transactions or other actions to comply with AML obligations in form of prohibiting disclosure of the identities of such individuals.

This variable is rated Medium Low (0.4).

**g. AML Knowledge of Business/Profession Staff**

FIA is yet to engage the sector through provision of tailor-made training on AML/CFT issues as such there is less knowledge in the sector. The Ministry and the Department of Mines have not been sensitised on AML/CFT provisions as such do not have adequate knowledge on these issues.

Subject to the availability of funds and sponsored training, players undergo different trainings in the mining sector but not those that deal with AML exclusively.

This variable is rated Very Low (0.2).

**h. Effectiveness of Compliance Function (Organisation)**

There are no compliance programmes or compliance officers in the associations or government departments engaged so far. The sector has not been sensitised on its obligations under the FCA. Audits for the government department are done by NAO but are not focused on AML but rather on how the department uses its funds.

This variable is rated Close to Nothing (0.1).

**i. Effectiveness of Suspicious Activity Monitoring and Reporting**

The sector has not been sensitised on its AML/CFT obligations, as such there are no reports (LCTRS and STRs) submitted to FIA.

This variable is rated Close to Nothing (0.1).

**j. Availability and Access to Beneficial Ownership Information**

The FCA has addressed the issue of beneficial ownership. However, this is a fairly new concept for the Mining sector as many are not aware of their AML/CFT obligations and have not been adequately equipped to identify their clients or conduct proper KYC/CDD/ECDD.

Under the MWEITI, the country has a goal of promoting beneficial ownership transparency in the sector through supporting efforts to address ML and other financial crimes in the economy, and promoting good governance and accountability in the sector, among others<sup>47</sup>.

This variable is rated Close to Nothing (0.1).

#### **k. Availability of Reliable Identification Infrastructure**

The Malawi Government has just introduced a national identification system, which has not yet been fully implemented. Passports and drivers' Licenses are the most reliable ID document with other forms of identification used by the sector being voter registration cards and letters from the village headmen. The latter two identification documents are easily prone to abuse. It is envisaged that the National ID will ease identification challenges once fully implemented.

This variable is rated Medium High (0.6).

#### **l. Availability of Independent Information Sources**

Although there are independent and reliable sources of information to determine transaction patterns of clients such as commercial history from Banks, former employers' reference, former employers, and utility bills, among others. Most entities that can provide independent sources of information which should be public knowledge, such as the Registrar of Companies and the National Credit Bureau are not readily accessible as it is time consuming to get information from them. In addition, some of these entities require payments to release information. It is therefore not easy to access comprehensive and reliable historical financial information and other information about clients.

This variable is rated Medium (0.5).

#### **m. Inherent Vulnerability**

The size of the business is medium as there are 250 officially registered miners with the Department of Mines but approximately over 40,000 Malawians are engaged in mining activities whether registered or not. This increases the vulnerability of the sector to the ML/TF threat. The law however is clear that no-one should engage in mining without a license. The Client base profile of the business/profession is high risk as domestic/international PEPs, high net-worth individuals, non-resident clients from various jurisdictions, clients with foreign business or personal interests, clients with business links to known high-risk jurisdictions, are in one way or the other engaged in the sector as buyers or agents whether legally or illegally hence the high-risk rating.

There is a medium level of cash activity associated with the business/profession because many small-scale and artisanal miners prefer cash transactions to subsist on. Use of agents is Medium Low, there are associations and individuals who act as agents. Possible anonymous use of the

---

<sup>47</sup> <https://eiti.org/malawi>, Beneficial ownership disclosure



product in the business/profession is available in that a person can purchase a precious metal or stone on behalf of another person or company. Tracing the transactions is difficult and time consuming considering that there are unregistered players in the sector and Malawi is a cash economy. The sector could be used in fraud or tax evasion schemes considering that there exists illegal dealing in mining.

ML typologies on the abuse of the business/profession exist. Below are examples of how the sector can be abused by criminals. These examples are not specific to Malawi but similar scenarios dealing with precious metals and stones found in the country are possible.

**Typology 1:**

**offence:** Money Laundering

**Dealers related offence:** N/A

**Jurisdiction:** N/A

**Subject:** Individual

**Instruments methods and techniques:** Jewellery

**Indicators:** Purchase of Jewellery using proceeds of crime

**Case description: Diamonds are a Launderer's Best Friend**

A lawyer of Country Y absconded with millions of US dollars from his "customer escrow" account. Investigations revealed that part of these funds was used to purchase loose diamonds and jewellery from a local jeweller in Country Y.

This case illustrates the use of direct purchase of precious stones to launder the crime proceeds. In particular, it shows the way for an absconder to conceal and move the proceeds of crime across different countries<sup>48</sup>.

**Typology 2:**

**Jurisdiction:** N/A

**Subject:** Company

**Instruments methods and techniques:** Payment for Jewellery through companies and banks

**Indicators:** splitting of payments through different companies and banks

**Case description: Limited Edition Jewellery**

Expensive Jewellery Limited (EJL), a foreign firm active in a small jurisdiction, noted that it was attracting an increasing number of very affluent customers. The owners of EJL considered that, in the same way there was a market in the jurisdiction for prestige, limited edition cars, there was also a market for very expensive, limited edition jewellery and forged business links with foreign firms to market high value jewellery. Occasionally, selected customers were invited to the jurisdiction to attend viewings. Sometime after it developed this new business line, EJL auctioned a diamond necklace. The necklace was sold for a sum in excess of £1 million to a buyer who was represented at the auction by his agent. Payment was made to the auctioneer's bank account as agreed. The bank informed the auctioneer that the £1million had been received but payment had been made from different companies via three different banks in different jurisdictions.

---

<sup>48</sup> FIU of Trinidad & Tobago's guidance notes for dealers in precious stones and metals

This information led the auctioneer to think that all was not quite right with this purchase and he made a disclosure to the local financial investigation unit. It was discovered through intelligence that the agent and his customer had drug trafficking convictions and were suspected of several frauds and laundering the proceeds of their own and other

#### n. Other Vulnerable Factors Including Illegal Mining

While section 2 subsections 3 & 4 of the Mines and Minerals Act 1981 prohibits mining without license, illegal mining activities still take place in the country. According to the Department of Mines, most problems with illegal mining are with the artisanal and small-scale mining sub-sector, who operate without licenses mostly in very rural or remote areas where the Department has challenges to inspect. There have been many cases of illegal mining for example, the gold rush in Makanjira, Mangochi, where about 300 unlicensed miners started mining alluvial gold along Onga River. Such cases are rarely documented. Illegal mining is rated at Medium (0.5).

### Lawyers

#### Background

The legal profession is regulated by the Malawi Law Society (MLS). As of 2017, the MLS had membership of 407 licensed lawyers (excluding those employed in government and have not been licensed) and 33 licensed firms. Out of 407 legal practitioners, 123 are employed in companies whereas 284 are working in law firms (as managing partners or employees). The number of legal practitioners varies from year to year as each year new lawyers are admitted to the bar (the profession). On average, about 40 people have been admitted to the bar every year for the past 3 years.

Once a legal practitioner is admitted to the bar, he or she becomes a general practitioner. He or she can practice in almost every type of work, be it in facilitating transactions in sale or buying of real estate, registration of business entities, creation of trusts and wills, etc. All law firms are involved in management of clients' funds held in bank accounts. There are a few law firms that are specialised in purely commercial transactions.

#### Vulnerability Assessment

Based on the assessment, the sector has final vulnerability **0.73 (Medium High)** and inherent vulnerability **0.73 (Medium High)**.

#### a. Comprehensiveness of AML Legal Framework

Lawyers are identified as DNFBPs under the FCA, which recognises legal practitioners and other legal professionals as reporting institutions for AML/CFT obligations. The FCA has adequately addressed issues related to risk assessment, establishment of a compliance function, client identification and verification, KYC/CDD, record keeping, PEPs, transaction monitoring and submission of LCTRs and STRs, independent testing of the compliance function, confidentiality, staff training and awareness, as well as staff screening. Further to this, the FCA has provided for both administrative and criminal sanctions. However, relevant subsidiary legislation, in the form of

Regulations, are currently in draft form. Despite this, the existing ML Regulations of 2011 are still in force.

This component is rated High (0.7).

**b. Effectiveness of Supervision/Oversight Activities**

The FIA is the overall supervisor on AML issues. However, section 35(2) of the FCA gives the FIA powers to delegate these supervisory powers. As at 30<sup>th</sup> December 2017, the FIA had not reached out to the lawyers and therefore had not conducted any supervisory work with the sector.

This variable is rated Close to Nothing (0.1).

**c. Availability and Enforcement of Administrative Sanctions**

Section 5 of the FCA empowers the FIA to impose and enforce administrative sanctions for breach of the Act. Under section 34, these include a written warning, a direction to do or refrain from doing certain acts, an order for compensation, publication of the non-compliant institution in a newspaper of widest circulation (naming and shaming), and recommending to the supervisory authority or self-regulatory body for sanctions under the respective law governing that person as a professional or employment or business authority misconduct. If enforced, these sanctions could deter or at least reduce incidents of further breach of the Act. However, these sanctions have never been tested.

The above is an indication that, as a legal profession, there is political will to enforce discipline or compliance with ethics. If the FIA goes ahead to delegate to the Society, the Society will be in a position to enforce compliance with the FCA.

This variable is rated Medium Low (0.4).

**d. Availability and Enforcement of Criminal Sanctions**

The FCA has a comprehensive legal framework that creates offences and provides for criminal sanction for non-compliance with the Act. No criminal sanctions have been imposed on lawyers for violating the FCA. However, there are three (3) lawyers who are suspected to have been involved in the *cash-gate* scandal. These lawyers have since been charged under the old ML Act and their cases are in court.

This variable is rated Medium (0.5).

**e. Availability and Effectiveness of Entry Controls**

There is a clear and comprehensive framework for entry into the legal profession. The Legal Education and Legal Practitioners' Act (LELP) provides for qualifications required for one to practice as a legal practitioner in Malawi. While the Act provides for recognition of qualifications obtained from foreign jurisdiction, not every jurisdiction / qualification is acceptable. In a way, therefore, this performs a sieving process in terms of who can practice law; it largely restricts foreigners from practicing in the country hence minimizing incidents of misconduct.

For legal practitioners to practice, they are required to have an annual license issued by the Registrar of the High Court. However, for the license to be issued or renewed, one needs to pay membership subscription fee to MLS. The MLS makes a recommendation to the Registrar to issue a license. Thus, if the Society makes a recommendation that a license should not be renewed, the Registrar would not renew it. This also acts as a control measure.

This variable is rated Medium Low (0.4).

**f. Integrity of Business/ Profession Staff**

The MLS has a Code of Ethic, which is enforced by a Disciplinary Committee. When renewing a license, each private practice lawyer has to submit an accountant's certificate and a tax clearance certificate issued by the MRA. Because of the involvement of the MRA and accountants, the process for license renewal ensures a measure of integrity. Further, the Society does not recommend renewal of license where a lawyer fails to produce audited accounts or has defaulted in tax compliance and does not have a tax clearance certificate from MRA. Nonetheless, we have cases of lawyers defrauding clients or being involved in illicit transaction, such as *cash-gate*.

There have been cases of integrity breaches by lawyers and in a year, the Disciplinary Committee hears close to 40 cases of complaints against lawyers. In 2017, the Committee heard 35 complaints against lawyers and made relevant recommendations. Most of the cases heard in 2017 had to do with non-remittance of clients' funds.

The jurisdiction of the Committee is to hear cases of misconduct or unprofessionalism not necessarily cases of violation of AML, although in handling such cases it is possible to also tackle some issues covered under the FCA.

There have also been a few cases of lawyers struck off the bar. In one case, *Jassan and Others Vs Telecom Networks (MW) Limited Civil Appeal No.7 of 2008* a lawyer, Mr. Christopher Chiphwanya, was in September 2016 struck off the bar (disbarred) by the High Court for abandoning his law firms/ his clients.

This variable is rated Medium (0.5).

**g. AML Knowledge of Business/ Profession Staff:**

There has been no AML awareness or training for lawyers and legal practitioners during the period under review as the FIA is yet to reach out to the lawyers. However, In September 2017, the FIA trained law students on AML issues as a way of sensitizing them of the FCA. While MLS conducts trainings for its members (legal practitioners) as part of continuing professional development, this has not extended to AML issues. However, MLS has organised the 2018 Annual Conference to be held in February 2018 and has invited FIA to raise awareness of the FCA and its obligations. The theme is 'the Malawian Lawyer in the 21<sup>st</sup> Century', whose aim is to equip lawyers with knowledge of current trends/issues in the law and the profession. Hence inclusion of the FCA, being a new Act whose contents are not known by most legal professionals.

This variable is rated Very Low (0.2).

**h. Effectiveness of Compliance Function (Organisation):**

Most law firms do not have internal AML compliance programmes that are commensurate to the level of the risk of the firms, taking into account factors such as jurisdictions of end user and professional intermediary clients, clients that are complex or opaque legal structures, the volume and nature of products provided; client-base profile transaction patterns and cross-border nature of transactions.

Further, most have not appointed a sufficiently-resourced, independent AML compliance officer at senior management level. Some do not take disciplinary actions against their staff in cases of breaches of compliance policy. Most firms perform internal and/or external audits, but these do not extend to AML audits.

This variable is rated Very Low (0.2).

**i. Effectiveness of Suspicious Activity Monitoring and Reporting:**

Most law firms do not have information systems that enable and facilitate the monitoring of client transactions and comparing them against the client's profile. There is very little attempt by law firms to verify the client profile provided to them.

This variable is rated Close to Nothing (0.1).

**j. Availability and Access to Beneficiary Owner Information**

Beneficiary information is available and accessible. The issue of access to beneficial ownership information has been addressed in the FCA. Lawyers are able to access beneficial ownership information from their clients using the available CDD measures.

This variable is rated Medium High (0.6).

**k. Availability of Independent Information Sources**

There are licensed credit reference bureaus operating in Malawi and lawyers can obtain credit information from these. The credit bureaus also provide independent information which lawyers can source. However, this is at a fee and in addition, the National Credit Bureau is still in its infancy hence there is inadequate information to facilitate decision making or verification of concrete information. Lawyers can also use utility bills to supplement customer details.

This variable is rated Medium (0.5).

**l. Availability of Reliable Identification Infrastructure**

MFIs use reliable identification documents such as passports and driving licenses. However, the majority of customers, especially those living in rural areas, do not have the passports or driving licenses. For such customer, reduced KYC is used instead and the customers are allowed to use other IDs such as Malawi Electoral Commission voter registration card, letters from the chief/village headman and unverifiable employer IDs. Nevertheless, the rolling out of a national identification system is underway and will address the challenge.

In this regard, the variable is rated Medium (0.5).

**m. Inherent Vulnerability**

The inherent vulnerability is rated Medium High (0.73) and this has been based on a number of variables including size, client base profile, level of cash activity, anonymous use of the services, use of agents and availability of ML typologies.

Total Size/ Volume of lawyers and legal practitioners is considered Medium. As of 2017, MLS had 407 licensed members. However, there are also other legal practitioners that have not renewed their annual licenses. In total the Society has about 440 legal practitioners.

The client base profile is rated medium risk. Legal practitioners offer a number of products including drafting of contracts, preparation of documents for establishment of companies (articles of association and memoranda), drafting of trusts, preparation of documents for obtaining letters of administration, documents for sale or transfer of land or movable property, etc. Almost every legal practitioner is involved in these products, except for those employed in Government. A single lawyer, in a year, handles more than 100 files/products.

Level of cash activity is rated High because the majority of clients for legal practitioners are local people who are unbanked and do pay cash for legal services. Even those banked prefer to pay cash rather than cheque. A few clients are companies and business which pay by cheque for their records. Legal practitioners almost always pay to their clients by cheque.

The use of agents is Low. Use of agents is there but is not encouraged. People use agents in personal injury cases who solicit clients for lawyers but it is not allowed. Law firms normally do not use agents.

Anonymous use of the product is not available. The only exception is that under our law, a client may be known to the legal practitioner but there is no obligation to bring the client to court for the court to verify the existence of the client. Thus, a legal practitioner can commence litigation in the name of a client and even if people question the existence of the client there is no way of knowing whether the name has just been cooked up or there is indeed a client.

It is easy to trace transaction records of the sector as lawyers keep records of their clients. Non-face-to-face use of the product of the business profession does not exist.

Fraud and tax evasion schemes exist in the sector. There are no ML typologies on the abuse of the business profession in Malawi but such typologies from other countries do exist. The following is an example on one such typology:

**Typology 1:**

**Jurisdiction:** United States

**Subject:** Company

**Case Description:**

The US attorney Mr. P was convicted on a federal charge of money laundering for handling \$177,500 in cash from a former client who is now facing prison for drug offences. Before the money laundering allegations came to light, Mr. P served as defence attorney and had a lucrative side business as an agent for professional hockey players. Mr. J, the attorney's client, was targeted in a federal investigation in 2012 after authorities learned of his involvement in a large-scale drug OC smuggling operation spanning from California to Maine. The laundering was done through smurfing and during the investigation Mr. P admitted that when he received more than \$10,000 from Mr. J at one time, he broke up the deposits into amounts under \$10,000 to avoid the currency reporting requirements, which was in violation of (federal law). The money was deposited into the attorney's escrow account and subsequently, cashiers' cheques were issued based on those deposits and used to partially cover the price of real estate bought jointly by Mr. J and Mr. P. Although the real estate was bought jointly by Mr. J and Mr. P, they intentionally removed J's name from the paperwork toward the end of the transaction. To explain the smurfing, Mr. P stated he did not want to file paperwork regarding the deposits. In addition to the above, Mr. J purchased an interest in a sports agency owned by Mr. P for \$250,000 paid in instalments of \$50,000 in cash, all delivered in backpacks. Mr. P was convicted for money laundering and imposed a fine of \$500,000.

## Accountants

### Background

Accountants in Malawi work across different sectors of the economy. Their activities are regulated by the Malawi Accountants Board (MAB) and supervised by the Institute of Chartered Accountants in Malawi (ICAM) as mandated by the Public Accountants and Auditors Act 2013 (PAAA) (Sec.26 (1) and Sec.40). Before the enactment of the PAAA 2013, the accountant profession was regulated by the Society of Accountants in Malawi (SOCAM), which had almost no control or mandate over accountants in case of unethical behavior. Accountants are required to abide by the international code of conduct for professional accountants of the International Federation of Accountants (IFAC).

Section 16(1)(d) of the PAAA 2013 gives MAB powers, with delegated powers to ICAM – Sec.16(3), *“to take such steps as appear necessary or desirable to advance the standing and effectiveness of the accountancy profession in Malawi”*. This Act also requires mandatory registration with MAB and ICAM of any person performing accountancy duties in Malawi. As at November 2017, there were an estimated 1,855 registered accountants and 275 pending applications. The number of unregistered accountants cannot be estimated reliably.

### Services Offered by Accountants

Accountants perform a range of tasks in accordance with International Financial Reporting Standards and International Standards on Auditing and Assurance Engagements that include, but not limited to:

- Preparation of financial statements – this involves maintenance of financial records and reporting financial results of an entity's operations
- Assurance services (including audit of financial statements)
- Business advisory services (transaction advisory, financial management advisory, corporate restructuring and recovery, strategic planning just to mention a few)
- Tax advisory

## *Assessment of Variables*

### **a. Comprehensiveness of AML Legal Framework**

The FCA meets most aspects of the assessment criteria in terms of CDD, Record-keeping, EDD for PEPs and high-risk countries, Reliance on third parties for CDD, including introduced business, suspicious transaction reporting, tipping-off and confidentiality, internal controls, foreign branches, and subsidiaries, licensing and supervision for AML compliance. However, subsidiary legislation in the form of regulations are not in place. The existing ML regulations, despite still being in force, are outdated as they were issued in 2011 and do not address some of the changes that have been included in the FCA.

In addition, FIA is mandated to supervise AML compliance and to delegate that authority where necessary. Subsidiary Regulations based on FCA 2017 are being drafted. Public Accountants and Auditors Act 2013 (PAA) requires mandatory registration/licensing of all qualifying accountants based on international professional ethical standards. This variable is rated High (0.7).

### **b. Effectiveness of Supervision/Oversight Activities**

The FCA mandates the FIA as the supreme AML/CFT supervisory authority. In addition, it has got powers to delegate its supervisory powers and section 35 of the Act outlines what is required of the delegated supervisory authority. Currently the FIA has not delegated its powers to ICAM. Further, staff of FIA are well trained and skilled in AML/CFT issues and possess good understanding of the ML risks of the accountant's profession. However, despite this, the FIA does not have sufficient human and financial resources to carry out its supervisory role effectively. FIA is yet to commence both on-site and off-site risk-based monitoring for the sector.

The Malawi Accountants Board (MAB) and ICAM conduct supervision of accountants and auditors with focusing on compliance with applicable International financial reporting Standards (IFRSs) and International Standards on Auditing (ISAs) but not AML/CTF. Further, mandatory registration of qualifying accountants is in progress to ensure compliance with Section 26 of the PAAA 2013 and high ethical conduct. This is expected to improve effectiveness of regulation and supervision. This variable is rated Low (0.3).

### **c. Availability and Enforcement of Administrative Sanctions**

The FCA has provided for administrative sanctions which include; issuing a written warning, monetary penalties, publicising the non-compliance and revocation of business license. and other sanctions under respective laws governing the contravening individuals. However, the sanctions have been recently introduced with the coming into effect the FCA, and the FIA is in the process of drafting regulations to guide the implementation of the administrative sanctions. There is currently no record of enforcement in this sector.

Section 36-38 and 42(1)(b) of the PAAA 2013 gives ICAM and MAB power to discipline members for unprofessional and ethical conduct. Sanctions include suspension from practice and membership



and monetary penalties. In addition, ICAM has an Ethics and Investigations Committee which investigates all cases of corruption, fraud and unethical behaviour by members. Once investigated, there is a Disciplinary Committee which hears the matters and issues administrative sanctions. As at December 2017, there were 17 cases awaiting to be heard by the Disciplinary Committee.

This variable is rated Medium Low (0.4).

**d. Availability and Enforcement of Criminal Sanctions**

The FCA has made provisions for criminal sanctions. Sections 42-53 provide a range of effective, proportionate and dissuasive criminal sanctions for AML/CFT contraventions applicable to both natural and legal persons, which range from a maximum fine of K500,000,000.00 and revocation of business licenses to a maximum custodial sentence of life imprisonment.

Further to this, under SOCAM's regulatory authority, registration for accountants was voluntary but now the PAAA Act mandates all accountants and auditors to register with MAB & ICAM. Failure to do so attracts a custodial sentence of 2 years and a fine.

This variable is rated Medium (0.5).

**e. Availability and Effectiveness of Entry Controls**

Entry controls are available as applicants are required to register with ICAM membership admissions committee and the MAB by submitting completed registration forms, copies of qualification certificates, two member of good standing who act as the applicant's proposer and seconder, declaration to abide by the ICAM code of ethics and by-law, comprehensive record of work experience, recommendation letter from employer and a registration fees.

However, these requirements do not guarantee prevention of criminals or their associates from being granted a business or professional license or being the beneficial owner with a significant controlling interest in the business or holding a significant management position.

This variable is rated Medium Low (0.4).

**f. Integrity of Business/Profession Staff**

Accountants are required to abide by the International Federation of Accountants (IFAC) code of conduct when carrying out their duties. Violation of this code can lead to disciplinary action which if found guilty, can result in membership suspension, membership withdrawal or withdrawal of practicing license. The *cash-gate* scandal revealed high level of integrity failure among accountants working at the Department of the Account General and other Government Departments through negligence or wilful blindness to suspicious transactions. Three (3) accountants were convicted and one was acquitted in the *cash-gate* scandal. It is suspected that there is a possibility of underreporting to MAB and ICAM, of incidences of integrity failure, and that the figure of integrity failure could be higher.

This variable is rated Medium Low (0.4).

**g. AML Knowledge of Business/Profession Staff**

While accounting firms with international connections, are relatively more aware international and local AML/CFT obligations there is need to enhance awareness raising for r local accounting firms and accountants. Neither ICAM/MAB nor FIA have not conducted specific AML/CTF awareness to reach out to a greater number of accountants and auditors, the FIA last made presentation at the ICAM annual conference in 2008. Plans are underway by ICAM and FIA to train them in the near future.

This variable is rated Low (0.3).

**h. Effectiveness of Compliance Function (Organisation)**

ICAM Has an independent Ethics and investigations committee while MAB has a Compliance department that ensures that members comply with ethical and professional standards. However, these are not specific to AML/CTF. Some audit firms with international affiliation have a compliance function although also not specific to AML/CTF. The FIA has not reached out to the sector, therefore the sector could not be aware of any compliance obligations as stipulated by the FCA.

This variable is rated Very Low (0.2).

**i. Effectiveness of Suspicious Activity Monitoring and Reporting**

Since 2013, there has been no STRs or LCTRs submitted to FIA by accountants and auditing firms. Audit firms maintain client files which contain findings and evidence, including reports on unsupported transactions. However, these are currently not specific to AML/CFT.

This variable is rated Close to Nothing (0.1).

**j. Availability and Access to Beneficial Ownership Information**

Poor record keeping poses challenges when obtaining beneficial ownership information. Auditors conduct Customer due diligence (CDD) to establish the ownership and control structure. This is used as basis to determine the reporting entity. Audit files include details of identities of shareholders and directors. However, most auditors and accountants do not always obtain full KYC/CDD information. There is a serious need to enforce KYC/CDD measures on all those involved in the sector

This variable is rated Medium (0.5).

**k. Availability of Reliable Identification Infrastructure**

Auditors are able to identify customers using IDs such as passports, driving licences and voter registration card. However, the passports and drivers' license have been prone to forgery and abuse. The national identification system is also currently being implemented and it is expected that the introduction of the national ID will help mitigate the problems posed by the other identification documents. This variable is rated Medium (0.6).

**l. Availability of Independent Information Sources**

Auditors (with client consent) do independent confirmations with third parties. Most entities that can provide independent sources of information which should be public knowledge, such as the

Registrar of Companies and the National Credit Bureau are not readily available as it is time consuming to get information from them. In addition, some of these charge for one to get information from them. It is therefore not easy to access comprehensive and reliable historical financial information and other information about clients. Deficiencies/room for improvement - Formulation of a system whereby all the involved parties in the audit/accounting industry would easily access and exchange clients' identification and relevant information at ease.

This variable is rated Medium (0.5).

#### **m. Inherent Vulnerability**

The inherent vulnerability of the sector is 0.66 and this rating has been based on a number of factors, such as size, customers, cash intensity, use of agents, anonymous use, tracing of transactions, money laundering typologies, existence of fraud and tax evasion and non-face-to-face use.

The size of the industry is considered Medium High. Although the number of registered accountants (with ICAM) seems low; 1,855, the size of unregistered accountants could be more than double the registered ones. An average of 500 Candidates complete ICAM diploma studies each year and it can be estimated that between 2013 and 2016 an average of 2000 completed. This does not take into account those studying other accountancy courses with universities or ACCA. An estimated 27% of accountants in audit firms are registered with ICAM while 73% is not registered.

The client base is Medium Risk as clients are spread across all sectors of the economy. The majority of clients are Malawians (80%) and few foreigners (20%). The level of interaction with clients by registered accountants is mostly formal with traceable transaction trail. However, the credibility of clients served by the unregistered accountants (mostly SMEs and PEPs) and other casual businesses may be questionable, even though there is no evidence to back the perception.

Audit firms and other registered consultants are mostly paid by cheque or online transfer. However, some accountants may accept cash, especially from PEPs and SMEs even though not on large scale. Cash payments are common with small businesses who prefer to use this mode for their convenience.

Use of agents by accountants is generally not common. The nature of accountancy and advisory services are such that they require direct contact with the client, once at some point during the consultation process. Interaction is mostly direct with the clients, with few exceptions on foreign clients where an agent could be engaged by the client to transact on his/her behalf. However, there are no statistics to support this.

The nature of the profession makes it difficult for the services to be carried out by a non-professional and therefore does not allow for anonymous use.

Tracing of transactions is easy as most accountants and auditors keep records of transactions handled for reference. These records are basis of reports which are the outcome of the work performed.

There are no money laundering typologies from Malawi, however, the typologies do exist from outside the country. However, the use of accountants in fraud and tax schemes exists but is limited. Non face-to-face use of accountants is available but limited as their services usually require direct contact with clients with limited exceptions to foreign based clients.

## **Real Estate**

### ***Background***

The real estate industry is regulated by the Board of Registration of Land Economy Surveyors, Valuers, Estate Agents and Auctioneers (hereinafter referred to as the Lands Board) which was established through the Land Economy Surveyors, Valuers, Estate Agents and Auctioneers Act, 1990. This Board regulates individuals wishing to practice as Land Economy Surveyors, Valuers, Estate Agents and Auctioneers. The Lands Board does not license real estate firms.

There are only 37 individuals registered with the Lands Board, while the FIA has compiled a list of 59 firms operating as real estate agents, valuers and / or auctioneers. It is however difficult to determine the size of the industry as there are many unregistered players.

### ***Overall Vulnerability***

The real estate sector vulnerability is dependent on the strength of the AML general controls and product specific variables. The overall ML/TF vulnerability for the real estate sector is rated High (0.89). The rating took into consideration the AML general controls, which were rated Medium Low (0.26) as represented below. The AML general controls looked at the quality of operations (Medium Low – 0.26), quality of AML policies and procedures (Medium Low – 0.39), quality of AML supervision (Low – 0.20), quality of CDD framework (Medium – 0.46), commitment and leadership of management (Medium Low – 0.27) and compliance of staff (Medium Low – 0.30). The rating for the sector during the 2013 assessment was Very High (1.0).

The current assessment has taken into consideration several variables as presented below.

### ***Assessment of Variables***

#### **a. *Comprehensiveness of AML Legal Framework***

The FCA conforms to international standards on combating ML as it covers all areas of KYC/CDD/EDD, reliance on CDD by third parties, record keeping, suspicious transaction reporting, tipping-off and confidentiality, internal controls, foreign branches and subsidiaries, regulation and supervision of financial institutions, supervisory powers and sanctions and administrative penalties

(See FCA sections 16 to 34). Subsidiary legislation (Regulations) issued under the repealed ML Act are still in force. However, Regulations under the FCA are expected to be concluded by March 2018. As a result of the above, this variable is rated High (0.7).

**b. Effectiveness of Supervision/Oversight Activities**

The mandate of the Lands Board, as Regulator of individuals dealing in the real estate business, does not extend to AML supervision. As such, the Lands Board does not have AML comprehensive supervisory framework such as supervision policies, procedures and manuals. The Lands Board has 37 registered real estate individuals while the FIA has identified 58 firms registered by the Registrar of Companies and trading as real estate agents.

The Land Economy Surveyors, Valuers, Estate Agents and Auctioneers Act states that the Minister shall appoint the members of the Board and that there will be a minimum of 5 and not more than 9 members. However, that is not the case as membership is currently voluntary. The Lands Board has been in existence since 1<sup>st</sup> July 1990 but there is no consistency of members and not much has been done to regulate the players in the sector. This Act also does not adequately provide for proper definitions, qualifications and roles of estate agents and auctioneers. Due to these shortcomings, it has been difficult to enforce the provision of the law. In addition, this law is in conflict with the Business Names Registration Act as one can easily register a business name with the Registrar of Companies, indicate their nature of business as real estate agents, while not fully complying with the Lands law and not registering with the Lands Board. This has contributed to the existence of a thriving parallel real estate system which is evidenced by the large number of unregistered and unsupervised players in the sector. The profession possesses little understanding and appreciation for ML and the Board does not have the AML knowledge and staff to competently provide AML supervision.

The introduction of the FCA brought changes in respect of AML supervision as this Act mandates the FIA to be the supreme authority regarding AML matters. The FCA further gives powers to the FIA to delegate AML/CFT supervision to other supervisory authorities or self-regulatory bodies (FCA s35 to 38). The FIA has made attempts to supervise the real estate sector, however this has not been consistent. Between 2013 and 2017, the FIA conducted on-site examinations on 4 of the 58 registered real estate entities in its database, representing 6.8% of the sector. This variable is therefore rated Very Low (0.2).

**c. Availability and Enforcement of Administrative Sanctions**

The FCA has made provision for administrative sanctions and these can be in the form of a warning, monetary penalties, publicising the act of non-compliance and loss of business. However, these have not yet been tested as regulations covering the sanctions are in draft form.

The Land Economy Surveyors, Valuers, Estate Agents and Auctioneers Act empowers the Board to, suspend a registered person or to strike out from the register a person who shall be found guilty of unprofessional conduct as defined under that act.:

However, there are no known cases of any such sanctions having been enforced by the Lands Board prior to the enactment of the FCA. As a result of the above, this variable is rated Low (0.3).

**d. Availability and Enforcement of Criminal Sanctions**

Part IV of the FCA has made provisions for criminal sanctions. However, there have not been any cases involving prosecution of offenders in the real estate sector. The criminal sanctions provided by the FCA are comprehensive and adequate. However, since no enforcement has taken place, this variable is rated Medium (0.5).

**e. Availability and Effectiveness of Entry Controls**

Section 3 of the Land Economy Surveyors, Valuers, Estate Agents and Auctioneers Act states that, *"...no person shall practice under any name, title or style containing the words land economy surveyor, valuer, estate agent or auctioneer or, for the purpose of gain, make any other use of such name, title or style, unless he is registered under the Act as a land economy surveyor, valuer, estate agent or auctioneer"*.

Although there is a Lands Board to control the entry of individuals wishing to engage in the real estate profession, one can also simply register as a business, with the Registrar of Companies and then proceed to venture into the real estate business. According to information provided by the Lands Board, the requirement involves one registering with the Board and then showing proof of the registration to the Registrar of Companies for the registration to be concluded. This however, does not happen.

The Lands Board is empowered under s5 of the Lands Act to make rules involving definition, mode of enquiry and methods of dealing with misconducts, penalties and prescribing terms and conditions on engaging of articulated pupils. Section 8 further outlines the qualifications for registration of individuals. These include that an applicant should be above twenty-two years, paid the registration fees, passed a qualifying exam (or its equivalent) which has been approved by the Board, not less than two-year practical experience. The Lands Board also considers the integrity of the applicant by conducting criminal checks with the MPS.

Despite there being entry controls in place, they are not implemented and this has contributed to the rise of a thriving unregistered real estate players. Therefore, the rating for this variable is Low (0.3).

**f. Integrity of Business / Profession Staff**

Real estate agents with individuals registered by the Lands board conduct strict background checks and vetting on real estate employees. There are checks done with previous employers in job applications for background checks of employees. However, there have been many cases of misconduct among those real estate agents who are not registered by the Lands Board and some of these incidents have led to civil prosecutions.

Further to this, integrity of staff is questionable as there have been suspicion of property buyers colluding with real estate agents and lawyers to under-declare the amount sold so that the seller pays less tax to government when conducting change of ownership, this has been discovered in cases where the Ministry of Lands conducts ad-hoc investigations. To tackle this problem, the Ministry of Lands entered into an agreement with the ACB, who investigate any such cases when a

report is made to them by the Ministry of lands. this is done as part of the Ministry of lands integrity initiative in the sector.

This variable is rated Medium Low (0.4).

**g. AML Knowledge of Business/ Profession Staff**

The FIA was unaware of the existence of the Lands Board and therefore has not extended its awareness programme to them. The Lands Board has also not been aware of its role in combating ML and the legal requirements under the FCA.

The FIA has held two trainings for the real estate sector since 2013, which were attended by both registered and unregistered entities. However, the trainings were not extended to other key staff of the individual real estate institutions as it is the responsibility of the individual real estate institutions to ensure that all relevant staff are aware of and trained in AML matters. The FIA provides such training when requested by the institution. Participants in the industry are not regularly updated on domestic and transnational money laundering schemes and typologies, including those involving the misuse of the business/profession and specialised knowledge and skills of its professionals and its products and services. Entities with international ties were generally well aware of AML issues at an international level as their international counterparts provide them with AML/CFT training, usually on an annual basis. However, these entities are not well conversant with the local scenario.

This variable is rated Low (0.3).

**h. Effectiveness of Compliance Function (Organisation)**

Most firms in the real estate profession do not have internal AML compliance programmes as there has been poor outreach by the FIA and the Lands Board has been inactive. Very few entities have appointed a sufficiently-resourced, independent AML compliance officer and these are not at senior management level. This variable is rated therefore Very Low (0.2).

Most if not all entities do not perform internal and/or external AML audits

**i. Effectiveness of Suspicious Activity Monitoring and Reporting**

Between 2013 and 2017, the FIA received 1 suspicious activity report from the real estate sector. In addition to this, there have only been a few threshold reports from one reporting institution submitted to the FIA. Many in the real estate profession do not have effective and appropriate systems for record keeping, monitoring and STR reporting to support AML policies and procedures

Most of the unregistered entities barely have established premises, with some just “borrowing” offices to conduct transactions when they have clients. These entities therefore do not have information systems that can facilitate monitoring of client transaction activities, compare client transactions against the client’s profile, perform AML screening and monitoring, carry out PEP screening and effectively identify and record all complex or unusual large transactions. This variable is rated Close to Nothing (0.1).

**j. Availability and Access to Beneficial Ownership Information**

A large number of the firms in the real estate sector do not have requisite expertise and resources to facilitate proper CDD requirements. When conducting real estate transfers and leasing property, the Ministry of Lands, Housing and Urban Development mostly process the applications via lawyers and legal professions and in few cases real estate agents. All parties in the transactions have to be identified by either a lawyer or government official working with Ministry of Lands. However, transactions can be conducted without the actual concerned parties being present at the Ministry of Lands and the lawyers do not always obtain full KYC/CDD information. Although property may be bought on behalf of someone, the person conducting the transactions will be known by the lawyer and the real estate agents.

The variable is rated Medium Low (0.4).

**k. Availability of Reliable Identification Infrastructure**

The Malawi Government has just introduced a national identification system, which has not yet been fully implemented. Passports and drivers' Licenses are the most reliable ID document with other forms of identification used by the sector being voter registration cards. However, these documents have been prone to abuse and forgery. It is envisaged that the National ID will ease identification challenges once fully implemented.

The variable is rated Medium (0.5).

**l. Availability of Independent Information Sources**

Although there are independent and reliable sources of information to determine transaction patterns of clients such as commercial history from Banks, former employers' reference, former employers, and utility bills, among others. Most entities that can provide independent sources of information which should be public knowledge, such as the Registrar of Companies and the National Credit Bureau are not readily accessible as it is time consuming to get information from them. In addition, some of these entities require payments to release information. It is therefore not easy to access comprehensive and reliable historical financial information and other information about clients.

The variable is rated Medium (0.5).

**m. Inherent Vulnerability Assessment**

The inherent vulnerability of the real estate sector is High. This has been based on a number of variables, including size of the industry, client base, cash intensity, whether the sector has been used for money laundering or fraud and whether the sector allows for anonymity.

The total number of service providers in the real estate sector (particularly the unregistered ones) is constantly increasing thereby increasing the ML vulnerability. Licensed service providers as well as unlicensed service firms or individuals can both provide such services which are supposed to be regulated by the Lands. Since the Lands Board has not been effective in its supervision, the real



estate entities have not been accountable to anyone and therefore it is difficult to determine the total size / volume of the industry. However, currently there are 37 individuals registered by the Lands Board to operate as real estate agents, valuers and auctioneers and over 50 companies registered as real estate agents.

The client base contains PEPs, High net-worth individuals and international clients who are rated as very high risk in terms of ML in addition to a huge base of local clients. Many PEPs have acquired more than one high value property and some of them were involved in the cash gate case. In addition, many foreigners have acquired property in Malawi, some of the foreigners include those from high risk jurisdictions such as Libya, Nigeria, Zimbabwe

The real estate sector is highly cash intensive, particularly among the unregistered entities. In addition to this, there is no law that bars or restricts the use of cash, therefore many entities prefer to use cash. The use of agents in the sector is very high which is evident from the adverts that appear in the local newspapers. Real estate transactions can be conducted anonymously in that one may purchase real property in trust of someone and the ultimate beneficiary may not be adequately identified.

The fact that there are unregistered players in the sector makes it difficult to trace transactions especially due to poor record keeping and the excessive use of cash. Some real properties are not registered with the Ministry of Lands Housing and Urban Development's Land and Deeds Registries, these can be resold several times without any reliable documentation being produced

There are no documented ML typologies from Malawi on the use of the real estate sector for money laundering. However, in the ongoing *cash-gate* cases it is alleged that some suspects and convicts converted the proceeds of crime into real estate by either purchasing or constructing houses. At an international level, there are well documented typologies. For instance, typologies as provided by FATF include the following:<sup>49</sup>

**Typology 1: Use of property management companies** (Predicate offence: suspected fraud)

The FIU received a suspicious transaction report from notary A on one of his clients, person B, a foreigner without an address in Belgium, who in his office had set up a company for letting real estate. The sole manager and shareholder of this company was a family member of B, who also resided abroad. Shortly after its creation the company bought a property in Belgium. The formal property transfer was carried out at notary A's office. The property was paid for through the account of notary A by means of several transfers, not from company X, but from another foreign company about which individual B did not provide any details. The establishment of a company managed by a family member with the aim of offering real estate for let and paid by a foreign company disguised the link between the origin and the destination of the money.

Police intelligence revealed that the individual was known for financial fraud. The investment in the property was apparently financed by the proceeds of these funds.

---

<sup>49</sup> Money Laundering and terrorist financing through the real estate sector – FATF, 29 June 2007

#### Indicators and methods identified in the scheme:

• Instruments: cash, wire transfers, real estate. • Mechanisms: notary, bank. • Techniques: business account, purchase of real estate, transaction inconsistencies, non-resident customer, unknown source. • Opportunity taken: the establishment of a company managed by a family member with the aim of letting real estate paid by a foreign company disguised the link between the origin and the destination of the money

**Source:** Belgium, 2005.

The real estate sector allows for anonymity due to the fact that one can buy or sell real property without actually meeting the real estate dealer. For instance, Malawians in the diaspora or foreigners based outside the country can acquire real property without meeting the real estate dealers or entities. This can be done using lawyers and the appointment of a power of attorney.

#### *Deficiencies and Gaps Identified for the DNFBPs Sectors*

The assessment established some gaps among the DNFBPs. There is generally lack of AML/CFT knowledge among the DNFBP sectors as the FIA and the other sector-supervisors are yet to reach out to some of the players and sensitise them on their AML/CFT obligations and the FCA. Further, there is insufficient supervision or oversight of AML/CFT activities in the DNFBP sectors and these are not carried out on a risk-based approach. The sectors generally have ineffective compliance functions with the lawyers, accountants and dealers in precious stones and metals having no compliance functions at all. As a result, the reporting of STRs is close to nothing for all the DNFBP sectors.

Below is a table indicating areas of focus to address the identified gaps for each of the DNFBP sectors.

*Table 19: Prioritisation of general AML controls for DNFBPs*

PRIORITY RANKING FOR GENERAL INPUT VARIABLES/ AML CONTROLS	PRIORITY RANKING - Casinos	PRIORITY RANKING - Lawyers	PRIORITY RANKING – Precious stones & Metals	PRIORITY RANKING - Accountants	PRIORITY RANKING – Real Estates
Comprehensiveness of AML Legal Framework					
Effectiveness of Supervision/Oversight Activities	3	2	2	2	2
Availability and Enforcement of Administrative Sanctions	5	6	7	9	6
Availability and Enforcement of Criminal Sanctions	6	9	8	7	8
Availability and Effectiveness of Entry Controls	6	5	6	5	5

PRIORITY RANKING FOR GENERAL INPUT VARIABLES/ AML CONTROLS	PRIORITY RANKING - Casinos	PRIORITY RANKING - Lawyers	PRIORITY RANKING – Precious stones & Metals	PRIORITY RANKING - Accountants	PRIORITY RANKING – Real Estates
Integrity of Business/ Profession Staff		7	5	6	7
AML Knowledge of Business/ Profession Staff	1	1	1	1	1
Effectiveness of Compliance Function (Organisation)	2	3	3	3	3
Effectiveness of Suspicious Activity Monitoring and Reporting	4	4	4	4	4
Availability and Access to Beneficial Ownership information		10	10	10	10
Availability of Reliable Identification Infrastructure	8	8	9	8	9
Availability of Independent Information Sources		11	11	11	11

### *Recommendations for the DNFBPs*

- 1) The FIA should consider delegating supervisory authority to sector-specific supervisors that are active in exercising AML/CFT supervision
- 2) All supervisors should develop a fully-fledged risk-based approach to AML/CFT supervision which takes into account the findings of the NRA
- 3) FIA in collaboration with the sector supervisors should conduct AML/CFT trainings for both regulators and players in the sector to enhance their knowledge of AML/CFT, institution and implementation of effective compliance functions and capacity to detect suspicious activities
- 4) Administrative sanctions for non-compliance with AML/CFT requirements should be administered to entities that are not complying with provisions of the FCA
- 5) The Lands Board should revise and ensure effective implementation of Entry Controls
- 6) The Lands Board should enforce sanctions on all unregistered real estate players  
The Department for Mines needs to introduce and implement entry controls for dealers in precious stones and metals that include fit and proper tests and AML/CFT CDD measures

## **Non-Governmental Organisations Vulnerability**

### **Background**

In Malawi, NGO means a Non-Governmental Organisation constituted for public benefit purposes. These comprise of faith based organisations, civil society organisations and community based organisations. The sector is regulated by the NGO Act 2001 which gives mandate to NGO Board to

register and regulate NGOs. The Council for Non-Governmental Organisations in Malawi (CONGOMA) is an association mandated to represent the collective interest of NGOs in Malawi. As of 2017 there are 660 registered NGOs with the NGO Board and 1140 NGOs registered with CONGOMA. However, there are more than 2,000 NGOs which are registered as legal persons by the Registrar of Companies operating in Malawi and this makes it difficult for the NGO Board to monitor transactions of those that are not registered with it. For instance, in 2017 the average turnover of 125 NGOs that submitted their annual reports to the Board was estimated at MK400-billion.

### Definition of an NGO

Non-Governmental Organisations in Malawi are defined as legally constituted, not for profit making, autonomous and non-partisan entity whose primary activities include service provision, development initiatives, humanitarian response, awareness raising and advocacy, provided under the framework of human development and good democratic governance. The assessment also considered the FATF definition of Non-Profit Organisation (NPO) which is 'legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, education, social or fraternal purposes, or for the carrying out of other types of good work.'

The number of NGOs worldwide is estimated to be 10 million, employing up to 7.5% of the global work force. NGOs influence global affairs differently such as its ability to modify behavior through use of ideas. Looking at some of the neighbouring countries with Malawi, the open source statistics shows that Mozambique has a total number of 250 registered NGOs and Zambia has 400 registered NGOs which makes Malawi to have the highest number of registered NGO.

The sector is very vital to the country's economy as it complements Government effort by contributing 20% (off budget support) of the national budget. Since 2013 donors stopped providing direct budget support to the Government and have been channelling all the support through NGOs. The NGOs are involved in a number of activities such as education, relief, health and disease control, religion, agriculture, minority rights, gender and child protection, youth, governance and charities which operate at grass roots level.

While the assessment considered the main issue of NGOs is terrorist financing since NGOs may easily be abused to raise, store, move funds by terrorist operatives, the assessment further noted that the NGO sector in Malawi faces other risks relating to ML, theft, fraud and corruption. A thorough assessment presents an opportunity to recommend risk mitigation measures that will protect NGOs against threats from the earlier predicate crimes and ML which in turn can play a role in mitigating TF risk.

Overall TF vulnerability is rated Medium Low and ML vulnerability for NGOs is at 0.40 which represents medium low vulnerability. The ratings have been influenced by the following factors:

1. **NGO registration:** In Malawi, NGOs are required to register with NGO Board under Section 20 of the NGO Act which states that *'Every NGO established or operating in Malawi which is recognized as a legal person under the laws of Malawi, except the exempt organisations,*

*shall register with the Board*'. The Act lists a number of documents which NGOs are required to file with the Registrar during registration namely, the NGO certified constitution, plan of activities to be undertaken and approval from respective Ministry, source of funding, physical and postal address of the NGO among others and names of board of trustee through affidavits.

As a starting point, Local NGOs are required to register with Registrar of Companies as a legal person and thereafter register with CONGOMA and then NGO Board to operate as NGOs in Malawi. The registration with the NGO Board presupposes registration with CONGOMA. However, in practice the NGOs have tended to register only with CONGOMA but not with the NGO Board. Currently it is estimated number that more than 900 NGOs operating without registration under the NGO Act and 130 NGOs who have pending registration with CONGOMA because they have not submitted all the required documents. For registration with CONGOMA, the applicants are required to submit the following documentation:

1. A filled CONGOMA Membership Application Form.
2. A certified copy of the NGO's Constitution or a Governing Instrument of the NGO.
3. A copy of minutes of the first meeting at which it was agreed to form an NGO.
4. A brief concept paper indicating physical address for offices, brief background to the NGO, mission statement, vision, values, districts where activities are being/will be implemented, sectors of operation (such as health and education), an outline of activities that the NGO has implemented or intends to undertake in Malawi under each of the sectors, sources of funding and number of employees/volunteers.
5. Sworn affidavits of trustees and/or directors, with their passport size photographs, giving their names, citizenship, occupation and address.
6. A copy of the trustees' / directors' declaration.
7. A copy of Certificate of Registration with the Registrar General.

International NGO are required to provide the following additional documents to NGO Board when registering namely;

1. Approval for registration from the Ministry of Gender, Children, Disability and Social Welfare which is responsible for NGO coordination before being registered with CONGOMA and NGO Board.
2. Names of board of trustees at least two should be Malawians who are also required to swear affidavits.

The Ministry approval process requires that the NGO should be vetted in terms of origin, sources of funding, governance structure and also reference from other countries where is/has operated in collaboration with the Ministry of Foreign Affairs and International Cooperation. However, it has been established that at the Ministry of Gender's officials it was found out that in practice the vetting process is not being carried out as the officials only look at the provided documents and verbal interview with the personnel holding the documents and then issue an approval memorandum of understanding (MoU). This decision to grant an approval or not is based on personal judgment of the officer present that day.

There have instances where International NGOs have been turned back for not meeting the mentioned requirements.

There are also NGOs existed before the NGO Act came into force, some of which were registered as Company Limited by Guarantee (meaning companies that are limited but do not make profit). (Refer to Legal Persons and Arrangements for registration of such kind of companies).

### **Registration Challenges**

Below are the major challenges on registration of NGOs in Malawi:

- Some NGOs are operating without registration with CONGOMA and NGO Board. This creates a challenge to monitor their activities and in the case of ML/TF, it is difficult to follow up as a country.
- The NGOs which chose to only register with the Registrar of Companies pose a challenge because the NGO board is unable to monitor their activities.
- Some NGOs believe that the registration process is too involving and long and duo registration exits, therefore they resolve to only register with either CONGOMA or NGO Board.
- The vetting process of international NGOs is not being properly done. Since there are some loop holes in the vetting process as a country we believe there is potential for abuse in terms of ML/TF.
- Some NGOs in Malawi are faith based and operate under the umbrella of religious denominations. These NGOs are not registered by the NGO board though they operate as NGOs and conduct non-evangelic activities.
- The information and documents provided for registration are not systematically verified. For example, in the case of trustees, only the name may be taken, without verifying IDs or other types of verifiers (e.g. affidavit from the NGO).

Despite these challenges highlighted above, both the TF/ML vulnerability level of this variable is Medium Low.

### **Reporting Requirements**

Section 22 of the NGO Act states that every registered NGO shall file with the Registrar's office the following documents and information which shall be part of the Registry accessible to the public on annual basis; its audited financial statements, its annual report outlining the activities undertaken by the NGO and its annual return form outlining trustees, sources of funding, auditors. Reporting to the NGO Board is and reporting to CONGOMA is implied.

The reports are an important AML/CFT monitoring tool and if not submitted it is very difficult to know the happenings within the sector. The statistics shows that in the financial year 2016 - 2017 the complied NGOs which represents 19% of registered NGOs with the NGO Board had a combined income of about MK250 Billion that's an indication that NGO sector deals with a lot of money. With this huge amounts of money in the sector, it is important to know the source of these funds and how they are being spent.

### Reporting Challenges

The reports submitted to NGO Board is supposed to be used to help the regulator supervise and monitor NGO activities in the reported financial year but currently this is not happening due to inadequate capacity and lack of resources for the Board to conduct such activities. The information received from NGOs is not verified because dependence is placed on the external auditors of each NGO who audit the accounts for truth and fairness.

The TF vulnerability is low and ML vulnerability is medium for this variable.

### Source of Funds of NGOs

The NGO Act under section 20 and 22 requires NGOs to disclose their sources of funding when registering and submitting annual reports. The annual reports do not just disclose origins/sources of funds but also an account of expenditure and whether the funds have been spent in a manner consistent with the status of the NGO. The disclosure of origins/sources of funds is important to ensure accountability and transparency in the NGO's operations. It is also important because it can facilitate the carrying out of proper due diligence on individuals and organisations that fund NGOs, receive money from NGOs or work closely with the NGOs.

Through the reports submitted to the NGO Board in 2016/2017 financial year, the source of funds for these NGOs were organisations based in Europe, United States of America, Canada and some were anonymous. Anonymity of source of funds may be difficult to maintain if funds are received through regulated financial institutions, it is still difficult to know source of funds if the funds are received through other means outside the formal financial institutions. From reports submitted to the NGO Board, most of the NGOs get their funding from Europe and America, very few from Middle East or origins which are anonymous.

However, considering that the small percentage of NGOs who submitted the reports it is still not known as to who finances a large number of the NGOs. This implies that it may not be possible to conduct a proper due diligence on a large number of NGOs. From open source information the NGOs who do not submit annual reports suspect that the information contained in their reports may not be used for the intended purpose by the regulators, but rather to victimise the NGOs.

In 2014, FIA disseminated one report to Law Enforcement on one NGO operated by foreign nationals whose origins of funds was a foreign organisation suspected to be financed by individuals one of whom was on an UN sanctions list. The expenditure items of the NGO were not consistent with the initial declaration of the activities of NGO. This report came through as a result of enhanced due diligence on the NGO through information from the financial institution maintaining the

accounts of the NGO. While results of the LEA investigations on the NGO are not yet out, the case highlights the need for knowing the source/origin of funds of the NGOs.

There is still much work to be done to mobilise the NGOs which do not submit annual reports to make them comply with the requirement.

From the above analysis, the TF vulnerability is medium low and the ML vulnerability is medium for this variable.

### **Adverse Reports to NGO Board and CONGOMA and How they were Handled**

All registered NGOs in Malawi are bound by the Code of conduct which was ratified by the General Assembly of NGOs in Malawi on 25<sup>th</sup> April 1997. The Code of conduct has five cardinal values namely; respect for law and Human rights, political non-partisanship, professional management structures, character and collaboration.

In promoting compliance to the code of conduct, CONGOMA elected the Standards Committee which is responsible for enforcement. The Committees' functions among others are to consider and determine any application, complaint or matter brought to it under this code through verification of all related facts. This committee has received over twelve cases ranging from misuse of funds for self-enrichment, obtaining goods and services under false pretence, among others which lead to deregistration of these NGOs.

The NGO Board has received not less than five case in the year 2017. These cases are handled by the Board of trustees of the NGO Board which form the disciplinary committee for the hearing process before the conclusion is reached and the NGO can appeal the decision in court of law.

Examples of some of the cases handled over the past year;

1. Maphunziro Foundation was deregistered in the year 2017. The NGO was suspected of misappropriating a grant, an audit was carried out by an independent auditor which confirmed the abuse, and the matter was taken to court of law where a judgment was obtained against the NGO.
2. Foundation for Promoting Psychology in Africa (FROPA) was deregistered in the year 2017. Some service providers and beneficiaries reported FROPA to NGO Board and CONGOMA for swindling money. Some of the NGO trustees were arrested and the estimated amount of money abused is Mk 20 million. Information from NGOs that sub-grant other NGOs indicates that there are cases of abuse of granted funds, which are not reported to the NGO Board or CONGOMA as a coordinator. The funding NGOs choose to sometimes handle such abuse cases internally through contract cancellation and black listing the NGO. The information of such cases is not made public and as such the abusing NGO can continue receiving funds from other donors without any action taken.

In conclusion, after looking at the above factors, there is a loop hole in the system for those NGOs that are operating yet not registered with NGO Board and CONGOMA. Even though the banking systems can monitor the movements of their finances, it is a problem for the regulators to know and keep records of their sources of income and also monitor their activities.



## Recommendations

1. NGO Board and CONGOMA should be trained by FIA on ML/TF issues as they relate to the NGO sector.
2. NGO Board and CONGOMA through the help of FIA should raise awareness of ML and TF to all NGOs
3. Every financial year NGO Board should have a budget line for supervision and monitoring of NGO activities for purposes of detecting TF.
4. The registration process of NGOs should be made rigorous to ensure that all documents are scrutinised and vetted.
5. NGO Board and CONGOMA should ensure that NGOs follow a 'Know your beneficiaries and associate NGO' rule which means making efforts to establish the identity of their donors, beneficiaries and the source of funds.
6. NGO Board should develop a working relationship with banks, Department of Immigration and Citizenship Services, NIB, FIA, and CONGOMA on any issues affecting the NGO sector.
7. Government should develop a policy requiring implementation of AML/CFT reporting obligation for the NGO sector.

## Legal Persons and Arrangements Vulnerability

### Background

There are diverse legal persons and arrangements that can be created in Malawi. Legal persons and arrangements were not assessed during the 2013 NRA. This assessment looked at legal persons and arrangements categorised as follows:

- a) Companies created under Companies Act 1984;
- b) Companies created under Companies Act 2013;
- c) Legal persons created under Business Registration Act 1964;
- d) Legal persons created under Business Registration Act 2012;
- e) Legal arrangements created under Trustees Incorporation Act; and
- f) Settlement Trusts.

### Assessment of Vulnerability

The legal persons and arrangements created in Malawi currently carry vulnerability of **Medium High** because the beneficial ownership information is not collected and stored by the Registrar General. Settlement/private trusts and the companies registered under the 1984 Companies Act whose information is not up to date present a particularly higher risk. Further to this, the information given to the Registrar General, including on source of funds, is not verified in any way.

### Corporate Entities

The Company Law in Malawi has recently been revised. Currently, the applicable law is the Companies Act 2013 which came into force in 2016 which replaced the Companies Act of 1984. The report will discuss both Law since the Companies that were created under the old law are still on the Companies with new companies being registered under the Companies Act of 2013.

### *Companies incorporated under Companies Act of 1984*

There are numerous companies on the Companies Register that were Registered under the Companies Act of 1984. Obtaining an actual figure has been difficult because only 80% of the records are digitised and that some information is still missing. Under this Act, the filing of annual returns by Companies was mandatory and penalties were applicable for failure to file the annual returns. However, the penalties were minimal as did not discourage non-compliance. For instance, a penalty of K10.00 per day was charged, from the date the annual returns became due, for every director, shareholder and the company.

Further, it was mandatory to file with the Registrar of Companies any changes of particulars of the directors, shareholders and addresses. Where the Company failed to comply with this requirement the penalties imposed were equally negligible with the result that compliance of companies in notifying the Registrar of Companies of any changes was not encouraged.

It should be noted that over 80% of companies registered under the 1984 Act have been digitised. However, this does not imply that all the information of all Companies registered under the 1984 Law is up to date. This poses a vulnerability for ML for companies whose information is not up to date.

#### **a. Company Limited by Shares**

This type of company had subscribers/shareholders with a requirement of a minimum of two shareholders. It was required that there should be a minimum of three Directors with at least one local resident director. The Articles and Memorandum of Association were required to be submitted for incorporation. The names, addresses and occupations of the shareholders, company secretary and directors were equally included in the application document. Further, a family trust could be a shareholder and there are still companies on the company registry that have family trusts as shareholders. Further to this, a foreign registered company can be a shareholder. It was sufficient for the foreign company to only provide copy of incorporation certificate, postal and physical address for it to be a shareholder.

Section 45 of the 1984 Act expressly prohibited bearer shares. A share certificate bearing the name of the shareholder and the shareholder register bearing the names of the shareholders is/was an indication of the owner and as such bearer shares were not permissible under the 1984 Act. Section 31 of the 1984 Act provided for the registration of shareholders in the shareholders' register, and the information entered on the share registry was the name, shareholding and address of the shareholder. This Act did not provide for issuing of nominee shareholders or directors. Nonetheless, the 1984 Act allowed shareholders or directors to nominate a proxy who could participate in a meeting on behalf of the director or shareholder.

#### **b. Company Limited by Guarantee**

A company limited by guarantee needed to have shareholders with a minimum of two shareholders. There was need for the company to have directors with a minimum of three local resident directors. Memorandum and articles of association were submitted for incorporation with the names, addresses and occupations of the shareholders, company secretary and directors included.

**c. External Company**

For an external company to register in Malawi under the 1984 Act there was need for certified copies of incorporation documents from the country where the company is registered. In addition, there was need for statement of particulars; providing information such as the country where the company is registered, physical address and postal address that will be used in Malawi, details of local directors, the name of the documentary agent, postal and physical address of documentary agent. There was need for letter of authority for the documentary agent. However, the Act did not require the provision of any identifications documents.

***Companies Incorporated Under Companies Act of 2013***

The Companies Act of 2013 came into operation in 2016, and it introduced significant changes in the creation and registration of legal entities in comparison to the Act of 1984 as will be highlighted in the proceeding discussion. Companies are now registered using the Malawi business registration system, which is an online business registration system.

**d. Company Limited by Shares**

The Company needs to have shareholders, directors with a minimum of one local resident director. There is a requirement that articles and memorandum of association are submitted for incorporation. The shareholders and directors are mandated to complete consent forms agreeing to act in that position and also providing information including their names, age, postal and residential addresses. Apart from the consent form, there is an application for that has to be completed with information stating the details for shareholders, directors, registered office address, postal address and share capital.

**e. Company Limited by Guarantee**

Similar to the company limited by shares, a company limited by guarantee also needs to have subscribers and directors, with a minimum of one locally resident director and information such as names, age, postal and residential addresses have to be included. There is equally a need to submit articles and memorandum of association for incorporation. Additionally, subscribers and directors ought to complete and sign consent forms to act as directors. All information is submitted together with an application form which contains further details pertaining to the company similar to that required for a company limited by shares.

**f. State Owned Company**

The government is the shareholder or subscriber in a state - owned company. The company needs a minimum of three directors and a company secretary and all these officers are required to provide their particulars such as full names, age, postal and residential addresses is obtained for the purpose of retaining information of the company. The directors holding the positions need to consent to act

in the position. Further, state owned companies also have to file articles and memorandum of association when registering the Company.

**g. Public Limited Company**

The 2013 Act provides that a public limited company ought to have a minimum of three (3) shareholders and a minimum of three (3) directors. A public company is mandated to have a company secretary. At the time of registration there is need for consent of shareholders, and consent of the directors and the company secretary, and the consent form will have particulars such as the names, age, postal and residential addresses of the officers of the company. All this information, including articles and memorandum of association, is submitted together with an application form.

**h. Foreign Company**

The 2013 Act provides for a comprehensive set of documents that are needed for a foreign company to be registered in Malawi. These include the following:

- Notarised incorporation documents from the country where the Company was registered.
- Details of shareholders and directors of the Foreign Company
- Local Resident Director (Names, age, postal and residential addresses).
- Completed Form 15 on Application to register in the Company Register.
- Completed Form 19 on Application to register a Foreign Company.
- Name Reservations Form (Form 4).
- Declaration that Company is not barred from Registering in Malawi.

**Relevant Observations on the Companies Act 2013**

In the proceeding paragraphs the discussion will focus on observations with regards to the 2013 Act that will inform the discourse of money laundering in relation to legal persons and arrangements in Malawi. Even though there are companies registered under the 1984 Act, these are now regulated by the 2013 Act.

Under the 2013 Act, only a natural or legal person can be shareholders. Further, bearer shares and nominee shareholders are not allowed under the 2013 Act. A shareholder of a company appears on the shareholder register of the company and also on a share certificate and this is in line with section 71 of the Act which defines a shareholder as *“a person whose name appears on the share register or appears as a shareholder on an application form”*

The 2013 Act requires that all directors /company secretaries and shareholders who should be natural persons provide identities when submitting the application for registration of a company. The identities that are accepted are driver’s license, passport, voter’s ID and national ID. On the other hand, legal persons provide their certificate of incorporation duly certificate and list of names of shareholders.

When there changes on the particulars of directors, shareholders or company secretary, the new information must be submitted to the Registrar of Companies within 28 days of the changes being

made. Failure to submit the changes may lead to penalties, which according to the Registrar of Companies Rules 2017 are K50, 000.00 when submitted within 25 working days after the prescribed time and K100, 000.00 when submitted beyond 25 days. These penalties are not dissuasive since they have not been revised in a very long time. They are currently being revised.

Further to this, Section 345 of the 2013 Act provides for penalties for any false or misleading information on any document submitted to the Registrar of Companies. At the moment, the Registrar General is working with the drafting section of the Ministry of Justice to come up with the schedule of penalties and the enabling regulations. The Ministry of Justice is also making regulations to enable the Registrar of Companies to collect beneficial ownership information which will further include penalties for non-compliance.

The assessment further revealed that there is a challenge in the timely access to information held by the Registrar of Companies. Currently, there is a partial database of all the company records in the Malawi Business Registration System (MBRS), which is an online registration system, as most of the records are in manual form. Although the law makes it mandatory for companies to file annual returns, and provides for fines to be levied for late filing, so far there is little enforcement.

#### **Business Names Registration under Business Registration Act of 2012**

Body corporates, partnerships and sole proprietorship are registered under the Business Names Act 2012, which came in force to replace the replaced Business Names Registration Act 1964. Under the 1964 Act, an applicant was required to submit a passport size photo and submission of a proper identification document. An ID was, however, not mandatory. However, under the Business Registration Act 2012, applicants are required to submit acceptable and verifiable identity documents such as passport, national identity, driver's licence and voter registration identification.

It is important to note that unlike the 1964 Act where the registration certificate had no expiration, the registration certificate under the 2012 Act expires after three years with an option of renewal.

The general requirements are summarised as follows;

- **Sole Proprietor:** These are businesses with a single owner. The documents required for registration are a completed registration form with details of the sole proprietor and a copy of a valid identity document of the applicant.
- **Partnership:** Applicants are required to submit a registration form, copies of identity documents of the partners and a copy of the Partnership Deed.
- **Body Corporate:** This refers to an entity owned by an incorporated company or trust. Applicants are required to submit registration form and copy of the certificate of registration.

### **Incorporation under Trustees Incorporation Act**

The Trustees Incorporation Act Cap 5:03 provides for registration of public trusts, charities and associations. For registration under this Act, applicants are required to submit a completed registration form containing information such as the name and postal addresses of the Trustees. Additionally, an applicant has to submit its constitution, a statutory declaration and minutes authorising the incorporation. Registration under this Act implies that the applicant is a body corporate with Trustees who are natural persons. Further, there is a requirement for the body corporate to file annual returns which contain names and postal addresses of previous and current trustees

### **Settlement/Private Trusts**

There is no domestic legislation that regulates settlement/private trusts. The principles applied in relation to settlement/private trusts are borrowed from common law and there is no requirement for registration. There is, hence, minimal jurisprudence on settlement/private trusts in Malawi.

For a private trust to be instituted there is a settlor, beneficiaries and trustees. In practice, there are some settlement/private trusts (mostly family trusts) with the settlor (most times being the head of the family) being also both beneficiary and trustee of the family trust.

In Malawi, besides not requiring the settlement/private trusts to be registered, the Deeds Registration Act requires the registration and payment of stamp duty on the settlement/private trust deeds for deed to be enforceable. Stamping is, however, not mandatory such that others opt not to register their settlement trusts.

### **Accessibility of Information by LEAs on Legal Persons and Arrangements Created**

Currently, there is no beneficial ownership registry in Malawi. However, there are initiatives for subsidiary legislation to be issued that will require disclosure of beneficial ownership information, with penalties for non-disclosure.

When LEAs need information of any company or registered business, they need to submit their request through a letter from the head of LEA or any officer who has authority to act in such a capacity. As there is a partial electronic database of the records for registered companies, businesses and incorporated trusts, some searches are still being conducted manually and thus may take three to five working days for information to be availed. Access to information by members of the public requires payment a fee and fill out a form indicating purpose of the information.

### **Features of Legal Arrangements That Make Them Particularly Vulnerable to ML**

The companies registered under the 1984 Act which have Family Trusts as shareholders present a risk to money laundering. Such companies are particularly vulnerable as it is not easy to identify the owners of a company as only the name of the family trust appears as a shareholder. There is high level of anonymity in such instances.

Companies which have foreign companies as holding companies registered under the 1984 Act equally present a risk to money laundering. The reason is that it is particularly difficult to identify owners of a Company as the registration requirements under the 1984 Act were not comprehensive, for instance the particulars of shareholders and the directors of the holding company and their identities were not provided. There is equally high level of anonymity with such companies. The commercial registry of Malawi does not ordinarily liaise with the company/commercial registry where the foreign shareholder is registered to validate the information supplied. The absence of a mechanism to verify the identities and residential addresses of directors and shareholders creates a great vulnerability. Further, there is no legal requirement for the disclosure of the beneficial owners at registration.

On the other hand, under the 2013 Act the risk levels are low, as only natural and legal persons can be shareholders. Unlike under the 1984 Act where a settlement/private trust could appear as a shareholder, the 2013 Act requires that only the names of the trustees appear as shareholders. In the case of a foreign company, the details of the directors and shareholders of the holding company are provided on registering.

Malawi has no legislation regulating Settlement Trust/Private Trust and there is no register for Private Trusts. This makes it difficult to identify and verify the beneficiaries of a particular Trusts. Additionally, businesses registered under the old Business Names Registration Act create a vulnerability as in some cases there was no valid identity provided as only passport size photos was used for registration purposes.

Furthermore, though there is a requirement to declare capital, there is no requirement to declare source of funds or source of capital at registration. This poses a risk for ML/TF as the sources used to start a business could be criminal proceeds. It would be ideal for AML/CFT purposes to require declaration of source of capital just like the FCA require reporting institutions to declare source of funds when entering into a business relationship.

#### *Case Examples where Legal Persons and Arrangements have been Used for ML*

Information sourced from the Malawi Police Fiscal and Fraud Unit of Malawi Police, ACB, MRA and DPP, indicate that there are. where legal persons and legal arrangements were used to hide proceeds of crime. It is apparent that LEA s are not aware of the wide range of legal persons and arrangements that are created in Malawi. The only common legal persons and arrangements that have been frequently searched by legal enforcement agencies are limited liability Companies; and Sole proprietorships and Partnerships under the Business Names Registration Act.

A research on the *cash-gate* cases revealed that most of the cases involved money laundering through contractors and suppliers, who had registered limited liability companies or as sole proprietors or partnerships under the Business Registration Act. Some registered their companies or business a few months or days before they received a fraudulent payment. as sole proprietors or partnerships. Examples of contractors/suppliers with limited liability companies used in *cash-gate* can be found in the following cases:

- The case of **Republic v Oswald Lutepo Criminal Case No. 02 of 2014 (HC) (Unreported)** where the defendant who was convicted of money laundering and conspiracy to defraud MK 4.2

billion from the Malawi Government used his business styled O & G Construction Limited Company;

- In the case of **Republic v Maxwell Namata and Luke Kasamba Criminal Case No. 65 of 2013 (HC) (Unreported)** the defendants, who were convicted of theft and money laundering for the amount of MK 24 million used a company named Cross Marketing Limited Company; and
- In the case of **Republic v Esnart Nenani Ndovi Criminal Case No. 1164 of 2013 (Unreported)** the defendant was convicted of the offence of lending a certificate of her Fusion Limited Company and laundering K 12.9 million (\$23,035) on her own plea of guilt.

Examples of cases where sole proprietorship or partnerships were used include:

- The case of **Republic v Carol Savala Criminal Case No. 28 of 2013 (HC) (Unreported)** who used her construction business styled Carmu Civil Engineering;
- In the case of **Republic v Oswald Lutepo Criminal Case No. 02 of 2014 (HC) (Unreported)** who used his business styled International Procurement Services;
- The case of **Republic v Angella Katengeza Criminal Case No. 26 of 2013 (HC) (Unreported)** where a fraudulent cheque was paid to the convict's business called Faith Construction;
- The case of **Republic v Wyson Dzinyemba** who used his business called Wymbaso General Dealers; and
- The case of **Republic v Allan Magombo Criminal Case No. 143 of 2014 (Unreported)** where suspect used his business called Down Stairs Lodge to launder stolen public funds.

In the *cash-gate* cases, the types of legal entities used, were not used because of the loopholes in the legal framework but simply because the registered businesses or companies were the ones that resources from government could easily be syphoned out through without easy detection. Essentially, since the legal arrangements were taken to be 'properly constituted' and conducting business with the government, funds were paid to the companies for apparent services or products 'presumably' offered and supplied.

On another note, there is currently a matter being prosecuted involving a company that was wrongly awarded a contract by a public authority, in which the CEO of the public authority was a beneficiary of the settlement trust that is a majority shareholder of the company.

## Financial Inclusion Products Vulnerability

### Background

As part of the ML/TF risk assessment, a complementary assessment was done on financial inclusion products. Financial inclusion products aim at providing financial services to low income earners and residents of remote areas, excluded from formal financial services.

Financial inclusion products have different names depending on the financial institutions and these include basic bank savings accounts, basic bank credit accounts, ordinary farmer bank account, mobile payments, mobile banking, local money remittance, member-based savings and credit, and micro-credit.



## Findings

### *Basic Savings Bank Account*

There are nine (9) commercial banks in the country, however only five responded to the questionnaire for this assessment. The five banks that responded to the questionnaire all offer basic savings account. The banks have various brand names for the basic savings account namely Student Saver Account, Fast account, Pafupi Savings Accounts and Bank on the wheel (Mobile Van) just to mention a few. The banks also apply slightly different measures to this product in terms of identification documents allowed, transaction limits and eligible customers. The product is being accessed by 185,357 customers from the five banks that responded.

Identification documents that used to open these accounts include; driving licences, passports, letter from a traditional leader, letter from an employer or association one belongs to, national voter registration card, employer identity card, Auction Holdings cards (tobacco selling company membership cards), student identity card and letter from college or school.

Specific findings for the product are as follows:

- The five banks use the threshold of K50,000 (US\$68.05)<sup>50</sup> for total monthly deposits or withdrawals per customer under this product. There is simplified due diligence that banks carry out when opening accounts for this product. It should, however, be noted that different accounts have different book balance limits for example, Ecobank Njatonse Saving Account has a book balance of K500 (US\$0.68) while Ecobank Savings Account has a book balance of K200 (US\$0.27). One bank indicated that there is no threshold on transaction value allowable for the product. The product is mainly offered to students whose flow of incomes varies based on the periods they are in school.
- There is no limitation on the number of transactions carried out per day or per month. The customers can as many times as they wish as long as the threshold value of K50,000 (US\$68.05) per month is not surpassed.
- The product does not provide for anonymity of the customers. All customers go through the normal KYC process namely filling account opening forms, presenting identification documents and ultimately being accepted by the banks after satisfactory fulfilment of the requirements. Likewise, simplified CDD is applied.
- Banks allow customers of this product to carry out transactions through both face to-face and non-face-to-face. Transactions can be conducted in banking halls, or through non-face-to-face means such as transacting at ATMs or using mobile banking to check balances, pay bills or transfer funds to other customers of the same bank.

---

<sup>50</sup> The rate used is 1US \$ = K735 based on the rate at the time of updating the NRA Assessment.

- One of the banks indicated that it allows cross-border transactions with this product, though it did not specify the jurisdictions involved. There is no limit on the amount of money that may be transferred through this account.
- There are no reports of any crimes or cross-border transaction from high-risk money laundering jurisdictions in the period of assessment.
- The banks only accept Malawian nationals residing in the country as customers with an exception of one bank that also accept non-Malawian nationals based in the country for the Student Saver Account if the customers provide passport copies and valid student residential permit to study in Malawi. Legal persons are not permitted to access this product.
- The players have to get approval from the RBM at the point of getting a license to offer banking services, which include basic and ordinary savings accounts. The banks are required to comply with directives and Regulations issued by the RBM from time to time.
- The sector is guided by the following legislative frameworks; FCA, FSA, Banking Act, Exchange Control Act and Regulations, and KYC Directive from RBM.
- Sections 23 and 29 of the FCA mandates all financial institutions to monitor transactions and report all suspicious transactions to the FIA.
- All financial institutions are regulated by RBM. In terms of AML/CFT supervision, they are supervised by FIA and there is a draft MoU between the FIA and RBM to delegate AML/CFT supervision of financial institutions to the RBM. In collaboration with the FIA, the RBM provides guidelines required for various operations of the banks in relation to preventing ML and TF. Following the passing of the Financial Crimes Act in February 2017, there are no specific guidelines for this product apart from the general guidelines issued for all products offered by the banks under the previous legislation.
- All financial institutions offering the product reported that they conduct AML/CTF trainings annually.

The ML vulnerability rating for this product was low based on the reasons that product is offered to customers who are mostly low-income earners and hence pose low ML risk.

The TF risk for this product is rated low considering that the product has never been suspected or linked to TF.

In conclusion, the basic savings account qualifies for financial inclusion. However, regulators need to work with the banks on revising volume and value of transactions upwards for all banks, use of cross-border transactions and foreigners accessing this product should be closely monitored.

### *Basic Bank Credit Account*

The basic bank credit account is a micro-loan product being offered by two banks and microfinance service providers to individuals and groups who are mostly low-income earners and those based in remote areas of the country. The customers are required to open a savings account with the bank and some are trained in basic business management skills. A total of 656,937 customers are accessing this product from one bank and various microfinance institutions which target both men and women while the other has about 45,000 customers and targets women only.

For identification, the banks accept letter from an employer, letter from a traditional leader, voter registration IDs, and Tobacco Control Commission IDs (for those who are tobacco farmers) as well as driver's licence and passport.

Specific findings for the product are as follows:

- There are 5 different forms of credit products offered by the banks targeting individuals or groups who run small-scale businesses. The customers who most times are women usually operate in groups of 3 to 30 people in order to access loans. The loan limits range from K30, 000 (US\$97) to K40, 000 (US\$130) per individual in a group or K300, 000 (US\$970) to K400, 000 (US\$1,300) for the group
- Anonymous transactions are not possible. The customers must be in groups or the individual should be well-known or properly identified in terms of residential address and the base of operating their business such as market places for them to access loans.
- Non-face-to-face operations are not possible as the groups or individuals have to repay their loans on a weekly or fortnightly basis.
- The banks only accept Malawian nationals residing in the country for this product.
- Every provider of this product is guided by the following legislative frameworks: FSA, FCA Banking Act; Microfinance Act, 2010; KYC Directive from RBM; and the ML&TF Regulations.
- The Financial Crimes Act, and Regulation 22 of the ML&TF Regulations oblige financial institutions to monitor transactions and report to the FIA all suspicious transactions.
- The product providers do not have automated system for monitoring suspicious transactions but indicated willingness to procure an automated system.
- There are no specific guidelines for this product.
- The level of training for the product providers is average as some key staff members are trained in AML/CFT. One of the providers of this product showed some commitment to promoting AML/CFT awareness among its employees. In March 2011, the bank trained 126 staff members in AML/CFT at three branches. The staff that were trained included

credit officers and supervisors, account opening officers and supervisors, tellers and their supervisors, risk officers and some support staff.

**ML/TF risk rating:** The ML risk for this product is low because the amounts involved are low in value and banks identify the customers through various means such as the identification documents as well as through their fellow customers of the bank who are in the same group with them or know them as people coming from the same community.

The TF risk is low since banks only allow Malawian nationals use this product.

### *Ordinary Farmer Bank Account*

Ordinary Farmer Bank account is an account which is offered by one of the banks in the country targeting small-scale farmers. Such farmers are usually based in remote parts of the country and most are semi-literate or illiterate. Most customers of this account open the account as part of a group (i.e. farmers' clubs). The farmers normally get the bulk of their earnings at once from sales of produce and then this is followed by frequent small or big withdrawals to help them in their farming endeavours such as purchase of farm machinery or other farm inputs.

Transactions in this account are usually for K300,000 (US\$408) and above. This applies to both individual or group accounts.

Specific findings for the product are as follows:

- Most customers are usually from rural and hard-to-reach areas, and usually come from Farmers Clubs. The accounts are used to collect proceeds from sales of annual produce or accessing micro-credit for their farming operations. The transactions for this class of customers are usually seasonal and at times the accounts become dormant until the next farming season.
- Customers are assigned their own banking suites or bank tellers where they can interact with the bank officers with ease.
- Identification documents presented by the customers include: voter registration ID, Auction Holdings cards (tobacco selling company membership cards), and a letter from traditional leaders.
- The customers are not involved in cross-border transactions and the product is accessed by Malawians only.
- Providers are guided by the following legislative frameworks; FSA Act; Banking Act; Exchange Control Regulations; KYC Directive from RBM; Financial Crimes Act; and the ML & TF Regulations.
- The Financial Crimes Act under Sections 23 and 29 and Regulation 22 of the ML & TF Regulations oblige all financial institutions to monitor transactions and report to the FIA all suspicious transactions.

- There are no specific guidelines for this product, apart from the general guidelines provided to banks on AML/CFT.

**ML/TF risk rating:** The ML risk rating for this product is low because customers mostly operate in groups and are well known to each other and sources of funds are easily identified. However, banks do not have proper transaction monitoring mechanism and farmers expect high values after sale of their produce but there are possibilities that some farmers may be involved in high value transactions outside the farming season. In such instances, banks request for the sources of funds when customers conduct transactions that appear to be unusual.

The product qualifies for simplified CDD. Regulators need to set specific guidelines and thresholds for farmer accounts and ensure that transactions are properly monitored.

## *Mobile Banking*

### **a. Background**

Mobile banking services allows bank account holders to access their accounts and make various transactions using the mobile phone. This service is different from internet-based or online banking as it does not require internet connectivity, but mostly uses the USSD functionality of the mobile phone. The common types of transactions for this product include balance inquiry, mini-statement, funds transfer to other accounts, payment for goods and services, utility bill payments and airtime top up. Mobile banking allows customer flexibility, convenience and reduces transaction costs as customers do not need to visit their bank branches for their transactions and, through use of USSD, ordinary mobile phones can be used and not just smartphones. Out of the 9 banks operating in Malawi, 5 are offering mobile banking, of which two offer interbank funds transfer functionality on their platform.

The product's impact on financial inclusion might not be significant as it caters for people who already have existing bank accounts. However, the potential impact could be in the add-on services or functionalities; for example, one of the banks allows subscribers to send money to non-customers which is then accessed through card-less ATM withdrawals. Clearly this has the potential to widen access to payment services to non-subscribers and/or unbanked. Over time such services can incentivise this segment to open bank accounts and/or subscribe to such services.

### **b. Findings**

Specific findings for the product are as follows:

- The transaction limits differ from bank to bank but range from K80,000 (US\$107) to K500,000 (US\$667), the latter being the regulatory stipulated limit for mobile banking and payments services.
- There are no limits on the number of transactions a subscriber is allowed as long as the total value per day is within the limit.

- All subscribers meet KYC requirements, since the product is offered to existing customers of banks. Only domestic transactions can be performed on the services.

#### c. Legal and Regulatory Environment

Banks are required to get the necessary approvals from the RBM before they roll out mobile banking services. The relevant legal instruments governing the services are therefore the FSA; Banking Act; Payment Systems Act, FCA and all other relevant regulations, directives issued under them.

**ML/TF risk rating:** The ML risk posed by this product is Medium because it is offered to already existing bank customers who may already have an inherent risk, and the transaction thresholds are low. However, regarding card-less ATM transmission of funds, the beneficiary may only be known and traced through their mobile telephone number.

The risk of TF is low because transactions are monitored and have thresholds.

The product does not qualify for simplified CDD as at the time the customer decided to use this product, CDD will have been done under the account type they decide to open. The determination for level of CDD will depend on type of customers and the type of account they open.

### *Mobile Money*

#### a. Background

Mobile money service is currently being provided by two existing telecommunication service companies namely: Airtel Limited and Telekom Networks Malawi (TNM); and one money transfer service provider known as Zoon Transactions limited. The product by Airtel and TNM is wallet based where by customers can initiate transactions from their wallets whilst the product by Zoon is non-wallet based and is offered through a network of agents. Mobile payments product is a mobile based financial service that allows subscribers (both banked and unbanked) to send and receive money, pay bills, and buy goods and services. It also allows for bulk payments, such as payment of salaries and loans.

#### b. Regulatory Framework

The RBM issued Guidelines for Mobile Payment Systems in March 2011 with the aim of facilitating the delivery of non-bank led mobile payment services to the banked and non-banked population in Malawi. In 2016, the Malawi Parliament enacted the Payments Systems Act which provides the legal mandate for RBM to regulate and oversee payment services in the country. In September 2017 the RBM issued the Interoperability Directive that mandates retail payment service providers to deploy open systems that can easily integrate with other payment systems and services. In October 2017, the RBM issued the Guidelines on Application and Authorisation of Payment Service Providers which supersedes the Guidelines for Mobile Payment Systems issued in March 2011.

#### c. Growth of the Product

As of October 2017, there were three mobile money service providers operating in the country. Two mobile telecommunication companies are operating mobile payments; Airtel Mobile

Commerce Limited has been offering the service since 2012 and TNM Limited since 2013. These providers have in place systems for monitoring transactions and stipulated thresholds. A third-party service provider known as Zoono Transaction Limited entered the market in 2015 with an agent-product that facilitates transfer of funds using a network of agents spread across the country. In contrast to the other two MNO-led services, customers of the Zoono product do not subscribe to the service and it also does not use a mobile-wallet. Instead, customers send and receive their money via the agents, and are required to produce an acceptable ID to the agent when doing their transaction.

Use of the subscription-based mobile money products requires compliance with KYC requirements. In addition to passports and drivers licence, other identification documents that are being used include a letter from an employer, letter from a traditional leader, voter registration ID and membership cards from recognised groups. If a customer would like to transact in large amounts, they have to present the main identification documents such as a passport or driver's license.

As of October 2017, Mobile Money providers had a total of 4.5 million subscribers and 29,929 agents spread across the country. The agents facilitate registration of customers, as well as cash in (receipts) and cash out (payments) services. Most of the customers especially those based in rural areas present simplified KYC documents when registering for the services.

#### d. Findings

Below are some of the specific findings for the product:

- Customers using simplified identification documents may only be allowed to transact up to certain limits set by the service providers based on their risk appetite. Customers can graduate to a higher level upon provision of formal identification documents such as a passport and a driver's license.
- Anonymity is not possible because only duly registered customers use this product.
- For MNO-led mobile payments, registration is done on face-to-face basis while transactions like sending funds, buying airtime or paying bills are non-face-to-face.
- Cross-border transactions can be performed based on the service provider. Currently there is one service provider conducting cross-border transactions.
- The product is offered to any individual resident in the country whether Malawian or not.
- Providers of the product have to be approved by RBM and are expected to adhere to the provisions in the Payments System Act 2016 and Interoperability Directive 2017. Other relevant legal instruments are the Financial Crimes Act, the Telecommunications Act.
- The providers have monitoring systems in place. They can identify suspicious transactions through their automated systems.
- Training in ML/FT is offered to staff and agents of mobile money service providers as part of building capacity for the officers to handle ML/TF related issues. The service providers are also committed to continue training their staff and agents in AML/FT.

**ML risk rating:** The ML risk posed by this financial inclusion product is low because the values of the transactions for customers that present simplified identification documents and that the strict limits set in the system make it more difficult for huge transactions to take place. .

Even though some operators allow for cross-border transactions, the countries in which the products are accessible are jurisdictions of low TF risk.

### *Local Money Remittance*

Due to low response rate on questionnaires administered, the assessment used information from the previous NRA (2013). Local Money Remittance is offered by Malawi Post Corporation (MPC) to enable people from various areas to send and receive money through the Malawi post offices. The product brands offered are:

- **Fast Cash:** This is an electronic funds transfer product, which allows a receiver to access funds in real time.
- **Postal Order:** Postal orders are transferred physically and usually take 2 to 7 days depending on the distance from the sender.

In 2011, a total of 452,330 people used Fast Cash and Postal Orders at MPC branches. Identification documents are required for recipients only. Documents allowed by MPC included voter registration ID, driver's license, passport, letter from an employer and letter from a traditional leader.

Specific findings for the product are as follows:

- There were no limits set for these products either on the value and number of transactions.
- Anonymity is possible on the part of the sender if he or she wants to use a false name while that could not be possible for the receiver as he has to present identification document at the point of collecting the money.
- The two products require face-to-face transactions at the point of both sending and receiving the money.
- The products are operated locally and not applicable for cross-border transactions.
- The products are designed to help Malawians remit funds to destinations within the country. Nevertheless, the products are also used by non-Malawian customers as long as the destination is within the country.
- The FSA, FCA, Communications Act and Payments Systems Regulations are the statutes that guide the providers. Apart from these, the RBM has in place draft Regulations for Money Transfer Agents.
- The Financial Crimes Act, and Regulation 22 of the ML Regulations 2011 oblige all financial institutions to monitor transactions and report to the FIA all suspicious transactions.



- The provider has an automated system in place which is used for transfers of funds and monitoring of transactions, however, the system does not monitor frequency of transactions carried out by specific customers and suspicious transactions that may take place.
- There were no specific guidelines for this product, and the RBM requires additional human resource to adequately undertake supervision of the product provider.
- Training of staff members of the product provider has not been adequate. Only 35 staff members of MPC were trained in AML/CFT in July 2011. The provider has a total staff compliment of about 900, a third of which are front officers who transact fast cash and money orders.

**ML risk rating:** The ML risk posed by this product is medium because the values of the transactions are usually low, however, there are no thresholds attached to this product and there are no controls on the number of transactions a person can conduct in a month.

The TF risk is rated low because the services are operated locally and no cross-border transactions are allowed.

It is recommended that specific guidelines for this product be developed and limits on number and value of transaction set. In addition, the regulator should work with the provider to raise awareness among staff members.

### *Member-based Savings and Credit*

Member based savings and credit products are offered by Savings and Credit Cooperatives (SACCOs). There are 34 licensed SACCOs operating in Malawi and are affiliated to the Malawi Union of Savings and Credit Cooperatives (MUSCCO).

SACCOs are formed based on a common bond among members and these include employee based and community based SACCOs. Members join SACCOs on the understanding that they will be making monthly savings and get credit according to the value of the savings accumulated by a member. Members can also buy shares of the SACCO as a way of investing their money. At the end of the year, members share the profits made based on the number of shares held.

The identification documents that are used by the SACCOs include letter from employer, letter from traditional authority or chief, witness ID (this is where one member of the SACCO group bears testimony of knowledge of a new member). They also accept driver's license and passport. All SACCOs, apart from United Nations SACCOs, do not allow non-Malawian citizen membership.

Specific findings for the product are as follows:

- SACCOs have no limits on number and value of transactions.
- Anonymity is not applicable as members are known to each other being employed in the same institution or belonging to the same community.
- Non-face-to-face transactions are not allowed.

- Cross-border transactions were also not allowed.
- The Financial Crimes Act under Sections 23 and 29, and Regulation 22 of the ML&TF Regulations 2011 oblige all financial institutions which include SACCOs to monitor transactions and report to the FIA all suspicious transactions.
- SACCOs have no AML/CFT monitoring mechanism.
- There are no automated processes available in any SACCO to monitor suspicious transactions. The monitoring is done manually.
- There are no specific guidelines at the moment for these products.
- There have not been any AML/CFT training for the sector.

**ML risk rating:** The ML risk posed by this product is medium because high value transactions are involved and there are no limits on the number and value of transactions and these features would be attractive to money launderers. In addition, SACCOs have no transaction monitoring mechanism to detect suspicious transactions. To mitigate this risk, SACCOs need to implement automated systems which would make it easy to monitor transactions and report any suspicious transactions to the FIA to reduce the ML risk. In addition, for the members that transact in large value transactions, there is a need to have thresholds and take more details for due diligence.

Since SACCOs are member based and transactions are local, the TF risk is low.

For the product to qualify for simplified CDD, specific guidelines and transaction thresholds need to be developed. In addition, the regulators need to work with SACCOs to raise AML/CFT awareness.

### *Micro-Credit*

There are 41 duly registered and licensed microfinance service providers offering micro-credit in Malawi as at September 2017. The microfinance service providers comprise 31 registered microcredit agencies, 9 licensed non-deposit taking microfinance institutions and one deposit taking microfinance institution.

The microfinance service providers are categorised into:

- Microcredit Agencies (MCA) - provides credit only;
- Non-Deposit Taking MFIs (NDTI)- provides credit plus other microfinance services but cannot mobilise deposits; and
- Deposit Taking MFIs (DMFIs)-can mobilise deposits and provide other MF services.

Microfinance service providers offer group and individual loans in the form of business, agricultural, emergency/salary advance, educational, mortgage, and non-mortgage housing loans. To access these products, customers need to provide identification documents, which include driver's license, passport, letter from an employer, letter from a traditional leader, letter from a landlord, witness ID, employment ID and village bank passports.

Out of all the registered institutions, 41 institution responded to the questionnaire for this assessment. Reliance was thus placed on quick phone interviews with some of the institutions and information from the RBM databases. The microfinance sector has a total of 323,731 customers and is offering the product to Malawians only.

Specific findings for the product are as follows:

- There were no regulatory limits on the number and value of transactions. The providers develop their own thresholds which are applicable to individual and group customers.
- Anonymity of customers was not applicable as customers needed to be identified as individuals or groups.
- Acceptance of non-face-to-face relationship creation is not applicable for this product.
- Cross-border transactions are not permitted as the product is designed to be used by customers within the country only. Further it is specifically offered to Malawians only.
- The Financial Crimes Act under Sections 23 and 29, and Regulation 22 of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Regulations 2011 oblige all financial institutions to monitor transactions and report to the FIA all suspicious transactions.
- There are no specific guidelines to address ML/TF risk.

**ML risk rating:** The ML risk posed by this product is low because the transaction values are generally low and mostly accessed by groups whose members are known to each other.

The TF risk for this product is **Low** because CDD is done on the customers when accessing services from the institutions.

### Recommendations

Financial inclusion is a very important ingredient of a country's financial system and requires deliberate effort to promote it. The following are therefore recommendations to promote financial inclusion in Malawi:

- a) A standard basic savings account targeting low income Malawians should be introduced by all providers with attributes that qualify it for simplified CDD.
- b) Products that qualify for simplified CDD should be monitored regularly to ensure that customers that exceed the set thresholds undergo enhanced CDD.
- c) The requirement in regulations for transaction threshold of K50, 000 per month for customers under simplified identification requirements is on the lower side in view of current economic environment. In view of this, it is recommended that the threshold should be raised upwards.

- d) Regulators should develop specific guidelines for all financial inclusion products to ensure that the products are in line with AML/CFT requirements.
- e) The RBM and the FIA should reach out to providers of financial inclusion products with AML/CFT awareness programmes.
- f) Institutions need to implement transaction monitoring mechanisms in order to allow for any suspicious transactions to be easily detected and report to the FIA

## CONCLUSION

---

This is a very significant document as it will guide the country in terms of understanding the criminal activities generating high proceeds that are vulnerable to ML/ TF. The assessment has also helped the country to identify the level of ML and TF vulnerability for each of the financial sectors, DNFBP sectors, NGOs and categories of legal persons and arrangements in the country. Further, the country has assessed financial inclusion products in terms of their level of ML vulnerability and they can benefit from assessment of financial sectors.

The findings in this assessment will lead to the development of an action plan to strategically address the risks identified at national, sectoral and institutional level. Institutions that participate in the national risk assessment are encouraged to use the report to help them identify the risk in their sector and institutions and to develop their action plans in line with this assessment to address the identified risks.



APPENDIX 1 – NRA ACTION PLAN

ML THREAT

Source Of ML/TF Threat	Key Action	1° Agency	2° Agency	Detailed Action Plan	Time Frame																							
					YEAR 1												YEAR 2											
					J	F	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O	N	D
LEAs focus is on predicate crimes only	The focus of investigations and prosecutions should also include identification, recovery and confiscation of proceeds of crime.	FIA	All LEAs	LEAs should have financial investigators specialising in Net Worth Analysis and Asset forfeiture																								
				Enhance capacity of LEAs in handling of seized assets																								







Source Of ML/TF Threat	Key Action	1° Agency	2° Agency	Detailed Action Plan	Time Frame																																								
					YEAR 1												YEAR 2																												
					J	F	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O	N	D																	
investigators, presiding officers, asset forfeiture investigators and other Law Enforcement Agencies	prosecutors and judicial officers to enhance their capacity		Immigration	specific needs for the various LEAs	█	█	█																																						
				Seek financial and technical assistance from central government and cooperating partners to train officers			█	█	█																																				
				Undertake training for the identified officers in these institutions					█	█	█	█	█	█	█	█	█																												
				Develop and implement measures to retain trained officers in those institutions/sections					█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█
Integrity failure among investigators, prosecutors	Establish enforceable policies and procedures to	FIA	MoJ, ACB, MPS, MRA,	Hold workshops with heads institutions on the need to check on staff integrity	█	█	█																																						









Source Of ML/TF Threat	Key Action	1° Agency	2° Agency	Detailed Action Plan	Time Frame																							
					YEAR 1												YEAR 2											
					J	F	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O	N	D
passports and driving licence			Tourism . Registrar of companies	financial background before issuing business and permanent residence permits																								
				Immigration and Malawi Investment and Trade Centre (MITC) to enhance and intensify inspections for illegal and unsanctioned trade by forcing traders.																								
Inadequate supervision of securities and remittance service providers sectors	Intensifying patrols on uncharted cross border routes to control movement of Cash , goods and people	Immigration, MPS	Ministry of Defence (MOD)	MPS to monitor movement of people and goods on uncharted border routes to minimise cross-border movement of un-authorized people, goods and cash.																								











Source Of ML/TF Threat	Key Action	1° Agency	2° Agency	Detailed Action Plan	Time Frame																																					
					YEAR 1												YEAR 2																									
					J	F	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O	N	D														
the RBM and FIA	perpetrated by staff are reported to RBM and FIA.			are reported to RBM and FIA.																																						
Inadequate internal controls in the banks	Banks should enhance internal controls to prevent and detect fraud	Banks	FIA, RBM	Banks should enhance internal controls to prevent fraud.																																						
	BAM should maintain updated list of Individuals involved in fraudulent activities. The information should be used by banks to screen staff at the point of employment and on an on-going basis	Banks, BAM	FIA, RBM	BAM should maintain updated list of Individuals involved in fraudulent activities. The information should be used by banks to screen staff at the point of employment and on an on-going basis																																						







Source Of ML/TF Threat	Key Action	1° Agency	2° Agency	Detailed Action Plan	Time Frame																																					
					YEAR 1												YEAR 2																									
					J	F	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O	N	D														
				<p>typology reports to be shared to the industry</p> <p>The RBM to also include administrative sanctions for the insurance sector</p>																																						
Effectiveness of supervision and practices	Finalise the MOU	FIA	RBM, industry associations	The FIA and RBM need to finalise their MOU so that their roles as regards AML supervision oversight are clear.																																						
Availability and effectiveness of entry controls	Inclusion of AML requirements as part of entry control conditions	RBM	FIA, Industry associations	RBM should align its entry controls for the insurance sector with those of the other financial sectors such as banks and capital markets which include AML issues																																						
Integrity of staff in	need to impose stiffer penalties	FIA	RBM, industry	The insurance entities should conduct regular screening of existing staff in order																																						





Source Of ML/TF Threat	Key Action	1° Agency	2° Agency	Detailed Action Plan	Time Frame																							
					YEAR 1												YEAR 2											
					J	F	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O	N	D
				i. AML compliance functions which meet international standards ii. reliable system of identification iii. reliable transaction monitoring and reporting systems iv. beneficial ownership information v. independent audit systems of the compliance function iv. ML risk identification and management systems																								
Effectiveness of Suspicious activity and monitoring	Monitoring and Detection of suspicious activity	FIA	RBM, industry associations	Systems need to be put in place to monitor and detect																								



















Source Of ML/TF Threat	Key Action	1° Agency	2° Agency	Detailed Action Plan	Time Frame																							
					YEAR 1												YEAR 2											
					J	F	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O	N	D
Lack of robust suspicious transaction monitoring systems for providers of financial inclusion products	Improve monitoring of transactions for financial inclusion products with regard to ML/TF	FIA, RBM	Reporting institutions	Meetings with individual financial institutions regarding suspicious transaction monitoring systems to help them understand important of monitoring transactions and identify problems in STR reporting process																								
				Acquisition of suspicious transactions monitoring systems by all financial institutions																								
				Training by reporting institutions for its staff on the acquired transaction monitoring system																								
				Training for reporting institutions																								



Source Of ML/TF Threat	Key Action	1° Agency	2° Agency	Detailed Action Plan	Time Frame																							
					YEAR 1												YEAR 2											
					J	F	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O	N	D
Lack of specific AML/CFT Guidelines for some financial inclusion products	Develop AML/CFT Guidelines for all financial inclusion products	RBM/FIA	Banks, micro-finance institutions, SACCOs, Airtel, TNM and Zozona	Development of AML/CFT Guidelines for banks and other institutions such as SACCOs and mobile money service providers																								
				Revision of thresholds such as the K50,000 threshold for basic bank savings account need to be revised while thresholds need to be developed for SACCOs, micro-finance institutions, local remittance																								
Inadequate supervision of financial inclusion products by the regulators	Develop capacity of the RBM and the FIA to conduct more supervision	FIA, RBM	Banks, micro-finance institutions, Malawi Posts Corporati	Recruitment of additional staff members by the RBM (bank, micro-finance and other institutions supervision departments) and the																								









Source Of ML/TF Threat	Key Action	1° Agency	2° Agency	Detailed Action Plan	Time Frame																							
					YEAR 1												YEAR 2											
					J	F	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O	N	D
Lack of a trusted NGO Governance Institutions	Improve governance structure of all NGOs to implement the provisions of the mandatory legislation (NGO Act)	Ministry of Gender	NGO Board, CONGOMA	Awareness campaign on the mandatory registration according to NGO Act	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█					
				Hold meeting with relevant stakeholders on issues of the mandatory registration for all NGOs		█	█							█	█			█	█						█	█		
				Procedures in place for rigorous verification of NGOs before registering them	█	█	█																					
Lack of reporting compliance by NGOs	Increased number of NGOs submitted their annual reports to NGO Board	Ministry of Gender	NGO Board	Awareness campaign on mandatory reporting requirements by NGO Act	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█					
				NGO Board commit annually funds on NGO activities				█																				



Source Of ML/TF Threat	Key Action	1° Agency	2° Agency	Detailed Action Plan	Time Frame																							
					YEAR 1												YEAR 2											
					J	F	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O	N	D
Lack of information sharing	Develop mechanism that will enhance information sharing among institutions	FIA and NIB	NGO Board and CONGOMA	MOUs among FIA, NIB, CONGOMA and NGO Board on information sharing		█																						
	Procedures on how to handle cases of AML/CFT					█																						
	Hold meetings with financial institutions, NGO Board, CONGOMA and MDAs											█																
<b>LEGAL PERSONS AND ARRANGEMENTS</b>																												
Lack of Legal Framework Enabling the Registrar General to Collect Beneficial Ownership information for Legal	Adoption of a legal framework enabling the Registrar General to Keep BO information and sanction non-compliance	RG, FIA, MWEIT	MoJ- Drafting	Government needs to expedite the adoption of Registrar's Regulations enabling the collection and retention of BO information. Meeting of relevant stakeholders to finalise the Draft																								









