SUMMARY OF THE MONEY LAUNDERING AND FINANCINGOF TERRORISM NATIONAL RISK ASSESSMENT OF ZIMBABWE

JUNE 2015

1. NATIONAL RISK ASSESSMENT OVERVIEW

1.1. Purpose of the NRA

1.1.1. Zimbabwe's first Money Laundering and Financing of Terrorism National Risk Assessment (NRA) was officially launched on 31 July, 2014. Preparations, however, had already started in June 2014, when the National Risk Assessment Coordination Committee was formed, under the auspices of the National Task Force on Anti Money Laundering and Counter Financing of Terrorism.

1.1.2. A money laundering and counter financing of terrorism NRA is conducted for the purpose of identifying, assessing and understanding the money laundering (ML) and terrorist financing (TF) risks facing a country, with a view to coming up with effective measures to mitigate the identified risks.

1.1.3. An NRA enables countries to mitigate the identified ML/TF risks in a cost effective manner by focusing more resources towards the high risk areas and less resources towards the lower risk areas.

1.1.4. An NRA, among other things, assists in identifying financial leakages and illicit flows within as well as across the country's borders. These leakages and illicit flows have a negative effect on national revenue collection targets as well as a negative impact on the national current and capital accounts.

1.1.5. The need to minimize leakages is also a vital pillar for the Zimbabwe Agenda for Sustainable Socio-Economic Transformation (ZIMASSET).

1.1.6. An NRA facilitates the effective implementation of AML/CFT measures, which enhances the integrity of the country's financial and economic sectors. Financial integrity is one of the preconditions for attracting much-needed foreign investment.

1.1.7. Apart from the NRA being a national necessity, it was also undertaken as part of the country's regional and international obligations in the global fight against ML and TF. An NRA is a requirement under the Financial Action Task Force (FATF), AML/CFT Standards. It is also a necessary prerequisite for all member countries of the Eastern and Southern Africa Anti Money Laundering Group (ESAAMLG) ahead of the Second Round of Mutual Evaluations.

1.2. Stakeholder Participation

1.2.1. The NRA is a multi-stakeholder process, involving regulatory authorities, law enforcement agencies as well as various government Ministries and departments. The process received high level Government support and stakeholder buy-in and participation from the start up to this stage of the process.

1.2.2. The National Task Force on AML/CFT provided a strong platform for cooperation and coordination of the NRA process.

1.2.3. The NRA process benefited immensely from the high level political commitment and stakeholder awareness that had been generated during the period when Zimbabwe undertook comprehensive reforms on the country's AML/CFT legal and institutional framework, in close cooperation with regional and international AML/CFT stakeholders, such as ESAAMLG and the FATF.

1.2.4. The National Risk Assessment Coordination Committee, which has been responsible for gathering and analyzing national data and coming up with the NRA results, consisted of participants seconded by the following organizations:

- The FIU,
- Ministry of Finance and Economic Development,
- Ministry Of Justice, Legal and Parliamentary Affairs,
- Ministry of Mines and Mining Development,
- Ministry of Home Affairs,
- The Attorney General Division,

- Zimbabwe Republic Police,
- Border Control and Minerals Unit,
- CID Fraud Squad,
- National Security Service,
- Zimbabwe Revenue Authority,
- National Prosecuting Authority,
- Department of Immigration,
- Zimbabwe Anti-Corruption Commission,
- Reserve Bank's Exchange Control Division,
- Reserve Bank's National Payments Division,
- Reserve Bank's Bank Supervision and Licencing Division,
- Securities and Exchange Commission,
- Insurance and Pensions Commission,
- Law Society of Zimbabwe,

1.3. The NRA Process and Methodology

1.3.1. The NRA exercise has been conducted in structured phases.

Phase One: Preparations and Planning

1.3.2. The initial phase consisted of preparations and planning on how to conduct the NRA process, including –

- Constituting the National Risk Assessment Coordinating Committee
- Designation of the Financial Intelligence Unit (RBZ) as Lead Agency and Secretariat
- Identification and engagement of relevant stakeholders
- Choice of NRA Tool to use in the process (World Bank Tool)
- Appointment and training of NRA Team Leaders
- Convening of an initial All Stakeholders' Workshop to explain the NRA process. The workshop was held at the Reserve Bank of Zimbabwe offices, on 31 July, 2014, signaling the official launch of the NRA process.

1.3.3. The workshop attracted a high turn-out of 156 participants, representing 91 institutions from both the public and private sectors.

Phase Two: Data collection and Analysis

1.3.4. This exercise involved gathering data to assess the national ML/TF threats and ML vulnerability.

1.3.5. The NRA Coordinating Committee constituted nine sub-groups or teams. The sub-groups mirrored the structure of the NRA Tool which is structured into nine modules. Each module focused on a specific thematic area of the NRA as follows:

- Module 1: - Money Laundering Threat,
- Module 2:- National Vulnerability to ML,
- Module 3:- Banking Sector Vulnerability to ML,
- Module 4:- Securities Sector Vulnerability to ML,
- Module 5:-Insurance and Pensions Vulnerability to ML
- Module 6:-Other Financial Institutions Vulnerability to ML
- Module 7:-DNFBPs Vulnerability to ML
- Module 8;-Financial Inclusions Products Vulnerability to ML
- Module 9.TF Risk in Zimbabwe.

1.3.6. The module teams were responsible for collecting data for their respective thematic areas, required for inputting into the NRA tool.

1.3.7. Each Module Team then came up with a report covering its area.

Phase Three: Compilation and consolidation of sectoral reports

1.3.8. This involved consolidation of the reports of the various working groups into the national report.

1.3.9. The NRA National Coordinating Committee then convened a three-day workshop held in the town of Kadoma, during the dates 12-14 December 2014.

1.3.10. The workshop, which was attended by all NRACC members and representatives of each Module Team was held to consolidate and review the NRA Results.

Phase Four

1.3.11. The intervening period between Phase 3 and Phase Four was spent cleaning up the detailed report, then sharing the draft report with key national stakeholders.

1.3.12. The draft report was also shared with the World Bank for their technical input and comments.

1.3.13. This phase also involved a discussion and review of the draft report and coming up with a draft detailed action plan to address the deficiencies identified by the report. This process took place at another workshop held in Kadoma, which was attended by all members of the NRA Coordinating Committee.

1.4. The World Bank NRA Tool and Technical Assistance

1.4.1. The country utilised the National Risk Assessment tool developed by the World Bank. The World Bank granted Zimbabwe permission to use its tool and also offered technical advice on the correct use of the tool.

1.4.2. The World Bank also provided funding for a number of workshops that were necessary for carrying out the NRA.

1.4.3. The process of gathering and analysing the required data and extracting and reviewing the results, was undertaken solely by the multi-stakeholder National Risk Assessment Coordinating Committee.

1.4.4. The IMF has also developed a tool for assisting countries to conduct their NRAs. The country opted for the World Bank tool because it was easier for stakeholders to understand and use.

1.4.5. A country's overall ML / TF **risk** is a combination of the country's ML/TF **threats** and **vulnerabilities**.

1.4.6. The country's ML/TF risks were, therefore, arrived at from an analysis of the ML/TF threats and the ML/TF vulnerabilities.

- The ML ***threat*** analysis focuses on collecting and analyzing relevant data in order to identify the prevalent crime types (predicate offences) that pose a threat in the country and that generate illicit proceeds. It also seeks to identify the origins of proceeds (both domestic and foreign) as well as the money laundering trends and methods.
- TF threat analysis, on the other hand, seeks to assess the level and sources of TF using statistics and other relevant information.

- The ML / TF ***vulnerability*** analysis assesses the vulnerability (weaknesses that can be exploited for ML purposes) of various components of the AML/CFT framework, namely –

  (a) Legal / judicial institutional framework, e.g.
    - Criminal justice and legal environment
    - Strengths and weaknesses in current AML/CFT legislation,

  (b) Political and Economic environment, e.g.,
    - Level of political commitment to fight crime,
    - Adequacy of human, financial and other resources to fight crime,
    - Average earnings of the population
    - Size of the Financial Services industry,
    - Nature of payment systems

  (c) Social and Geographical environment, e.g.
    - Cultural factors and nature of civil society,
    - AML/CFT regime not well understood and implemented,

1.4.7. For each of the indicators above, a threat, vulnerability or risk level is assessed based on the information and statistics provided.

2. SUMMARIZED NATIONAL RISK ASSESSMENT FINDINGS

2.1.Overall National Money Laundering Risk Rating

- Zimbabwe's ML threat was found to be **high**.
- National vulnerability to ML was found to be **medium**.

Overall Threat						
	High	M	M	MH Zimbabwe overall Risk Rating HERE.	H	H
	Medium High	M	M	MH	MH	H
	Medium	ML	M	M	MH	MH
	Medium Low	ML	ML	M	M	M
	Low	L	ML	ML	M	M
		Low	*Medium Low*	*Medium*	*Medium High*	*High*
		Overall vulnerability				

Zimbabwe's ML risk was, therefore, found to be Medium-High.

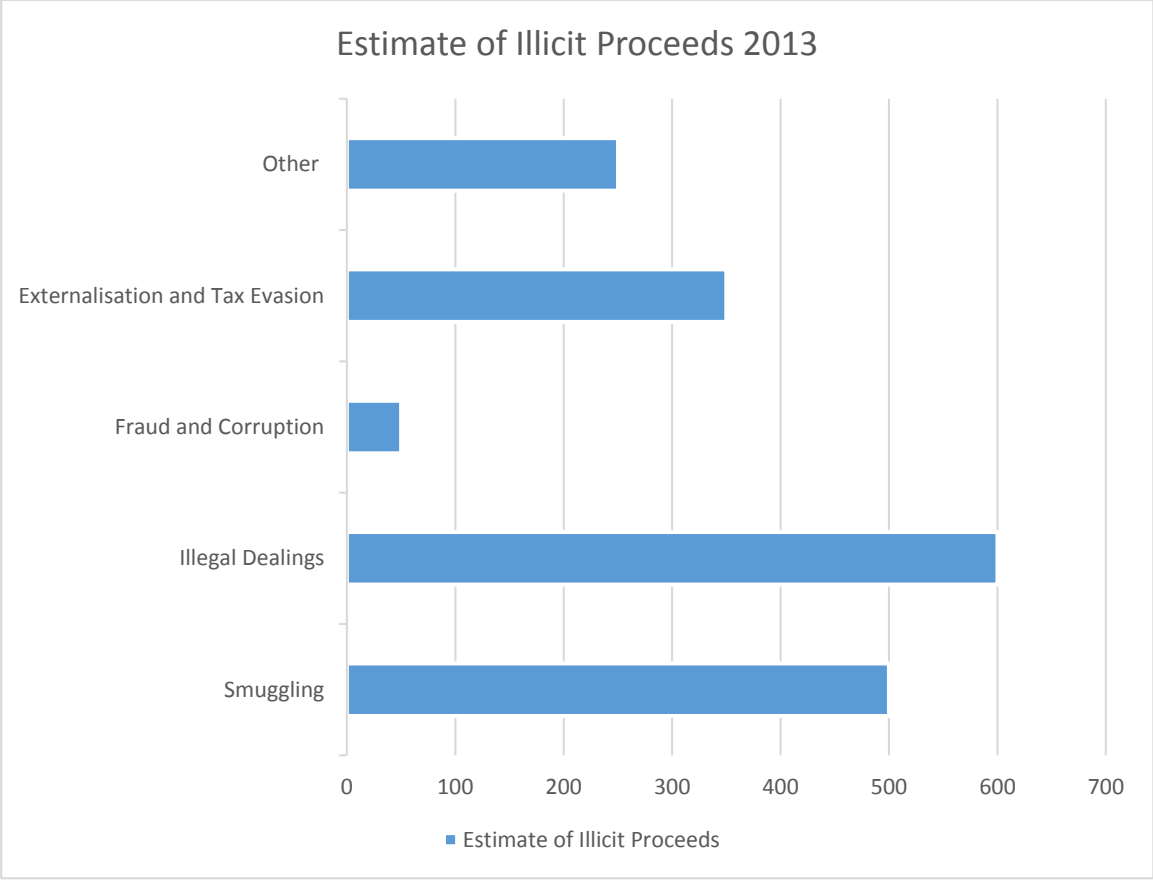
- Zimbabwe's risk to Terrorist Financing was rated low. No evidence was found to suggest the existence of terrorist groups or of persons or entities involved in financing terrorism.
- The Terrorist Financing risk assessment, however, recognized the need for continued vigilance.

The national ML risk rating is a product from the findings of the separate modules as summarized below:

2.2. National Threat Assessment, Module 1

(a) Predicate Offence Threat Analysis

- This module assessed the national ML threats by identifying the main types of offences that generate proceeds of crime in the country.
- The four major predicate offences in Zimbabwe, in terms of volume of proceeds generated, are:
  - (i) smuggling (in and out);
  - (ii) illegal dealing in gold and precious stones;
  - (iii) corruption;
  - (iv) fraud; and
  - (v) Tax evasion.
- All these offence types together generated an estimated US$1.8 billion of illicit proceeds in the year 2013



(b) Sectoral Threat Assessment.

- Taking a sectoral view, the NRA assessed the five key sectors in the economy and these were rated as follows in terms of their ML risk:

SECTORAL THREAT	RANKING	BASIS
Banking Sector	1	Most of the Predicate Offences Channeled Through Banks.
DNFBPS	2	The Real Estate Sector, Mining as well as Second Car Dealers were associated with proceeds from predicate Offences.
Other Financial Institutions Sector	3	Reports and Activity in this sector were relatively moderate.
Insurance and Pensions Sector	4	In terms of predicate offences and trends of ML, the sector was relatively moderate.
Securities Sector	5	No major predicate offences were registered in this period.

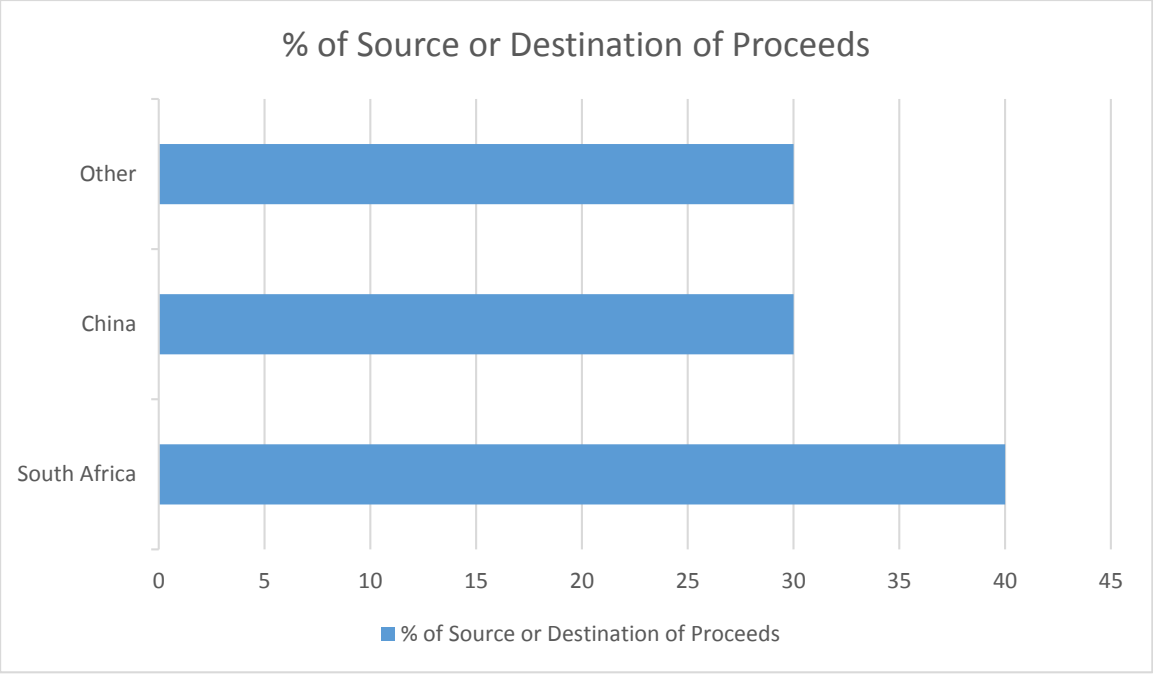
- The Banking Sector and the DNFBP sectors were found to be the most vulnerable, while ***Other Financial Institutions***, ***Pensions and Insurance*** and the **Securities Sector**, followed in that order.

(c) Source and Destination Threat Analysis

Regarding destination, proceeds of crime from Zimbabwe were found to be destined mostly to the following jurisdictions, in order of value, starting with the highest -

- South Africa (minerals and tobacco, and scrap metals, mainly copper),
- (ii) China, (cash being externalized by businesses);

- (iii) Botswana, (minerals, fuel and fraud);
- (iv) Mauritius, (proceeds of externalization),
- (v) UK/BVI (Proceeds of externalization and proceeds from smuggling of gold)
- (vi) United Arab Emirates (Dubai) (proceeds from music and video piracy as well as gold and other precious minerals).



Proceeds of crime into Zimbabwe were found to come mostly from the following jurisdictions, Mozambique and Malawi (drugs and second hand goods), (ii) South Africa (proceeds from tobacco smuggling and gold smuggling) and (iii) Zambia (poaching and tobacco smuggling).

2.3. National Vulnerability Assessment - Module 2

2.3.1. This module assessed Zimbabwe's overall vulnerability to ML. In assessing the country overall vulnerability, the module reviewed:

(a) the country's ability to deter and dissuade ML, (i.e. a review of its combating ability) and

(b) The vulnerability of each of the key economic sectors.

2.3.2 It is these two components, (i.e. combating ability and sectoral vulnerability), assessed together, that produce the national vulnerability rating.

2.3.3 Strengths and weaknesses of the country's AML/CFT regime

2.3.3.1 This module assessed legal /judicial / institutional vulnerability in order to determine the strengths and weaknesses of the country's law enforcement, prosecutorial and judicial elements that are key to an effective AML/CFT regime.

2.3.3.2 The module also considered other national structural issues that are important for the effective operation of an AML/CFT regime.

2.3.3.3 The assessment looked at the following 24 variables that are relevant to the country's AML/CFT framework:

- Capacity of presiding officers
- Capacity of prosecutors
- Integrity of prosecutors
- Policy implementation
- Asset forfeiture investigation
- Financial crime investigation
- Integrity of presiding officers
- Formalization of economy
- Corporate trust transparency
- Integrity of asset forfeiture investigators
- Criminalization of Money laundering
- Criminal penalties
- Domestic Co-operation
- International Co-operation in Criminal Matters
- Capacity of Presiding Officers
- Asset Forfeiture Laws
- Asset Forfeiture Orders
- International Cooperation in Asset Forfeiture

- Auditing and Accounting Standards and Practices
- Tax Disclosure
- Identification Infrastructure
- Availability of Independent Information Sources
- Financial Integrity
- STR data analysis.

2.3.3.4 An analysis of these 24 variables identified the following high vulnerability areas –

- Capacity and Integrity of Financial Crime Investigators.
- Capacity and Integrity of Presiding Officers.
- Policy Implementation.
- Asset Forfeiture.
- Formalization of Economy.
- Corporate trust and Transparency.

2.3.4 ***Sectoral vulnerability (financial institutions and DNFBPs)***

- This component of the national vulnerability assessment assessed the ML vulnerability of each of the key economic sectors of the economy, i.e. all the financial institutions and DNFBPs.
- The finding was that Designated Non-Financial Businesses and Professions (DNFBPs) are the most vulnerable, followed by the Banking Sector, with Other Financial Institutions coming third. The Securities and Insurance and Pensions sectors were found to be the least vulnerable to ML.

SECTORAL VULNERABILITY	RANKING	RISK RATING
Banking Sector	1	0.58
DNFBPS	1	0.58
Other Financial Institutions Sector	3	0.50
Insurance and Pensions Sector	4	0.32
Securities Sector	5	0.21

2.4 Banking Sector Vulnerability Assessment- Module 3

2.4.1 While module 2 dealt with the broader picture of national vulnerability, module 3 represented a detailed ML vulnerability assessment of the banking sector.

2.4.2 The module gives an analysis that sheds more light on why in the vulnerability assessment the Banking got its rating.

2.4.3 The assessment in this module was two-fold:

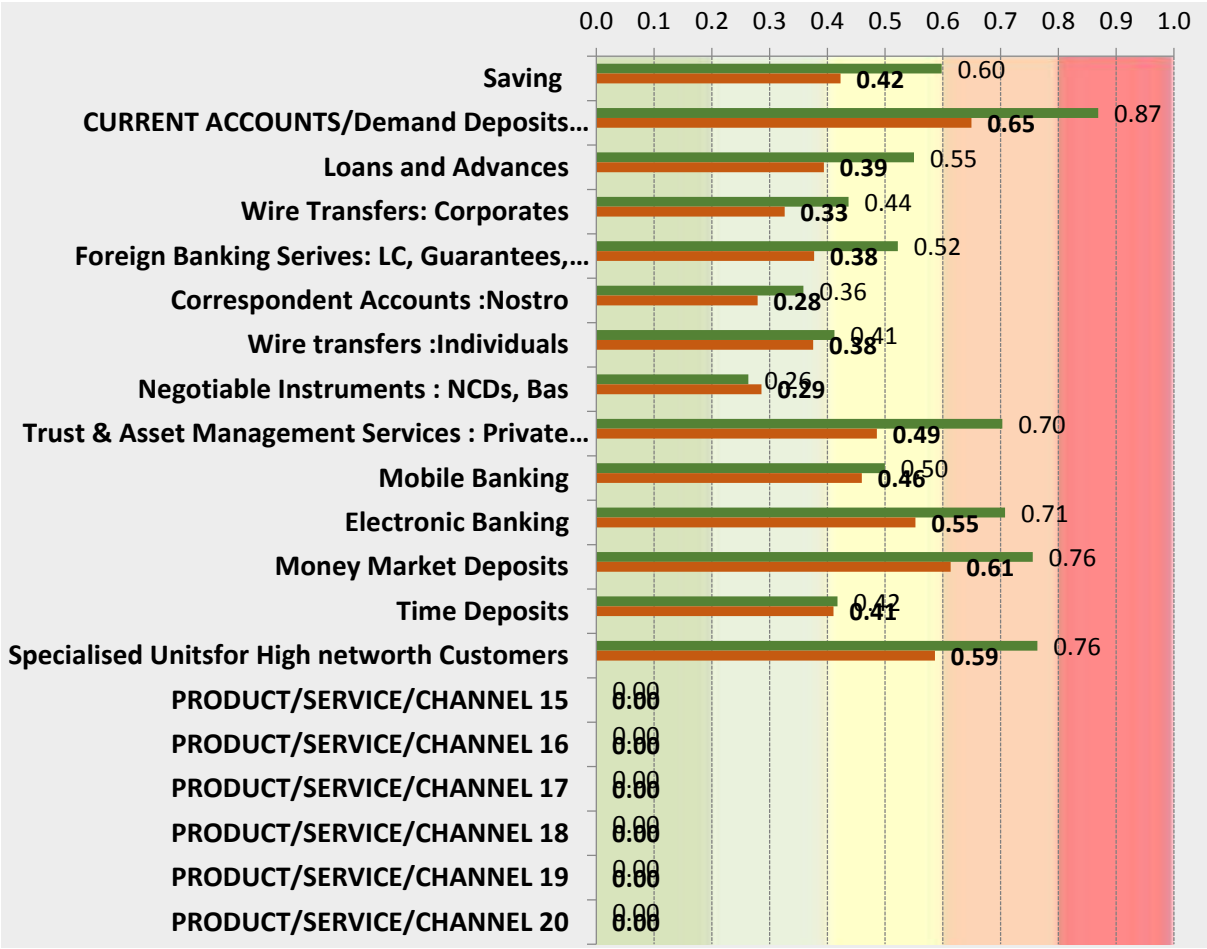
(a) An analysis of thirteen (13) general AML vulnerabilities as well as controls that exist and operate within the sector, and

(b) An assessment of the ML vulnerability of the thirteen (13) banking products that were found to exist within the country.

2.4.4 The general input variables that were considered were rated as follows:

	Input Variable	Rating
1	AML Laws and Regulations (preventive measures and supervision)	(0.9) Close to Excellent
2	Quality of AML Supervision	(0.6) Medium High
3	Market Pressure to Meet AML Standards	(0.8) High
4	Commitment to Good Corporate Governance	(0.7) High
5	Penalties	(0.6) Medium High
6	Enforcement of AML Obligations	(0.5) Medium
7	Staff Integrity	(0.7) High
8	Staff Knowledge	(0.7) High
9	Compliance Function	(0.8) High
10	AML Monitoring Systems	(0.6) Medium High
11	Corporate and Trust Transparency	(0.6) Medium High
12	Identification Infrastructure	(0.9) Close to Excellent
13	Availability of Independent Information Sources	(0.8) High

2.4.4 The banking products available in Zimbabwe were assessed for their vulnerabilities, specifically reviewing their inherent vulnerability characteristics as well as the general AML controls applicable to the products.



2.5 Securities Sector Vulnerability Assessment- Module 4

2.5.1 The Securities sector was found to be the least vulnerable out of the five sectors that were assessed, with a vulnerability rating of 0.21

2.5.2 The low vulnerability of the Securities Sector is a combination of several factors. Transactions on this sector generally do not involve cash, as most of the transactions or pass through the banking channels, where they are subject to the requisite CDD, KYC and related controls.

2.5.3 Furthermore, due to the prevailing economic conditions, characterized by general illiquidity, the Sector has over the last few years witnessed a significant decline in activity as far as investments are concerned.

2.5.4 The sector is also generally well-regulated for AML/CFT purpose, thereby making the sector less susceptible to ML.

2.5.5 The little measure of vulnerability that exist in this sector is attributable to the fact that the Securities Sector is exposed to international transactions more than most of the other sectors.

2.6 Insurance and Pensions Sector Vulnerability Assessment- Module 5

2.6.1 As with the Securities Sector, vulnerability to ML was found to be low in the Insurance and Pensions Sector. The sector's ML vulnerability was rated at 0.32.

2.6.2 Most Insurance and Pension funds are group-related funds and /or related to employee benefits. The nature of such funds does not therefore present a significant ML vulnerability, thus the low vulnerability rating of this sector.

2.6.3 This sector's vulnerability rating is only higher than that of the Securities Sector on account of weak controls and enforcement of AML/CFT obligations.

2.7 "Other Financial Institutions" Vulnerability Assessment - Module 6

2.7.1 This module assessed three clusters namely:

(i) Bureau de change,

(ii) Money Transfer Agencies and

(iii) Micro Finance Institutions.

2.7.2 The aggregated vulnerability rating for this sector was found to be medium, at 0.51, being the weighted average of the three clusters whose individual ratings were –

- Micro Finance Institutions, with a vulnerability rating of 0.51,
- Money Transfer Agencies (0.43); and
- Bureau de Change (0.7)

CLUSTER	Vulnerability Rating	WEIGHTING	WEIGHTED AVERAGE
Micro Finance	0.51	5	3.5
MTAs	0.43	4	1.7
Bureau De Change	0.7	4	2.1
OVERAL SECTOR VULNERABILITY			0.51

2.8 DNFBPs Sector Vulnerability Assessment- Module 7

2.8.1 This module assessed the aggregated vulnerability of the following clusters that were grouped into a single module of Designated Non-Financial Businesses or Professions (DNFBPs) –

- Second Hand Car Dealers,
- Real Estate
- Dealers in Airtime Products,
- Wild life and Fisheries,
- Dealers in Precious Stones and Metals,
- Wildlife and Fisheries,
- the Firearms industry and,
- Casinos and the Gaming Industry.

2.8.2 This averaged vulnerability of this sector was found to be equal to that of the banking sector (module 3).

2.8.2 Assessment of this sector considered both the threat variables and the control variables for the eight (8) different clusters and the table below indicates the assessment results –

Sector	Vulnerability Rating	Weight *(5 being the heaviest in terms of size, activity, importance etc.)*	Weighted Average	Rank in the Module *(starting with the most vulnerable)*
Precious Metals and Stones	0.60	5	3.00	**1**
Real Estate	0.70	4	2.80	**2**
Car Dealers	0.71	3	2.14	**3**
Airtime Products	0.63	3	1.88	**4**
Lawyers	0.51	3	1.50	**5**
Accountants	0.41	2	0.81	**6**
Casinos & Gaming Houses	0.30	1	0.30	**8**
Firearms	0.3	1	0.30	**8**
Wildlife	0.61	1	0.61	**7**
OVERALL DNFBPs Vulnerability: 0.58				

2.9 Financial Inclusion Products Vulnerability Assessment - Module 8

2.9.1 The module reviewed the financial inclusion products and services available in the country.

- The assessment identified the following as the most vulnerable order:
  - Housing Co-operatives (High)
  - micro finance services (Medium); and
  - Mobile financial services (Medium).

2.10 Terrorist Financing Risk- Module 9.

2.10.1 This module assessed several factors to determine the country's TF threats and vulnerability and, ultimately, the country's TF risk.

2.10.2 To assess TF risk, the module reviewed the following variables -

(a) Funds generated domestically for acts of terrorism at home,

(b) Funds generated domestically for acts of terrorism abroad,

(c) Funds generated abroad for acts of terrorism at home and

(d) Funds generated abroad for acts of terrorism abroad (transit Financing)

2.10.3 No cases associated with the above were investigated or prosecuted and no seizures were made by law enforcement agencies.

2.10.4 The TF threat in the country was therefore, found to be low.

2.10.7 The Module also assessed TF Vulnerability by reviewing the following variables

(a) Legislation

(b) Intelligence Gathering

(c) The Financial Intelligence Unit

(d) International cooperation

(e) The NPO sector

(f) The Political Environment.

2.10.8 All the above indicated strong controls against TF.

2.10.9 The low vulnerability and the low threat level produced a low TF risk rating.

3 SUMMARY OF THE DETAILED IMPLEMENTATION ACTION PLANS (DIAPs)

3.1 Overall Recommendations

3.1.1 The NRA findings relating to the ML threats and vulnerabilities of the country, as summarized above, point to the need for capacity enhancement for most national institutions involved in the fight against ML and TF.

3.1.2 These institutions range from the Financial Intelligence Unit, Law Enforcement Agencies, the National Prosecuting Authority and presiding officers. The capacity building requirements vary from module to module with issues that range from simple training to the need for more resources.

3.2 Recommendations in the DAIP- National Threat Analysis. - Module 1

3.2.1 In Module 1, threats of ML arising from predicate offences may be reduced by increasing the capacity of financial crime investigators.

3.2.2 Specialized training is required for Law Enforcement Agencies, such as the Police with particular focus on ML investigation.

3.2.3 Smuggling is the major predicate offence that was identified in the country. This calls for the increase in capacity for institutions manning the country's entry and exit points.

3.2.4 Further stakeholder engagement is recommended to identify the methods and measures to enhance capacity.

3.3 Recommendations in the DAIP - National Vulnerability Module Two.

3.3.1 The issue of capacity and integrity of prosecutors and presiding officers and was noted in the report.

3.3.2 There is need to come up with training programs for these key stakeholders to enhance their capacity.

3.3.3 Apart from training it is also recommended that resources which include manpower may be increased. Other issues that affect integrity such as appropriate staff retention and motivation schemes may also need to be explored.

3.3.4 From a national vulnerability perspective, there is need to increase the AML/CFT agenda's visibility in the national landscape. The DAIP therefore proposes the adoption and implementation of a national AML/CFT policy for the country.

3.3.5 It was noted that the country is not doing enough in terms of asset forfeiture as a way of depriving criminals of their illicit gains. It is recommended that an asset forfeiture unit be formally created in the country and be allocated adequate resources.

3.4 Recommendations in the DAIP- Banking Sector –Module 3

3.4.1 The NRA Assessment identified weakness in the quality of AML Supervision for banks as the greatest source of vulnerability.

3.4.2 There is need to enhance supervision and monitoring systems on the banking sector by the FIU and Bank Supervision.

3.4.3 As regards banking products regarded as highly vulnerable, the DAIP recommends enhanced CDD and product monitoring.

3.4.4 Fuller details on these activities are set out in the Detailed Action Plan

3.5 Recommendations in the DAIP- Securities, Insurance and Pension Sector– Module 4 and 5

3.5.1 These were identified as the lowest risk sectors. Recommendations are for continued enforcement of standard CDD for players in the sector.

3.6 Recommendations in the DAIP- Other Financial Institutions –Module 6

MFIs

- There is need to issue sector specific AML/CFT guidelines for the sector.
- There is also need to capacitate the sector's supervisory authority to enable conducts AML/CFT monitoring of the sector.

MTAs

- There is need to computerize monitoring systems in the sector due to high volumes in order to monitor them effectively.
- Border controls on cash couriers also need to be enhanced to suppress illegal money transfer operations.

Bureau De Change

- There in need for stakeholders (who include Police, ZIMRA, Department of Immigration and Zimbabwe Anti-Corruption Commission), involved in the prevention of gold and cigarette smuggling, and cash couriers, which are the source of these funds, to increase their efforts.

3.6.1 **Recommendations in the DAIP- DNFBPS –Module 7.**

Precious Stones and Metals.

- AML/CFT guidelines for the precious stones and precious metals is being developed by the FIU, which will enable the sector to develop its AML/CFT policy document for implementation.
- The Ministry of Mines and Mining Development, will ensure that AML/CFT requirements are complied with throughout the sector, through delegated authority to Zimbabwe Mining Development Corporation and Mineral Marketing Corporation of Zimbabwe.
- Enhancement of security arrangements throughout the value chain, from production to marketing of the precious stones and precious metals.
- The above objectives can be met with more resources allocated to beef up surveillance mechanisms in order to strengthen the monitoring regime.

Real Estate Sector.

- AML/CFT guidelines for the real estate sector has been issued, and on-going training is in progress.

Lawyers

Guidelines for Lawyers will be developed by the FIU and issued to the sector to be followed by relevant training programs.

- In light of the above, these high risk sectors are required to establish the sources of funds of their customers, monitor transactions, and identify and report suspicious transactions to the FIU.

Car Dealers

- The car dealers sector, which is not statutorily designated for AML/CFT purposes, was found to be highly vulnerable and attractive to money launderers. The high vulnerability is attributed to the high cash intensive nature of the sector and the absence of any AML/CFT controls.
- It is recommended that a supervisory authority, Central Vehicle Registry (CVR), be designated to regulate this sector for AML/CFT requirements.

Casinos and Gaming Houses

Casinos and Gaming Houses were found to present a low money laundering risk. While in other parts of the world, casinos present a relatively high money laundering risk. This was, however, found not to be the case in Zimbabwe, where the industry is small and well monitored.