



**REPUBLIC OF BOTSWANA**

**MONEY LAUNDERING/TERRORIST FINANCING  
NATIONAL RISK ASSESSMENT  
REPORT**

**October 2025**

## Republic of Botswana National Money Laundering and Terrorist Financing Risk Assessment Report

---

This consolidated report presents Botswana’s comprehensive National Risk Assessment (NRA) on Money Laundering and Terrorist Financing (ML/TF). It integrates various sectoral assessments into a single, coherent framework aligned with the World Bank methodology. The findings reflect the collaborative efforts of national stakeholders and highlight the country’s progress, vulnerabilities, and priorities for strengthening the AML/CFT framework.

## ACRONYMS

<b>AML</b>	Anti-Money Laundering
<b>ASWJ</b>	Al-Shabab or Al-Sunna wa Jama'a
<b>ATMs</b>	Automated Teller Machines
<b>AUMs</b>	Assets under Management
<b>BAOA</b>	Botswana Accountancy Oversight Authority
<b>BDF</b>	Botswana Defence Force
<b>BICA</b>	Botswana Institute of Chartered Accountants
<b>BO</b>	Beneficial Owner
<b>BoB</b>	Bank of Botswana
<b>BPS</b>	Botswana Police Service
<b>BURS</b>	Botswana Unified Revenue Service
<b>BWP</b>	Botswana Pula
<b>CDD</b>	Customer Due Diligence
<b>CFT</b>	Countering the Financing of Terrorism
<b>CIPA</b>	Companies and Intellectual Properties Authority
<b>CITES</b>	Convention on International Trade in Endangered Species
<b>CIU</b>	Collective Investment Undertakings
<b>CLGs</b>	Companies Limited by Guarantee
<b>CFP</b>	Countering Financing of Proliferation
<b>STRs</b>	Suspicious Transaction Reports
<b>DCD</b>	Department of Cooperative Development
<b>DCEC</b>	Directorate on Corruption and Economic Crime
<b>DeFi</b>	Decentralised Finance
<b>DFI</b>	Development Financial Institution
<b>DIS</b>	Directorate of Intelligence and Security
<b>DNFBPs</b>	Designated Non-Financial Businesses and Professions
<b>DPP</b>	Directorate of Public Prosecutions
<b>DRC</b>	Democratic Republic of Congo
<b>EDD</b>	Enhanced Due Diligence
<b>ENR</b>	Environment and Natural Resources
<b>EPS</b>	Electronic Payment Services
<b>ESAAMLG</b>	Eastern and Southern Africa Anti-Money Laundering Group
<b>FATF</b>	Financial Action Task Force
<b>FIA</b>	Financial Intelligence Agency

<b>FI</b>	Financial Institution
<b>FIUs</b>	Financial Intelligence Units
<b>GDP</b>	Gross Domestic Product
<b>GWP</b>	Gross Written Premiums
<b>ICRG</b>	International Co-operation Review Group
<b>IFSC</b>	International Financial Services Centre
<b>INTERPOL</b>	International Criminal Police Organisation
<b>ISCAP</b>	Islamic State and Islamic State Central Africa Providence
<b>KYC</b>	Know Your Customer
<b>LEA</b>	Law Enforcement Agency
<b>ML</b>	Money Laundering
<b>MLA</b>	Mutual Legal Assistance
<b>MoUs</b>	Memorandum of Understanding
<b>NBFIRA</b>	Non-Bank Financial Institutions Regulatory Authority
<b>NCCFI</b>	National Coordinating Committee on Financial Intelligence
<b>NPOs</b>	Non-Profit Organization
<b>NRA</b>	National Risk Assessment
<b>OBRS</b>	Online Business Registration System
<b>OECD</b>	Organisation for Economic Cooperation and Development
<b>PAYE</b>	Pay As You Earn
<b>PEPs</b>	Politically Exposed Persons
<b>PF</b>	Proliferation Financing
<b>PICA</b>	Proceeds and Instruments of Crime Act
<b>PIP</b>	Prominent and Influential Person
<b>REAC</b>	Real Estate Advisory Council
<b>ROS</b>	Registrar of Societies
<b>RSA</b>	Republic of South Africa
<b>SACCOS</b>	Savings and Credit Cooperative Societies
<b>SADC</b>	Southern African Development Community
<b>STR</b>	Suspicious Transactions Reports
<b>TF</b>	Terrorist Financing
<b>TFS</b>	Targeted Financial Sanction
<b>TOEs</b>	Traditionally Obligated Entities
<b>TSPs</b>	Trust Service Providers
<b>UNSC</b>	United Nations Security Council

---

<b>UNSCRs</b>	United Nations Security Council Resolutions
<b>UNSCTFS</b>	United Nations Security Council Targeted Financial Sanctions
<b>VAs</b>	Virtual Assets
<b>VASPs</b>	Virtual Asset Service Providers
<b>VAT</b>	Value added tax

---

Table of Contents

ACRONYMS .....	iii
EXECUTIVE SUMMARY .....	viii
DEFINITION OF KEY CONCEPTS .....	xii
CHAPTER 1: INTRODUCTION.....	1
CHAPTER 2: MONEY LAUNDERING RISK.....	9
Key Drivers Contributing to the National Money Laundering Risk in the Country.....	9
Domestic Prevalent National ML Threats.....	12
(a) Corruption .....	12
(b) Tax Offences .....	14
(c) Stealing by Servant .....	15
(d) Obtaining by False Pretense .....	16
(e) Fraud .....	17
(f) External Money Laundering Threats.....	18
CHAPTER 3: NATIONAL MONEY LAUNDERING VULNERABILITY.....	21
Sectoral factors attributing to Vulnerabilities .....	21
CHAPTER 4: SECTOR VULNERABILITIES.....	24
(a) Banking Sector .....	24
(b) Securities Sector.....	29
(c) Insurance Sector .....	35
(d) Other Financial Institutions Sector .....	40
(e) Designated Non-Financial Businesses and Professions.....	48
CHAPTER 5: TERRORIST FINANCING RISK ASSESSMENT.....	61
CHAPTER 6: NON-PROFIT ORGANISATIONS RISK ASSESSMENT.....	72
CHAPTER 7: LEGAL PERSONS, LEGAL ARRANGEMENTS AND BENEFICIAL OWNERSHIP RELATED RISKS.....	80
CHAPTER 8: VIRTUAL ASSETS AND VIRTUAL ASSETS SERVICE PROVIDERS RISK ASSESSMENT.....	88
CHAPTER 9:TAX                    CRIMES                    RISK                    ASSESSMENT .....	98
CHAPTER 10:ENVIRONMENTAL AND NATURAL RESOURCES CRIMES RISK ASSESSMENT .....	108
Main Threats facing ENR Sector.....	108
(a) Wildlife Sector.....	108
(b) Mining Sector.....	109
(c) Waste Management Sector .....	111
(d) Forestry Sector .....	111
CHAPTER 11: FINANCIAL INCLUSION PRODUCTS RISK ASSESSMENT.....	122



## **EXECUTIVE SUMMARY**

The Botswana Money Laundering and Terrorist Financing (ML/TF) Risk Assessment (2020–2024) is the country's second national assessment following the inaugural exercise concluded in 2017. The risk assessment adopts the World Bank Risk Assessment Tool which evaluates national threats; scale and nature of illicit proceeds terrorist financing (TF) as well as vulnerabilities, being weaknesses that may enable criminal exploitation. The findings of the assessment are expected to provide Botswana with a comprehensive understanding of its ML/TF threats and vulnerabilities, thereby supporting all stakeholders to implement risk-based supervision, informing policy development, guiding resource allocation, and enhancing coordinated mitigation efforts.

### **Country Context**

Botswana is a landlocked Southern African country covering 581,730 km<sup>2</sup>, with a population of 2,359,609 (National Census of 2022). It shares borders with South Africa, Namibia, Zimbabwe, and a small boundary with Zambia. Botswana's GDP per capita showed a dip in 2020 due to global factors and showed recovery in 2021 – 2022, followed by mixed (generally positive) trend by 2024, reflecting economic recovery and resource market dynamics. The country has one of the highest gross national incomes and the highest Human Development Index in Sub-Saharan Africa.

Botswana has a stable and well regulated financial sector which is mostly dominated by commercial banks and a large non-bank financial institutions sector, largely consisting of retirement funds. The banking sector comprises of nine (9) commercial banks (where 8 are subsidiaries of international bank) and two (2) statutory banks. The non-bank financial sector comprises mostly of retirement funds, insurance, securities, microlenders, bureau de change, money value transfer services (MVTs) and many others. Designated Non-Financial Businesses and Professions (DNFBPs) comprise of various sectors such as precious metal dealers, real estate agents, accountants, casinos, and legal practitioners.

There are close to 150,000 legal structures in Botswana, made up of 141,252 legal persons and 1,971 legal arrangements.

### **NRA Process**

The NRA was conducted through module-based Working Groups made up of public sector institutions, private entities, and civil society. Both quantitative and qualitative information was gathered through questionnaires, interviews, and research. The assessment relied on information provided by relevant sectors of the economy/society and also relied on expert knowledge.

## ML Risk Findings

Botswana’s overall money laundering (ML) risk is assessed as **Medium**, driven by both a Medium ML threat and Medium vulnerability. The threat analysis reviewed all predicate offences under national law and identified five major domestic sources of illicit proceeds: **Tax Crimes, Obtaining by False Pretense, Corruption, Fraud, and Stealing by Servant**. Tax Crimes posed the highest ML risk, with **underdeclaration of income** and **non-remittance of PAYE** emerging as the largest sources of illicit proceeds.

Wildlife crimes and drug trafficking were assessed as significant **external ML threats** due to their transnational nature. Within wildlife crime, **unlawful possession of elephant tusks** and **unlawful killing of rhinos** presented the most substantial ML risks. Although Botswana has legislation addressing environmental and natural resource offences, penalties were found to be insufficiently proportionate and dissuasive, reducing their deterrent effect. A summary of rating of the prevalent offence ratings is shown in the table below.

Domestic money laundering threats		External money laundering threats	
Predicate Offence	Rating	Predicate Offences	Rating
Tax Crimes	Medium High	Wildlife Crimes	High
Obtaining by False Pretense	Medium	Drug trafficking	Medium
Corruption	Medium		
Fraud	Medium		
Stealing By Servant	Medium Low		
<b>Total</b>	<b>Overall - Medium</b>		<b>Overall – Medium high</b>

The assessment found that most suspected predicate offences proceeds are ultimately channelled through the **banking sector**, making it the primary channel for ML exposure. **Real estate, legal structures, and securities** were found to be **moderately targeted for laundering of proceeds**, while the **insurance sector** was least targeted.

The assessment found that **Real Estate** poses the highest money-laundering vulnerability, driven by its large economic contribution and limited oversight, which enables the layering of illicit funds through high-value, often opaque transactions. The **Precious Stones sector** also presents elevated vulnerability due to high-value commodities, substantial cash use, and challenges in tracing the origin of stones, compounded by weak AML/CFT supervision across the diamond value chain. The table below shows a summary of the threat, vulnerability and risk ratings for each sector:

<b>Sector</b>	<b>ML Threat Rating</b>	<b>ML Vulnerability Rating</b>	<b>ML risk RATING</b>
Precious Stones	Low	Medium high	Medium
Casino	Low	Medium	Medium low
Real Estate	Medium	Medium	Medium
Banking	High	Medium	Medium high
Legal Practitioners	Low	Medium	Medium low
Insurance	Medium low	Medium	Medium
Securities	Medium	Medium low	Medium
Auditors	Low	Medium	Medium low
Accountants	Low	Medium	Medium low
Trusts and Service Providers	Low	Medium	Medium low
Legal Structures	Medium	Medium	Medium
Micro Lending	Low	Medium	Medium
Pawnshops	Low	Medium low	Medium low
Financing Companies	Low	Medium	Medium
Leasing Companies	Low	Medium	Medium
Retirement Funds	Low	Medium low	Medium low
IFSC	Low	Medium high	Medium high
MVTS / EPS	Low	Medium high	Medium
Bureau de Change	Low	Medium	Medium
DFI	Low	Medium	Medium
SACCOS	Low	Medium low	Medium low
Environment and Natural Resources (ENR) Sector	Medium	Medium high	Medium High
<b>NATIONAL</b>	<b>Medium</b>	<b>Medium</b>	<b>Medium</b>

## **TF Risk Findings**

Botswana recorded no terrorist attacks during the review period and had no known links to terrorist groups or individuals. Nonetheless, its participation in the SADC Mission in Mozambique (SAMIM) creates a potential exposure to retaliatory threats, particularly from Al-Shabab or Al-Sunna wa Jama'a, and its proximity to countries with active terrorism and known terrorist sleeper cells.

The assessment determined that both domestic and international terrorist-financing (TF) threats are very low, with no incidents linked to known TF typologies or activities.

Sectoral analysis found TF threat levels to be low for banking, MVTS, and bureaux de change, and very low for other financial institutions and DNFBPs.

Overall, the national TF risk was assessed as Medium for outgoing, incoming, and transit TF, and medium-low for domestic TF. The review found no evidence of terrorist financing abuse within Botswana's NPO sector.

## **Conclusion**

Botswana's risk is identified to have diverse origins, from the geographic nature of Botswana's porous borders with no effective natural barriers, new technology features of financial products, financial inclusion products that are cash intensive and cross-border by nature and the country's economic model which aims to attract foreign investment. It is therefore imperative that the country keeps abreast of its risks (both threats and vulnerabilities) to come up with relevant combating mechanisms to stop criminals from abusing the financial system and avoid international sanctions (grey listing) and terrorists from destabilizing national security of the country and its neighbours.

## DEFINITION OF KEY CONCEPTS<sup>1</sup>

- (a) **Risk** is a function of three factors- threat (motivation/capacity of criminals), vulnerability (weaknesses in systems/controls) and consequence (proportionate AML/CFT measures).
- (b) **Threat:** In the ML context, this refers to criminal individuals, groups or entities and their facilitators seeking to conceal the illicit origins of funds through past, present and future ML activities (and not the predicate offences themselves). The threat assessment typically serves as an essential starting point in developing an understanding of ML risk. For this reason, understanding the environment in which predicate offences are committed and proceeds of crime are generated to identify their nature, size and volume is important to carry out an ML risk assessment. In some instances, certain types of threat assessments might serve as a precursor for a ML risk assessment.
- (c) **Vulnerabilities:** Can be exploited by the threat or may support or facilitate its activities. **In the ML risk assessment context**, looking at vulnerabilities as distinct from threat means focusing on, for example, the inherent features of a particular sector, a financial product or type of service that make them attractive and feasible for ML purposes. Certain inherent characteristics of a country can also make it vulnerable to ML including a large financial, trade, or company formation sector. Vulnerabilities may also relate to a weakness in law, regulation, supervision, or enforcement. For example, deficiencies in AML controls, as well as non-compliance or partial compliance of national legislation with the requirements of the FATF Recommendations will impact the vulnerabilities in a country. Countries may include the adequacy or quality of AML controls in vulnerability assessment or focus their vulnerability assessment on inherent vulnerabilities and assess controls as a standalone component of ML risk.
- (d) **TF threat** is a person or group of people with the potential to cause harm by raising, moving, storing or using funds and other assets (whether from legitimate or illegitimate sources) for terrorist purposes. TF threats may include domestic or international terrorist organisations and their facilitators, their funds, as well as past, present and future TF activities, and individuals and populations sympathetic to terrorist organisations.
- (e) **The concept of TF vulnerability** comprises those things that can be exploited by the threat or that may support or facilitate its activities. Vulnerabilities may include features of a particular sector, a financial product or type of service that makes them attractive for TF. Vulnerabilities may also include weaknesses in measures designed specifically for CFT, or more broadly in AML/CFT systems or controls, or contextual features of a jurisdiction that may impact opportunities for terrorist financiers to raise or move funds or other assets (e.g. large informal

---

<sup>1</sup> FAFT ML/TF Guidance- <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Money-Laundering-NationalRisk-Assessment-Guidance-2024.pdf>.coredownload.inline.pdf,<https://www.fatf->

economy, porous borders etc.). There may be some overlap in the vulnerabilities exploited for both ML and TF.

- (f) **Consequence** refers to the impact or harm that ML or TF may cause and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally.

## CHAPTER 1: INTRODUCTION

1. Recommendation 1 of the Financial Action Task Force (FATF) Standards, requires countries to identify, assess and understand its money laundering, terrorist financing and proliferation financing (ML/TF/PF) risks, and to take action to ensure that these risks are mitigated effectively.
2. Understanding ML/TF/PF risk is a foundational element on which national AML/CFT/CPF systems and structures are built and improved by responding to changing environmental factors, assessing new information and identifying emerging risks that may materialise.
3. In line with these objectives, the Government of Botswana has reaffirmed its unwavering commitment to a rigorous, impartial, and expert-informed National Risk Assessment (NRA) process. This undertaking is grounded in the principles of expert autonomy, operational independence, and accountability, pillars that ensure integrity to drive an informed decision-making process across various national structures.
4. The Financial Intelligence Act of 2022 enshrines the responsibility for the coordination of the NRA to the National Coordinating Committee on Financial Intelligence (NCCFI). However, the 2025 amendment of the act rested the responsibility on the National Coordination Office (NCO). The NCO was established through the same amendment and reports directly to the NCCFI. The NCCFI is a high-level committee headed by the Permanent Secretary to the President (PSP), and it is established as the national policy-making body responsible for the combating of ML/TF/PF.
5. The NRA Working Groups, through the authority of the NCCFI, were fully empowered to access all relevant data and information from government entities, the private sector, and other stakeholders, ensuring the process reflects the broadest and most comprehensive range of insights. The Government, above all, upholds the professional independence of all experts and specialists engaged in the NRA including exercising their professional judgment and technical expertise without interference, thereby safeguarding the objectivity and credibility of the assessment process.

### National Risk Assessment Process

6. The ML/TF NRA is a comprehensive national assessment undertaken to identify, evaluate and understand the country's ML/TF risks. It examines threat and vulnerabilities across sectors, activities, geographic locations, client types, products and channels, to provide a holistic picture of the country's exposure to ML/TF.
7. Botswana conducted its first NRA in 2017 using the World Bank Money Laundering and Terrorism Financing Risk Assessment Tool. To ensure continued relevance, the NRA was updated in 2025 using data covering the period 2020 – 2024. The assessment identified all the relevant sectors exposed to ML/TF risks, including the financial sector, designated non-financial businesses and professions (DNFBPs), non-profit organisations (NPOs), and other emerging areas.

8. The NRA exercise involved the coordination of different public and private sector entities with a view of developing a National Strategy that supports the implementation of AML/CFT measures on a risk-sensitive basis.
9. The key objectives of this national risk assessment are to:
  - (a) Identify, assess and understand the ML and TF risks facing Botswana,
  - (b) Make recommendations to mitigate the consequences of the risks identified including through the formulation or calibration of national AML/CFT policies,
  - (c) Develop an action plan to help in prioritising and allocating AML/CFT resources for competent authorities,
  - (d) Provide a base for risk assessments conducted by competent authorities and to feed into the AML/CFT institutional risk assessments.

#### The National Risk Assessment Tool

10. The NRA adopted the standard risk assessment framework of the World Bank which guides countries in conducting their ML/TF risk at a national level. This allows for easy comparison with the 2017 NRA which employed the same guidance. The NRA tool is an analytical risk assessment framework comprising of several Excel-based and interrelated modules that enable countries to assess their ML/TF threats and vulnerabilities.
11. The general structure of the tool consists of fourteen modules (eight old and six new) that make it possible to assess ML/TF threats and vulnerabilities. The tool is centred around eleven modules that focus on the ML risk assessment. In addition, the tool includes a module to assess the risk of terrorist financing and non-profit organisations as well as a module to assess the risks of financial inclusion products.
12. Although a separate risk assessment of financial inclusion products was conducted, a decision was made not to make a separate report on the module as the products fall within the various sectors assessed being banking, insurance, new technologies and other financial institutions.
13. This World Bank Risk Assessment Tool provided Botswana with a structured model to enable the collection and collation of both quantitative and qualitative information to determine the ML/TF risk level.

#### NRA Working Groups & Structures

14. To undertake the NRA, the country established Working Groups (WGs) categorised according to Modules which consisted of public and private sector as well as civil society representatives in order to build a complete picture of national ML/TF risks. The list of participating stakeholders is shown as **Annex 1**. The level of seniority and expertise of participants released by various institutions ensured provision of adequate data and ease of collaboration by the stakeholders. Members of the various working groups held

numerous meetings. Participants provided informed professional and expert judgements on the ratings. The Modules are tabulated below:

<b>ML Risk Assessment</b>	<b>TF Risk Assessment</b>	<b>Financial Inclusion Product Risk Assessment</b>
<ul style="list-style-type: none"> <li>• National Threat</li> <li>• National Vulnerability</li> <li>• Banking Sector Vulnerability</li> <li>• Securities Sector Vulnerability</li> <li>• Insurance Sector Vulnerability</li> <li>• Other Financial Institutions</li> <li>• DNFBP Vulnerability Sectors</li> <li>• Tax Crimes Vulnerability</li> <li>• Environmental &amp; Natural Resource Crimes Vulnerability</li> <li>• Virtual Assets &amp; Virtual Asset Service Providers</li> </ul>	<ul style="list-style-type: none"> <li>• Terrorist Financing Risk Assessment</li> <li>• Non-Profit Organisations</li> </ul>	<ul style="list-style-type: none"> <li>• Financial inclusion products</li> </ul>

#### Data Collection

15. The NRA used both qualitative and quantitative data, which were collected through various primary data collection techniques including questionnaires and interviews and research. Trained AML/CFT Assessors vetted the questionnaires, which were developed for the various modules, for adequacy/quality before being administered. Follow-up interviews were conducted to collect additional data where responses to the questionnaires did not provide adequate data. Research was conducted from information sources obtained from intelligence agencies, public and private sector and civil societies. Such data included ML/TF cases investigated, prosecuted and convicted and the amounts of the proceeds of crime identified, seized, frozen and confiscated. The assessment also utilised data on size and complexity of sectors, published ML/TF typologies/trends, perception indices/surveys and academic reports.
16. Manual data collection in some institutions resulted in delay in accessing the information and data collation.

## Botswana's AML/CFT Legal and Institutional Framework

17. This section assesses the comprehensiveness of the AML/CFT legal and institutional framework; and identifies gaps and weaknesses in the legal and institutional framework, which cause vulnerabilities in national combating ability.

### Criminalisation of ML/TF Offences

18. Consistent with Article 3(1) (b) and (c) Vienna Convention and Article 6(1) Palermo Convention, section 47 of the Proceeds and Instruments of Crime Act (PICA) criminalises money laundering and is applicable to a wide range of predicate offences as covered in the FATF glossary. Section 5 of the Counter-Terrorism Act criminalises the Financing of Terrorism consistent with Article 2 of the International Convention for the Suppression of the Financing of Terrorism.
19. Accordingly, the NRA process took into account the full range of predicate offences as enacted in Botswana's laws and as identified as prevalent and significant in the national context.

### AML/CFT Institutional Framework

20. Botswana has established a number of key institutions to support and coordinate efforts to develop a more accurate and comprehensive understanding of ML/TF and enable early detection and investigation of financial crimes, terrorist and proliferation related activity. These institutions include amongst others regulatory and supervisory authorities responsible for overseeing and enforcing compliance with AML/CFT regulations within specific sectors, law enforcement agencies responsible for investigating and prosecuting financial crimes and government ministries that influence and determine AML/CFT policies and practices. These institutions include amongst others the following:
  - the Financial Intelligence Agency (FIA) created in terms of the Financial Intelligence Act, to receive, analyse, and disseminate financial intelligence;
  - the Directorate of Intelligence and Security (DIS) established in terms of the Intelligence and Security Services Act to protect national security;
  - the Counter Terrorism and Fusion Division (CTAFD) which facilitates information sharing and cooperation is a department under the DIS, which brings together various LEAs/ intelligence bodies;
  - the Directorate on Corruption and Economic Crime (DCEC) is responsible for investigating, preventing corruption and other economic crimes;
  - the Chemical, Biological, Nuclear, Radiological Weapons Management Authority (CBNRMA) as the principal Authority for the management of scheduled chemicals and nuclear material;
  - the Drug Enforcement Agency (DEA) established to deal with information on illegal use of narcotic drugs and psychotropic substances;
  - the Director of Public Prosecutions (DPP) is in terms of section 51A of the Constitution, responsible for instituting all criminal prosecutions in Botswana;

- the Office of the Receiver has the primary responsibility of preserving and maintaining seized, restrained or confiscated assets that are instrumentalities or proceeds of crime;
- Information and Data Protection Commission which monitors and enforces protection of personal data requirements and develop international cooperation mechanisms.

## Regulation & Supervision

21. The Financial Intelligence Act is the primary Act for AML/CFT regulation and supervision. The FI Act empowers supervisory authorities to conduct AML/CFT supervision activities including risk assessments, onsite and offsite examinations, issuing guidance notes, outreach and applying administrative sanctions<sup>2</sup>. The table below outlines the various supervisors and reporting entities.

Table 1: Supervisors and Reporting Entities

<b>Supervisory Authorities</b>	<b>Supervised Entities</b>
Bank of Botswana	Banks, MVTs, Bureau de changes
Real Estate Advisory Council	Real Estate Professionals
Gambling Authority	Casinos & Betting Operators
Law Society of Botswana	Attorneys
Non-Bank Financial Institutions Regulatory Authority	Non-Bank Financial Institutions
Registrar of Societies	Societies
Botswana Institute of Chartered Accountants	Accountants
Botswana Accountancy Oversight Authority	Auditors
Diamond Hub	Precious stone dealers
Director of Cooperative Development	Savings and Credit Cooperatives
Master of the High Court	Trust Service Providers & Trustees
Department of Mines	Precious metals & stone dealers
Companies and Intellectual Property Authority	Company Service Providers
Financial Intelligence Agency	Development Finance Institutions and any other specified entities without a supervisor

## National Systems and Technological Tools (Beneficial ownership information and electronic verification)

22. Botswana has an independent and reliable identification infrastructure issued by the Department of Civil and National Registration through the National Registration Act. The national identity card, commonly referred to as Omang, is issued through a secure system National Identification System (NIS) and is valid for a period of 10 years. Citizens

<sup>2</sup> Section 49 of the FI Act

below the age of 16 years are identifiable through the birth certificate issued under the Births and Deaths Registration Act.

23. Omang has various security features that are visible to the naked eye and some that contain ultra violet (UV) fluorescent light readable features. The document is also printed using specialized printing techniques that are difficult to replicate. Botswana issues identity cards for refugees, however, verification is manual. Botswana relies on passport for identification of foreigners.
24. Some AML-regulated entities (mainly commercial banks) have access to the national identity database, which facilitates efficient verification of customer identities. However, entities without access to this platform face ongoing challenges, often relying on certified copies of identity documents for verification, which reduces reliability and increases vulnerability to identity related risks.
25. The Companies and Intellectual Properties Authority (CIPA) maintains a beneficial ownership (BO) registry through its Online-Business Registration System (OBRS), which can be viewed by reporting entities for verifying company BO information.

#### Established structures

26. The National Coordinating Committee on Financial Intelligence (NCCFI) is a high-level committee that coordinates implementation of AML/CFT activities, including assessing the effectiveness of policies and measures for combating ML/TF crimes and making recommendations on policy reforms.
27. The NCCFI consists of several key stakeholders to support the AML/CFT framework of the country, these stakeholders include, Ministry of Finance, DCEC, Botswana Police Service, Attorney General's Chambers, DPP, Bank of Botswana (BoB), Botswana Unified Revenue Service (BURS), Non-Bank Financial Institutions Regulatory Authority (NBFIRA), Ministry responsible for international Cooperation, Directorate of Intelligence and Security Services (DIS), Ministry responsible for Defence, and Ministry responsible for Immigration.
28. The National Coordination Office was established in 2025 following the amendment of the FI Act (Section 9). This followed the 2024 Mock Mutual Evaluation which found that although the NCCFI had been established to promote coordination in the development and implementation of AML/CFTP policies, some of its functions were at a technical and operational level hence had a potential to slow down the implementation and impede effectiveness. The amendment hence delegated the operational functions to the NCO including the coordination of the NRA, assessment of the effectiveness of policies and measures to combat financial offences, and recommendation to the NCCFI for legislative, administrative and policy reforms.

## International Cooperation & Information Sharing

29. Botswana as a member of the international community, has mechanisms in place for the exchange of information as it relates to international cooperation on financial crime investigations, prosecutions and asset forfeiture matters.
30. The DPP is the Central Authority responsible to facilitate the provision and obtaining of international assistance in criminal matters. In addition, LEAs and FIA are legally empowered to share information with their foreign counterparts. Botswana signed four (4) Mutual Legal Assistance (MLA) and Extradition agreements; and a number of Memoranda of Understanding on Combating Cross- Border Transnational Organised Crime with Foreign States and where there was no mechanism in place, assistance was given on the basis of Reciprocity. There was also informal cooperation in place for exchange of intelligence and information.
31. The Extradition Act of 1990 and its amendments, international treaties/protocols and based on bilateral agreements establish procedures for the surrender of fugitives to and from Botswana. This adds value to the quality of criminal investigations and prosecutions. The table below highlights progress made by Botswana in this area;

Table 2: Extradition Statistics (2020-2024)

<b>OUTGOING REQUESTS FROM BOTSWANA</b>						
<b>YEAR</b>	<b>2020</b>	<b>2021</b>	<b>2022</b>	<b>2023</b>	<b>2024</b>	<b>TOTAL</b>
Number of requests	16	9	13	3	9	<b>50</b>
Sent out (response)	7	9	0	3	9	<b>28</b>
Extradition granted	4	1	1	0	0	<b>6</b>
Number Withdrawn	1	0	0	0	0	<b>1</b>
Pending Feedback	1	8	12	3	9	<b>33</b>
Denied	3	0	0	0	0	<b>3</b>
<b>INCOMING REQUESTS FROM OTHER JURISDICTION</b>						
<b>YEAR</b>	<b>2020</b>	<b>2021</b>	<b>2022</b>	<b>2023</b>	<b>2024</b>	<b>TOTAL</b>
Number of requests	1	1	2	8	3	<b>15</b>
Repatriation granted	1	1	0	1	0	<b>3</b>
Withdrawn	0	0	0	1	0	<b>1</b>
Denied	0	0	0	0	0	<b>0</b>
Pending repatriation	0	0	0	0	0	<b>0</b>

Table 3: Mutual Legal Assistance Statistics (2020-2024)

<b>OUTGOING REQUESTS FROM BOTSWANA</b>						
<b>YEAR</b>	<b>2020</b>	<b>2021</b>	<b>2022</b>	<b>2023</b>	<b>2024</b>	<b>TOTAL</b>
Number of requests	58	68	83	50	24	<b>281</b>
Number sent out	31	15	3	50	8	<b>107</b>
Feedback received	4	2	2	0	1	<b>9</b>
Feedback pending	27	36	80	50	7	<b>200</b>
Requests denied	0	0	1	0	0	<b>1</b>
<b>INCOMING REQUESTS FROM OTHER JURISDICTION</b>						
<b>YEAR</b>	<b>2020</b>	<b>2021</b>	<b>2022</b>	<b>2023</b>	<b>2024</b>	<b>TOTAL</b>
Number of requests	6	20	3	10	3	<b>42</b>
Feedback sent	4	0	3	5	3	<b>15</b>
Received back	4	0	0	0	0	<b>4</b>
Requests denied	2	0	0	0	0	<b>2</b>

32. Different competent authorities in the country have subscribed to several regional and international bodies such as Asset Recovery Inter-Agency Network for Southern Africa (ARINSA), EGMONT and International Criminal Police Organisation (INTERPOL), Southern African Regional Police Chiefs Co-operation Organisation (SARPCCO), the Organisation for Economic Cooperation and Development (OECD) Global Forum, and Southern Africa Customs Union (SACU). Botswana also utilised international law enforcement networks such as Customs Enforcement Networks (CEN) that provides for the exchange of information related to tax crimes trends globally.

## CHAPTER 2: MONEY LAUNDERING RISK

33. Money laundering (ML) risk for Botswana is found to be Medium. The ML risks faced by Botswana arise from a combination of institutional, operational, and structural threats and vulnerabilities. While the country has made and continues to make efforts to strengthen the national anti-money laundering (AML) framework, criminals may still explore existing weaknesses to launder funds.
34. The increasing complexity of transnational criminal activity, weak international cooperation and porous borders increase the country's exposure to cross-border ML schemes and contribute to the threats of ML across the sectors.

### Key Drivers Contributing to the National Money Laundering Risk in the Country

#### Threat-Related Drivers

- (a) **Transnational Organised Criminal Activity:** Exposure to transnational organised crime networks presents a significant money laundering threat, as criminal syndicates exploit jurisdictional differences, cross-border trade and financial linkages to generate, move, and conceal illicit proceeds.
- (b) **High-Value Predicate Offences:** Predicate crimes, including tax crimes, fraud, corruption, and environmental offences, generate substantial illicit proceeds that require laundering, thereby elevating the overall money laundering threat level.
- (c) **Cross-Border Illicit Financial Flows:** The movement of illicit proceeds across borders through regional and international financial channels increases exposure to money laundering, particularly at the layering and integration stages.
- (d) **Tax-Related Money Laundering:** Tax evasion and under-reporting schemes constitute a material money laundering threat, as offenders seek to conceal and legitimise proceeds derived from fiscal crimes through the financial system.
- (e) **Environmental and Wildlife Crime-Related Money Laundering:** Environmental and wildlife crimes generate illicit proceeds that are laundered through both formal and informal channels, contributing to national money laundering risk.

#### Vulnerability-Related Drivers

- (a) **Inadequate Financial, Technical, and Human Resources:** Constraints in financial, technical, and human resources impede effective money laundering detection, investigation, and case management. The limited availability of forensic accounting and cyber-investigative expertise further restricts the ability to trace, seize, and recover illicit assets, particularly in complex and cross-border cases.
- (b) **Limited Timeliness and Quality of Financial Intelligence Dissemination:** Delays and quality gaps in the dissemination of financial intelligence reduce operational value and limit impact on law enforcement and prosecution outcomes.

- (c) **Speed and Ease of Cross-Border Funds Movement:** The rapid remittance of funds into and out of the country creates vulnerabilities that may be exploited to quickly layer and integrate illicit proceeds before detection.
- (d) **Predominant Use of Administrative Sanctions for Tax Violations:** The reliance on administrative rather than criminal sanctions for tax offences weakens deterrence and facilitates the concealment of illicit proceeds through tax evasion and under-reporting schemes.
- (e) **Limited Use of Parallel Financial Investigations:** Failure to consistently conduct parallel financial investigations alongside predicate offences results in missed opportunities to trace, seize, and confiscate illicit assets, allowing criminals to retain and reintegrate illicit gains into the legitimate economy.
- (f) **Insufficient Quantification of Environmental Crimes:** The lack of reliable data and quantification of environmental crimes limits understanding of their scale and money laundering impact, undermining effective risk assessment and mitigation.
- (g) **Leniency of Sanctions for Money Laundering Offences:** Relatively low or non-dissuasive penalties for money laundering and related financial crimes reduce deterrence and weaken the effectiveness of the AML enforcement framework.
- (h) **Insufficient supervision oversight on the IFSC sector:** IFSCs create a possibility of abuse of the tax system where companies, often with no substantial economic activity in Botswana, use the IFSC status to enjoy the tax benefits derived from the status.

ML Risk Level as a function of ML Threat and ML Vulnerability

35. Botswana’s overall ML Risk Level is Medium. This is as a function of ML Threat rated Medium and ML Vulnerability rated Medium as depicted below:

<b>Overall threat</b>	H	M	M	MH	H	H
	MH	M	M	MH	MH	H
	M	ML	M	M	MH	MH
	ML	ML	ML	M	M	M
	L	L	ML	ML	M	M
		L	ML	M	MH	H
<b>OVERALL VULNERABILITY</b>						

Money Laundering Threat at National Level

36. In line with FATF standards, the NRA process considered the complete range of FATF-defined predicate offences to determine the most prevalent crimes that contribute to

national money-laundering threat. In identifying and assessing the threat environment, the assessment relied primarily on domestic criminal, intelligence, and FIA data. In addition, it considered threats originating from neighbouring countries, along with any other sources of information and mechanisms deemed relevant to the analysis.

37. This assessment evaluated the country's money-laundering threats by analysing the scale, nature, and impact of predicate offences in line with FATF requirements. It identified the most significant underlying criminal activities, examined their associated laundering methods and channels, and assessed the extent to which the offences generated proceeds that pose a threat to the integrity of the national financial system.
38. For the period under review, several predicate offences (money laundering threats) were identified as prevalent at a national level and recorded with law enforcement agencies. The total amount involved was estimated at P6, 290,641, 257.10 as indicated in **Annex II** attached. Out of these offences, five top offences that generate proceeds domestically are in the table below.

Table 4: Five top offences that generate proceeds domestically

<b>Predicate Offence</b>	<b>Estimated Amounts Involved (BWP)</b>	<b>Rating</b>
Tax Crimes	1,707,405,065.94	Medium-high
Obtaining by False Pretence	955,846,390.94	Medium
Corruption	922,080,377.57	Medium
Stealing By Servant	380,457,720.00	Medium
Fraud	6,867,409.36	Medium
<b>Total</b>	<b>3,972,656,963.81</b>	<b>Overall - Medium</b>

39. Financial institutions, fund managers, real estate agencies, and securities firms were collectively identified as the primary channels through which most criminal activities were facilitated.
40. The assessment identified the most prevalent typologies within these sectors as identity fraud, cyber fraud (such as social engineering scams and computer enabled crimes), committed mostly through the banking, money value transfer services (MVTs) and real estate sectors. Mobile network operators and social media were abused to advertise and lure victims. The proceeds were mostly invested in buying movable and immovable assets such as houses and motor vehicles.

Table 5: Breakdown of each sector contribution

Sector	No. Of Cases	Amount Involved	Sector Weight	ML Threat Rating
Banking	82	649, 732, 034.69	2	High
Securities	1	240, 000, 000.00	8	Medium
Insurance	8	100, 881, 006.38	6	Medium low
Real Estate	34	81, 187, 645.65	5	Medium
<b>Total</b>	<b>126</b>	<b>1,109,800,686.72</b>		<b>Medium</b>

41. The money laundering threat for other sectors such dealers in precious stones, casinos, accountants, auditors, legal practitioners and trusts and companies service providers was assessed as low risk and hence were not included here.

#### Domestic Prevalent National ML Threats

42. The national money-laundering threats prevalent in Botswana arise from a combination of underlying criminal activities and systemic vulnerabilities. These include weaknesses in supervision, along with gaps in the rule of law that are exploited by criminal actors. In assessing each threat and determining overall risk rating, several key factors were considered, including the following:

- Extent – The scale of illicit funds generated (e.g., the estimated volume of criminal proceeds produced by the crime type that require laundering particularly in comparison to other crimes).
- Nature – The complexity and sophistication of laundering methods used (e.g., the diversity and technical sophistication of techniques used to conceal and move funds).
- Actors – The profile and organisation of parties involved (e.g., organized crime groups, serious and organized criminal networks, or other actors linked to the illicit activity)

#### (a) Corruption

43. Corruption was assessed as posing a **medium** risk. Corruption involves conduct in which public or private sector officials unlawfully enrich themselves or others through the misuse of entrusted authority. Such conduct includes bribery, extortion, and related illicit activities that undermine governance, public trust and economic stability. In Botswana, section 24 (1) (2) of Corruption and Economic Crime Act (CECA) criminalize corruption by or of a public officer and Section 24 (2) criminalises corrupt acts committed by the private sector actors, whether domestic or foreign.
44. Corruption was identified as one of the prevalent money-laundering threats in the country. The crime generated substantial illicit proceeds and enabled criminals to exploit public institutions and conceal the movement of illegal funds.

45. During the review period there were 856 reported corruption cases, of which 163 were investigated. Of the investigated cases 4 were prosecuted and 3 convictions were obtained. Of the investigated cases 71 triggered ML investigations, with one prosecution and conviction.
46. The nature of corruption allegations reported and received by the Directorate generally centre around procurement corruption, involving national projects and contracts as well as petty corruption.
47. Considering the extent, nature and actors involved, corruption risk was **rated medium** for the following reasons.
- The monetary value involved in the corruption cases was significantly high as compared to other predicate offences, thereby contributing substantially to the overall risk.
  - The methods used to launder the proceeds were not complex in nature as funds were mostly self-laundered using corporate vehicles and banks, with very minimal use of tax haven linked bank accounts (facilitated by local institutions) noticed.
  - The persons committing the offense were found to be low-level offenders not linked to any serious and organised crime (SOCG) activities. Generally, there were notable cross-border transactions to neighbouring countries e.g. South Africa, for purchases of properties, with proceeds later laundered back to the country.
48. Furthermore, consideration was also given to the country's performance on Transparency International's Corruption Perceptions Index for 2020–2024, as illustrated below.

Table 6: Botswana Corruption Perception Index ratings (2020-2024)

Year	CPI Rank	Results Score	Perceived Level
2024	43/180	57/100	Medium
2023	39/180	59/100	Medium
2022	35/180	60/100	Medium-Low
2021	45/180	55/100	Medium
2020	35/180	60/100	Medium-Low

The CPI ranks 180 countries and territories worldwide by their perceived levels of public sector corruption. The results are given on a scale of 0 (highly corrupt) to 100 (very clean).

### Corruption Case Study

In State vs C.N Morupisi and Others, the accused person (Permanent Secretary to The President, also Secretary to Cabinet and Chairman of Botswana Public Officers Pension Fund) was convicted for Corruption Offences (Abuse of Public Office and Bribery) and money laundering offence for permitting himself to be influenced by a valuable consideration (motor vehicle) to corruptly award a P500,000,000.00 private equity contract to a private fund management company Capital Management Botswana (the corruptor), which was regulated by NBFIRA

#### (b) Tax Offences

49. Tax offence encompasses any violation of tax laws that results in the infringement of a government's right to collect tax revenue. These offences range from relatively minor administrative breaches to more severe acts of fraud or tax evasion. Tax evasion means the use of illegal methods by taxpayers to avoid paying tax or reduce tax payable. The assessment identified various tax crimes for the period under review.
50. Under declaration of income and non-remittance of pay-as-you-earn (PAYE) were identified as the two (2) highest proceed generating tax crime recorded during the review period. For under declaration of income, typically, the modus operandi involves the use of personal accounts to deposit business proceeds, overstating of claimable expenses, and claiming of expenses with fake documents. Non remittance of PAYE involves failure to remit withheld tax by employers.

Table 7: Statistics of Tax Crimes (2020-2024)

TAX OFFENCES	No. of cases	Amount Involved (BWP)
Under declaration of income	1451	1,580,112,395.39
Non remittance of PAYE	61	70,882,787.79
Non/under declaration of cash	62	6,504,282.40
Non declaration of goods (Smuggling of goods)	1936	5,296,239.00
Falsified records and self-invoicing	99	44,274,583.00
Under valuation	2032	6,839,060.30
<b>Total</b>		<b>1,707,405,065.48</b>

51. Tax crime was assessed as posing a **medium-high** money laundering threat.
52. The crimes under assessment were characterised by the deliberate and unlawful evasion of legally owed taxes and involved active measures by the perpetrators to conceal income, profits, or gains.

53. The value and scale of proceeds generated from tax crimes were significantly higher than those from other offences, thereby contributing substantially to the overall risk. The risk is impacted by the associated loss of government revenue and the externalization of funds to foreign jurisdictions. Some of the method used to move funds includes the use of trade-based money laundering, the exploitation of transfer pricing leading to profit shifting and treaty shopping, and the manipulation of thin-capitalization rules which resulted in further base erosion.
54. The persons involved in this offence were diverse and included professional service providers such as accountants, auditors, bankers, tax consultants, and clearing agents, as well as executive management, shareholders, directors, and multinational companies.

#### **Tax Offence Case Study**

- The case involved allegations of under declaration of income by a company director. The Director was alleged to have externalised untaxed company turnover of approximately P98 million to foreign jurisdictions where he maintained his wealth. To avoid being taxed, the money was syphoned from the company through: paying company projects directly into personal accounts rather than company accounts and reporting project payments as sales.
- huge sums of money transferred from the company business account before taxation to personal accounts in foreign jurisdictions.
- huge sums of money from company projects paid in cash to the director and kept at the company premises and his residential place, and eventually smuggled out of the country by his friends.

Investigations revealed that from 2010 to 2020, P85 million undeclared turnover from company projects was transferred to the director's personal bank accounts. Total tax assessments of P206, 636,303.20 and P95, 357,958.00 were raised for income tax and value added tax, respectively for the company. A tax investigation was also carried out on the director. A total tax assessment of P56, 000,000.00 was raised on the director's personal taxes. Money laundering investigations are ongoing. The money that was seized during the raid was deposited towards the reduction of income tax and personal tax liabilities. Further collection efforts on the case are still ongoing.

#### (c) Stealing by Servant

55. Stealing by servant refers to the misappropriation of property, funds, or assets by an employee entrusted with access in the course of employment. It is a recognised predicate offence under the national AML/CFT framework. Stealing by servant presents a moderate threat to the AML/CFT system. Weak internal controls, delayed detection, and low asset recovery elevate vulnerability. Recommended mitigation measures include strengthened internal controls, improved segregation of duties, enhanced employee vetting, fraud-awareness programmes, and better coordination between institutions and law enforcement.
56. Stealing by servant was assessed as posing a **medium** money laundering threat.

57. There were 1003 reported cases of stealing by servant during the review period. Incidences reported between 2020 and 2022 were found to be low, however the values involved were significantly high. This may be attributed to the Covid-19 period where internal controls were compromised by protocols applied to control the spread of the virus. Similarly, the amounts restrained or confiscated were minimal during the same period as compared to the total values involved. This was largely due to delays in identifying and reporting the incidents to LEAs and thereby giving the offenders more time to conceal the money trail and ultimately making it difficult to recover the stolen funds. All the cases recorded involved Batswana (citizens of Botswana). The table below shows the number of cases of stealing by servants and amounts involved.

Table 8: Cases of Stealing by Servant (2020 to 2024)

Year	Investigated	Prosecuted	Convicted	No. of Persons	Amount involved (BWP)	amount seized or restrained (BWP)	Amount confiscated (BWP)
2020	20	2	2	3	298 191 266.20	83 000.00	0.00
2021	10	1	0	0	24 227 683.90	1 800.00	0.00
2022	14	0	1	0	21 581 506.99	720.00	0.00
2023	543	88	58	65	17 346 356.75	68 771.75	77 000.00
2024	416	77	71	80	19 110 906.20	4 886 715.49	800 000.00
<b>Total</b>	<b>1003</b>	<b>168</b>	<b>130</b>	<b>148</b>	<b>380,457,720.00</b>	<b>5,041,007.24</b>	<b>877,000.00</b>

58. The extent of criminality associated with stealing by servant was assessed as moderate, although it only accounted for approximately 6% of the total proceeds generated from national predicate offences, the high number of reported incidence and its upward trend over the years poses a higher level of risk whilst on the other hand the amounts involved was on average decreasing.

59. Although the methods used were not highly sophisticated, they often involved collusion among multiple individuals and the use of various tactics to avoid detection, which increased the difficulty of uncovering these offences. The actors involved were typically low-level individuals acting alone or with minimal coordination, with no indication of organised syndicate involvement. However, some offenders possessed sufficient knowledge of internal systems and processes, enabling them to exploit operational vulnerabilities.

(d) Obtaining by False Pretense

60. Obtaining by false pretense is an offence in terms of section 308 of the Penal Code. It refers to any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen. During the period under review, 9948 cases involving a total amount of P289, 477,377.57 were investigated. Of these cases 197 cases were prosecuted, with convictions in 124 cases involving a total of 130 persons.

61. The low prosecution was attributed to limited resources such as few prosecuting personnel, out of court settlements and inadequacy of evidence. Majority of these cases were committed in Botswana while there were incidences where funds were transferred outside the country. The assessment observed a significant rise of the cases on the offence from 125 in 2020 to 3469 in 2023, and a decline to 2857 cases in 2024. This decline was attributed to strengthened enforcement efforts.
62. Obtaining by false pretense was assessed as posing a **medium** money laundering threat.
63. The extent of this offence was assessed as moderate as compared to other crimes. The diversity and sophistication of the methods used to launder funds generated by the crime included internet links, pseudo-online platforms, voiceover techniques, and direct contact approaches such as phone calls used to obtain personal information. These techniques allow both organised groups and individual actors to target a broad population. Many of the victims also voluntarily disclosed information, contributing to their vulnerability. Most perpetrators are locals with a limited number of foreign actors identified.
64. The offences were perpetrated through banks and mobile network operator platforms. Intelligence further indicated the existence of networks that coerce individuals, including prisoners, to participate in these schemes. Other platforms abused included online purchasing platforms and pension scheme systems. While a few high-level cases involving significant monetary losses were recorded, the majority of incidents involved individual actors or small syndicates targeting smaller amounts. Most perpetrators operate alone or in small groups, with some exploiting privileged access to personal information to commit offences through false pretences.

(e) Fraud

65. Under Penal Code 342A, fraud is committed when a person intentionally makes an unlawful misrepresentation that causes prejudice — financial or otherwise — to another. The offence carries a penalty of up to seven years' imprisonment, a fine of up to P100,000, or both.
66. Fraud was assessed as posing a **medium** money laundering threat.

Table 9: Cases of Fraud (2020 to 2024)

Year	Investigated	Prosecuted	Convicted	No. of Persons	Amount involved (BWP)	Amount seized / restrained (BWP)	Amount confiscated (BWP)
2020	0	0	0	0	0	0,00	0,00
2021	0	0	0	0	0	0,00	0,00
2022	6	0	0	0	3 489 821.36	202 300,00	0,00
2023	7	0	0	0	3,012,090,00	0,00	0,00
2024	6	0	0	0	365,498,00	0,00	0,00
<b>Total</b>	<b>19</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>6,867,409.36</b>	<b>19, 790, 611.05</b>	<b>0.00</b>

67. A rise in investigated cases was recorded in 2023 which recorded the highest number of incidences and value amounting to P186, 685, 714.81 (not included int table above). It is worth noting that a significant amount of the recorded value was related to a pyramid scheme case. None of the cases recorded during the review period was prosecuted due to various reasons such as complexity of the fraud case investigations and involvement of foreign jurisdictions to obtain evidence which prolonged completion of investigations for prosecution. Therefore, ML threat relating to "Fraud" was rated **medium**.

(f) External Money Laundering Threats

68. Transnational organised crime poses significant challenges to any economy by undermining governance, threatening the stability of financial institutions, and causing both social and environmental harm. In Botswana has categorised wildlife crime and drug trafficking as external money laundering threats due to their inherently transnational nature and the elevated risks they pose. These crimes have been identified as issues of national concern because of their cross-border dynamics and the substantial illicit proceeds they generate. ML threat associated with wildlife crime is rated Medium High, while drug trafficking is rated medium.

(i) Wildlife Crimes (Poaching)

69. FATF's report on Money Laundering and Illegal Wildlife Trade of, June 2020 refers to illegal wildlife trade as a major transnational organised crime, which generates billions of criminal proceeds each year. Countries are encouraged to prioritise the combatting of financial flows from the illegal wildlife trade, by identifying and assessing their money laundering risks relating to the illegal wildlife trade. Botswana's appeal to wildlife criminals is due to its large wildlife populations, particularly the country is known to have the highest elephant population in Africa.

70. The prevalent environmental crimes in Botswana were found to emanate from illegal trafficking of wildlife and wildlife products and illegal mining (gold). The findings of the assessment are discussed in detail under the Environmental Natural Resources (ENR) Sector assessment.

71. Wildlife crime was considered to be the most significant threat under environmental crimes resulting in it being considered as a national threat. Wildlife crime was assessed as posing a high money laundering threat.
72. The country identified significant challenges in assessing the scale and estimated value of criminal proceeds generated by wildlife crime. These challenges were largely due to the absence of a standardised approach for quantifying the financial impact, including determining the life-value of the targeted species and the value of the poached animal products such as horns or tusks.
73. To address this, three valuation scenarios were considered:
  - Existing in-country approach: Limited by available Convention on International Trade in Endangered Species (CITES) valuation data and low levels of detection of poached wildlife products such as tusk and rhino horn. This process requires the weighing of the products. Using this method the estimated value for the period is P2, 844,096.85.
  - Research-based methodology: Utilising lifetime valuations from studies conducted by international independent researchers and organizations. The lifetime value for the elephants and rhinos poached during this period is estimated at P12,470,895,000.
74. The research-based methodology scenario, which represents the highest amount was adopted for the purposes of assessing money laundering risk. Other models that could be considered is to use valuation adopted by the FATF following the typology; June 2020 report on Money Laundering and Illegal Wildlife Trade.
75. Other factors considered in the threat assessment included the sophisticated methods used by criminals to evade detection, such as accessing the country through swampy areas. The assessment also noted potential information leaks from insiders and the involvement of well-known criminal syndicates, as well as former anti-poaching operations personnel, who contribute specialised skills to poachers.

(ii) Drug Trafficking

76. Drug trafficking is globally identified as a key transnational crime whose financial proceeds are used to fund other illicit activities. The proliferation of illicit narcotics or psychotropic substances remained a concern in Botswana. The transnational nature of the crime posed various challenges to the country since it was difficult to trace the drugs back to the supplier and or determine the country of origin. Drug trafficking was assessed as posing a **Medium** money laundering threat.

77. During the period under review, 720 persons were convicted of drug trafficking<sup>3</sup>. 95 percent of the convicts were Batswana while the rest of the offenders were Zimbabweans, South Africans, Zambians, and Tanzanians. Intelligence suggested that the drugs (marijuana) originated mostly from the Kingdom of Eswatini. The total amount involved in drug trafficking was **P61, 583,063.03** as indicated in table 6.7 below.

Table 10: Drug Trafficking Statistics (2020-2024)

Year	Investigated	Prosecuted	Convicted	No. of Persons	Amount involved (BWP)	Amount seized	Amount confiscated
2020	1655	127	121	155	13,859,673.63	13,859,673.63	13,859,673.63
2021	1332	85	84	113	5,341,618.11	5,341,618.11	5,341,618.11
2022	1418	51	31	74	9,465,304.40	9,465,304.40	9,465,304.40
2023	1234	100	48	102	16,774,969.89	16,774,969.89	16,774,969.89
2024	914	91	40	276	16,141,497.00	16,141,497.00	16,141,497.00
<b>Total</b>	<b>6553</b>	<b>454</b>	<b>324</b>	<b>720</b>	<b>61,583,063.03</b>	<b>61,583,063.03</b>	<b>61,583,063.03</b>

78. According to the reported incidences the drug of choice in Botswana is marijuana (locally referred to as dagga or motekwane) accounting for P48,765,433 of the total amount, followed by growing incidences of methcathinone (CAT) at P5,696,795. The rest is made up of smaller quantities of various drugs such as cocaine, methamphetamine (crank/crystal) and ephedrine (a precursor ingredient). The proceeds generated during the review period were assessed as low when compared to other prevalent predicate offences in the country. It is assessed as low due to the fact the amounts involved under trafficking relate to street value of the drugs confiscated not proceeds generated. Proceeds are made and laundered externally However, the overall risk was elevated due to the significant social impact of drug use on local communities and society at large, as well as the economic burden placed on families and the government, particularly regarding national security and community safety. The assessment also found that the actors involved were organized, comprising multiple participants who employed various methods to evade detection, including the use of MVTS for cross-border payments to suppliers.
79. The assessment established that Botswana was not an exception to the social effects of illicit drugs. The effects include among others, health hazard, economic burden to the government, family and social impact, community safety, youth and education, stigma and discrimination.

<sup>3</sup> The repeal and re-enactment of the Medicines and Related Substances Act in 2018 resulted in two Acts i.e. the Medicines and Related Substances Act and the Illicit Traffic in Narcotic Drugs and Psychotropic Substances Act.

## CHAPTER 3: NATIONAL MONEY LAUNDERING VULNERABILITY

80. The national money laundering vulnerability is informed by a combination of the national money laundering combating ability and the overall sectoral vulnerability. The vulnerability assessment considered Botswana's ability to prosecute, penalise instances of ML offences and forfeiture of proceeds and instrumentalities of crime. Additionally, the assessment considered the money laundering vulnerabilities of financial institutions (banking, money remitters, micro lenders and bureaux de change, securities, insurance) and DNFBPs (casinos, legal practitioners, precious stones and precious metals, including semi-precious stones).
81. The level of the overall money laundering vulnerability was rated Medium. The national vulnerabilities were mostly driven by sectoral vulnerabilities.

### National factors attributing to vulnerabilities

82. National factors that contribute to Botswana's money laundering weaknesses maybe attributed to the following:
- varying levels of AML/CFT maturity across supervisory bodies and respective sectors. There are notable weaknesses in regulation, supervision, and enforcement within some sectors such as **DNFBP** where supervisory authorities are still in the process of building capacity and expertise on risk-based supervisory frameworks.
  - Corruption by public servants, exploiting positions to siphon government funds.
  - Limitations in the ability of reporting entities to reliably verify national identification cards, as well as confirm beneficial ownership of legal persons and arrangements.
  - Insufficient financial, human and technical resources across all LEAs and FIA.

### Sectoral factors attributing to Vulnerabilities

83. The money laundering vulnerability of individual sectors directly influences and shape a nation's overall exposure to money laundering risks. Sectors characterised by non-transparent transactions, complex ownership structures, or limited regulatory oversight substantially increase national vulnerabilities. On the other hand, robust anti-money laundering (AML) frameworks and effective risk-mitigation measures within vulnerable sectors can substantially reduce a country's overall risk profile.

Table 11: Summary of the sectoral vulnerabilities and overall impact and significance to national risk

Sector	ML Vulnerability Rating	Rating Justification
Precious Stones and precious metals, including semi-precious stones)	Medium High	high-value commodities, significant cash involvement, and difficulty in tracing origins of stones Weak AML/CFT coverage, especially in upstream and downstream diamond value chain activities.
Casino	Medium	high cash turnover, customer anonymity, and historical supervisory gaps.
Real Estate	Medium High	second largest GDP contributor but low oversight, presents opportunities for layering illicit funds through high value transactions, often cash-based, and structured to obscure ownership.
Banking	Medium	Diverse range of products and services offered; exposure to high-risk clients, expansion of digital and remote delivery channels; high volumes and values of international transactions effected through the global payments ecosystem; and cash-intensive services.
Legal Practitioners	Medium	the ability to create legal arrangements and financial structures that may obscure beneficial ownership.
Insurance	Medium	low cash involvement, limited cross-border product usage, life insurance products with investment components and cash-back features, Regulatory oversight exists, but there remains room for strengthening supervision and control measures across the sector.
Securities	Medium low	investment Institutions served as vehicles for large-scale cross-border investments, investment products in the securities sector are relatively simple and less sophisticated compared to those in developed markets, limited diversity of investment opportunities locally, cross-border flows coupled with limited investment product diversity locally. due to limited sector diversity and low liquidity, the customer base is primarily local, resulting in minimal foreign or non-resident participation
Auditors	Medium low	no reported typologies for the Audit Sector and no cases of fraud or tax evasion
Accountants	Medium low	maintain business relationships with higher-risk clients, including domestic and foreign PIPs, real estate entities and NPOs.
Trusts and Service Providers	Medium low	no STRs filed due to limited awareness on STR reporting requirement, limited PIP screening, high number of PIP client base, and limited typologies.
Other Financial Institutions	Medium	substantial scale and the diversity of credit products offered by some of the entities, lack of stringent corporate governance requirements for smaller firms, including demonstrated limited commitment to strengthening AML controls by management, high use of cash e.g. micro-lenders, pawnshops

84. The assessment of ML vulnerability considered the following risk factors; contribution to GDP, transaction volume and complexity, potential for ML misuse or facilitation and regulatory oversight strength. The table below presents the sizes of all sectors according to the contribution to the GDP, the ML vulnerability score and the weights assigned to each sector. The weight of 1 represents the least important while 10 represents the most important sector to the country's economy.

Table 12: Sector size contribution to GDP

	<b>Sectors</b>	<b>Contribution to GDP (P million)</b>	<b>Contribution to GDP (%)</b>	<b>Final Vulnerability Score</b>	<b>Weights (Assigned as per GDP)</b>
1.	Banking	5,707	2.17	0.54	9
2.	Securities	586	0.22	0.40	4
3.	Insurance	3,247	1.23	0.47	8
4.	Casino	N/A	N/A	0.52	
5.	Real Estate	9,711	3.69	0.57	10
6.	Precious Stone Dealers	5,043	0.97	0.55	7
7.	Legal Practitioners	819	0.31	0.50	5
8.	Auditors	1,480	0.56	0.41	6
9.	Accountants				6
10.	Trusts and Service Providers	304	0.12	0.41	3

N.B. The Sector contribution to GDP as at 2024 and the total GDP was P263,135 million<sup>4</sup>.

Note: "N/A" reflects sectors without separate GDP data but which carry significant ML/TF risk.

85. Botswana's overall national vulnerability arises from a combination of high-risk poorly supervised DNFBP sectors, and large, systemically important institutions. While the diamond value chain, casinos, and real estate present the most significant risk factors, the banking, insurance, and securities sectors contribute to national risk through scale, product complexity, and cross-border activity.

<sup>4</sup> Source: Statistics Botswana

## CHAPTER 4: SECTOR VULNERABILITIES

### (a) Banking Sector

86. Botswana's banking sector is relatively mature, stable, well-capitalised, profitable and characterised by strong regulatory oversight and significant progress in digital transformation. As at 31 December 2024, there were nine commercial banks and two statutory banks operating in Botswana, with total assets of P144 billion, customer deposits of P107.3 billion and gross loans and advances amounting to P87.1 billion. According to the Banking Supervision Annual Report, 2023, the banking industry was dominated by four (4) commercial banks which jointly controlled 74.9 per cent, 74.4 per cent and 71.3 per cent of total assets, deposits, and loans and advances, respectively – this posing as a concern for concentration risk.
87. Eight commercial banks are subsidiaries of foreign banking groups from the following countries.
- South Africa - Absa Bank Botswana Limited, Stanbic Bank Botswana Limited and First National Bank of Botswana Limited.
  - Malawi- First Capital Bank Limited.
  - Nigeria - Access Bank Botswana Limited.
  - Namibia - Bank Gaborone Limited.
  - India - Bank of Baroda (Botswana) Limited
  - United Kingdom - Standard Chartered Bank Botswana Limited.
  - BBS Bank Limited is the only local/indigenous commercial Bank. Botswana Savings Bank and National Development Bank are owned by Botswana Government.
88. The banking sector is actively embracing digital transformation by enhancing digital platforms, expanding mobile and internet banking services, and launching innovative solutions to enhance customer experience and promote financial inclusion. This proactive approach to digitalisation positions the sector for continued growth and adaptability in a rapidly evolving technological landscape. The increasing technologies reliance and interconnectedness exposes the sector to cyber vulnerabilities.
89. The financial sector plays a crucial role in economic development, however, the liberalisation of financial markets and greater connectivity between global financial markets, have increased financial system risks and crisis, and enabled the proliferation of criminal activities. Moreover, rapid technological advancement has facilitated adoption of borderless technology-based platforms in the financial system. These developments, could, if progressive and significant, become an increasing concern to the health of the financial sector and the general economy

### Main threats facing the Sector

90. The banking sector was assessed as posing a **High** money laundering threat.
91. The FIA Annual Report highlighted that in 2022/23 and 2023/24 financial years, the banking sector accounted for 69.6 and 88.7 per cent of all the suspicious transaction

reports (STRs) submitted to Agency. These STRs amounted to P1.7 billion and P420 million, representing 1.6 and 0.4 per cent of total customer deposits as at December 2023 and December 2024.

92. For the financial year 2023/24, the most prevalent suspected predicate offences were tax crimes, fraud, and illegal deposit taking facilitated through the banks. Tax-related offences involved the use of personal accounts to process business transactions and the externalisation of business proceeds. This included the non-declaration of business bank accounts and use of personal bank accounts for business purposes which were not declared to BURS.
93. Fraud offenses included obtaining money by false pretenses and various computer-aided scams. The Agency received 404 STRs linked to illegal deposit-taking activities, which observed patterns involving pyramid schemes (Ponzi), investment, religious, and romance scams. Additionally, the FIA ML/TF Trend Analysis Report (July to December 2023), revealed that the suspected perpetrators of financial crime were from various nationalities including Botswana, China, Zimbabwe and Zambia.

Patterns of Criminal Abuse in the Banking Sector
--

<p>The banking sector experienced the highest incidence of abuse for both predicate and ML offences, recording 82 cases. Of the P1, 109, 800, 686.72 laundered across various sectors, P649,732,034.69 was channelled through the banking system. A significant portion of these funds arising from four major cases was transferred to neighbouring countries including Zambia, Zimbabwe, and South Africa, as well as to offshore accounts held in Caymans Islands and Luxemburg.</p>
---

<p>In addition, the proceeds were transferred from Serbia into Botswana through the banking system and facilitated by legal practitioners. Overall, the banking sector recorded both the largest number of predicate offences committed through it and the highest value of funds laundered. of money laundered.</p>
--

### Banking Sector vulnerability

94. Given the nature of business, the size of their customer base, scale of operations, distribution channels and global reach, banks are more likely to have exposure to money laundering risks. Banks in Botswana are no exception to the inherent risks associated with;
  - the diverse range of products and services offered;
  - presence of high-risk customers in client base;
  - expansion of digital and remote delivery channels; and
  - high volumes and values of international transactions effected through the global payments ecosystem.
95. Although many banking products demonstrated low vulnerability to money laundering, the overall sector rating remained medium due to elevated risks associated with several products and services. These include deposits by legal entities, electronic banking channels, retail deposits, private banking and current accounts, retail credit facilities, wire transfers, and deposits made by prominent influential persons (PIPs). The

vulnerability levels of these products ranged from medium-low to medium-high, resulting in an overall medium vulnerability rating for the banking sector.

#### Product/channel Vulnerabilities in Banking Sector

96. The inherent vulnerability of each product was assessed using several variables including total size or value, average transaction size, client base profile, existence of investment or deposit feature, level of cash activity and frequency of international transactions of the product. The assessment focused on the most commonly used banking products and services namely: private banking, retail deposits, deposits by legal persons, credit facilities for retail customers and legal persons, current accounts, trade finance, deposits by PIPs, automated teller machines (ATMs) and/or automated deposit taking machines (ADTM), prepaid, debit and credit cards, point of sale transactions, internet banking, mobile banking, cash-send (money vouchers) services, bank-to-wallet, card-to-wallet and wallet-to-bank transfers.
97. The products and services offered by commercial banks were broadly similar, and the vulnerabilities identified were common across the sector.
- Private banking is mainly accessible to PIPs and high-net-worth clients. As at 31 December 2024, deposits to private banking as a proportion of total deposits was 13.83 per cent. Private banking and high-value deposit products were found to carry elevated inherent ML risks due to large transaction sizes, personalized services, and the ability to structure complex portfolios.
  - As at 31 December 2024, total banking industry deposit amounted to P107.3 billion, and retail deposits comprised 20.29 per cent of the total deposit. The retail deposit base is characterised by large number of customers, high volumes of small transactions that can be used for structuring as the transactions may be below reporting threshold. The level of cash activity associated with the product is high due to some cash intensive businesses. Deposits from legal persons and deposits by PIPs further heighten these risks because of the corporate structures, layered ownership, and political influence. Retail deposits, current accounts, and everyday credit products for both individuals and legal persons also contain inherent vulnerabilities, primarily due to their high transaction volumes and ease of access.
  - The banking sector carries out electronic funds transfer, both domestic and cross-border through the SWIFT platform. For the period January to December 2024, the total value of cross border inflows and outflows wire transfers were P216 billion and P201 billion, respectively. Wire transfers and cross-border payment channels presented inherently higher ML risks due to the speed and global reach of international fund movements. During the review period, cases were identified in which the banking sector was exploited for money laundering, as illustrated in the examples below.

### Cases of wire transfer abuses

#### Case A:

Wire transfer service was abused by suspect employed as a Money Market Dealer in one of the local banks who fraudulently transferred USD2, 064,239.49 (P22 million) into multiple individual's accounts narrated as beneficiaries.

#### Case B:

Wire transfers were abused in the tax evasion offences as the intelligence report received from FIA showed numerous transactions of transfers of funds going out of the country, with the investigations revealing that the company was under declaring income. Additional tax assessments amounting to P1, 919,698.80 for value added tax (VAT) and P3, 187,291.80 for income tax were made and the bank accounts were garnished to collect the funds.

- Trade finance was particularly more vulnerable due to cross border nature, third parties and complex supply chain involvement. Trade finance as a proportion of total deposits was 3.62 per cent. Because of its cross-border and third-party involvement, trade finance is considered a high-risk product that may be used to launder funds through under or over invoicing or fraudulent documentation.
- Vulnerabilities were also identified in ATM/ADTM usage, prepaid cards, debit/credit cards, through their high volume, widespread availability, and potential for anonymous or low-traceability activity.
- With Botswana embracing digital transformation by enhancing digital platforms, the associated risks of channels such as internet banking, mobile banking, cash-send vouchers, and electronic wallets inherently increase ML risks because they allow non-face-to-face interactions and fast, remote transactions. Criminals have been found to exploit these features to move funds quickly, use multiple accounts, or obscure their true identity.

### AML Controls & Mitigation

98. The overall quality of AML controls across the banking sector was assessed as adequate and effective in mitigating vulnerabilities. The assessment considered the robustness of the legal and regulatory framework, the implementation of a risk-based approach, customer due diligence (CDD) measures, and the use of automated monitoring systems and tools to detect ML risks. The review also evaluates the adequacy of monitoring mechanism and internal controls designed to identify and mitigate money laundering risks and the level of maturity and effectiveness of the compliance function in implementing regulatory requirements. Overall, the quality of general AML controls indicated that banks possess strong combating capabilities and exhibit lower residual vulnerability to associated risks. This is supported by a comprehensive AML legal framework and robust supervisory practices which further strengthen the sector's resilience. Where non-compliance issues are identified, the Central Banks devises appropriate supervisory action for the affected bank and in some instances, imposes monetary penalties. During the period under review, four banks were fined by the Central Bank for breaches of AML/CFT obligations as follows:

YEAR	BANK	FINES	REASONS FOR FINES
2020	Bank 1	P50 000	Failure to conduct risk assessment, ongoing customer due diligence, establish and verify the identity of beneficial owners of companies and identify prominent influential persons.
2022	Bank 2	P200 000	Failure to report large cash foreign currency exchange transactions conducted by non-bank customers.
	Bank 3	P250 000	Failure to file a suspicious transaction report with the Financial Intelligence Agency.
2023	Bank 3	P1.5 million	Failure to file a suspicious transaction report with the Financial Intelligence Agency, within prescribed period.
2024	Bank 4	P160 000	Maintaining relationship with trust customers that had not been registered with the Master of the High Court and failing to identify ultimate beneficiaries of some legal entities and trust.
			Failure to monitor and report large cash transaction and failure to provide accurate information to the Bank.

99. Market pressure was also found to play a significant role in reinforcing compliance within the sector. Institutions face strong expectations from regulators, counterparties, and customers to uphold high AML standards. This external pressure drives banks to maintain rigorous controls. Institutions maintain sound compliance systems, supported by reliable suspicious activity monitoring and reporting processes that ensure timely detection and escalation of risks.
100. The integrity and AML competence of bank staff also contribute significantly to overall effectiveness. Continuous training and strong ethical standards have helped ensure that employees can identify risks and comply with regulatory obligations.
101. Access to accurate information—such as beneficial ownership data, reliable identification infrastructure, and independent information sources—supports thorough customer due diligence and enhances the accuracy of risk assessments.
102. Overall, the alignment of legal, supervisory, institutional, and informational safeguards creates a robust and effective AML environment within the sector. Each component works together to address vulnerabilities and ensure that money-laundering risks are consistently identified, mitigated, and managed.
103. Based on all these factors, the overall ML vulnerability of the banking sector was assessed as medium. Given that the residual ML vulnerability of the banking sector is rated medium, while the ML threat is high, the sector’s overall ML risk is assessed as medium-high. Although the sector’s control measures are rated medium-high—indicating relatively strong mitigation and a moderate level of vulnerability, the elevated threat environment results in a residual ML risk of medium-high.

## (b) Securities Sector

104. The Securities sector consists of 114 entities of various types, primary of which include securities exchange, asset management and collective investment undertakings (CIUs) firms, investment advisors, custodial and trustee entities. The sector is an integral part of the country's economy given its size and nature, as it serves as a vital vehicle through which capital is raised, investments are made and wealth is created.
105. The sectors' assets under management is largely concentrated amongst asset management and CIU entities, which stood at P80 billion in 2024. On the other hand, the country's only exchange, the Botswana Stock Exchange boasts of a total market capitalization of P686 billion as at 2024, exceeding the country's GDP by more than two folds and making it the third largest in the southern African region by market capitalization. The table below shows a distribution of securities sector entities by type for year 2023 and 2024.

Table 13: Distribution of securities sector entities by type for year 2023 and 2024.

<b>Securities entities</b>	<b>No. of entities: 2024</b>	<b>No. of entities: 2023</b>
Asset Managers	20	19
Securities Brokers	3	3
Investment Advisors	18	19
Securities Infrastructure Businesses	2	2
Market Makers	2	2
Securities Services	1	1
Nominated Transfer Secretaries	1	4
IFSC Accredited Entities	1	1
CIU Management Entities	9	9
Local CIU Funds	49	46
Investment Companies	2	2
Trustees and Custodians	3	3
Custodians	3	3
<b>TOTAL</b>	<b>114</b>	<b>114</b>

106. The ML risk in the securities sector has been assessed as **medium**, considering the sector's customer base, products, services, and overall control environment. The market is mostly dominated by institutional investors, primarily domestic, which account for 87% of assets under management (AUMs) with the remaining share associated with retail customers.
107. The sector has implemented adequate control measures, including ongoing regulatory supervision, dedicated compliance functions, and routine AML training. However, three cases involving fraud and money laundering by asset managers point to significant risks

within the sub-sector. One case has resulted in a conviction, while the other two remain under investigation. Moreover, although investment firms typically use automated transaction monitoring systems, such systems are generally lacking among securities exchanges and brokerage firms, which poses a vulnerability given the high volume of transactions in those areas.

#### Main threats facing Sector

108. The securities sector was assessed as posing a **Medium** money laundering threat. The securities sector recorded low levels of threats during the assessment period. Among the four subsectors, Securities Infrastructure Businesses (SIBs) reported a few notable incidents related to market manipulation and insider trading, threats typically associated with securities trading. During the period, one case of market manipulation, six cases of director dealings, and one case of trading during a closed period were recorded. Additionally, approximately five incidents of integrity failures were reported, involving misappropriation of funds, conflicts of interest, and acts of dishonesty.
109. The sector also registered generally low levels of STRs during the review period. However, the low levels of STRs observed may indicate underreporting, which could result in an understatement of the actual threat levels in the sector.
110. Despite the overall medium threat levels, there was one money laundering case involving the use of a licensed asset manager by a prominent public official. The matter was brought before the High Court of Botswana, which resulted in a money laundering conviction. Overall, failure by directors of listed companies to report dealings within the stipulated timeframe remains the most common incident in the securities sector. The table below shows breakdown of each sector contribution.

Table 14: Breakdown of each sector contribution

Sector	No. Of Cases	Amount Involved (BWP)	Sector Weight	ML Rating	Threat
Securities	1	240 million	8	Medium	

#### Case study

ML typologies within the sector frequently arise from fraudulent schemes involving senior executives of investment institutions, often in collusion with the management of institutional investors to siphon funds.

In a convicted case, a senior executive of a retirement fund was found guilty of fraud, corruption, and ML after awarding over P500 million in fund assets to an asset manager without board approval and subsequently receiving property kickbacks. The funds were funnelled through various transactions to related-party companies, resulting in more than P200 million remaining unaccounted for.

The two ongoing investigations involve similar alleged misconduct, with estimated losses exceeding P240 million in customer funds. The cases highlight incidents of related party transactions that are not conducted at arm's length which are further exacerbated by governance failures. The scale of these incidents underscores the significant ML risk facing the sector

## Securities Sector Vulnerability

111. Overall, the Securities Sector ML vulnerability was rated **medium low**. Money laundering risks in the securities sector arise from complex financial instruments, hidden ownership structures, and cross-border transactions. Criminals exploit the speed and global reach of markets, using fraud and market manipulation to generate and launder illicit funds.
112. A number of key indicators were assessed to establish the ML vulnerability in the sector which included the overall size and value of institutions, portfolio complexity and diversity, customer profiles, portfolio liquidity, and the frequency of international transactions. Larger institutions, complex products, high-risk clients, liquid portfolios, and frequent cross-border activity increase exposure to ML risks. Other factors considered include the use of anonymous or omnibus accounts, known ML typologies, market manipulation, weak record traceability, non-face-to-face transactions, and any cash activity. These indicators collectively highlight the sector's susceptibility and guide supervisors in prioritising risk-based controls and oversight.

### Size and value of institutions

113. Asset and CIU management entities hold significant total assets and AUMs (P80 billion), representing nearly one-third of the country's GDP. This significant scale means the sector processes large volumes of funds, increasing the sector to ML risks. Smaller firms, however, often operate with limited financial and human resources, making them more susceptible to governance weaknesses and, consequently, more vulnerable to misuse for money laundering or related predicate offences such as fraud.
114. Securities Infrastructure Businesses, which include the exchange, securities depository, stockbrokers and transfer secretaries, supported 31 listed stocks on the main board as of end of 2024. The Exchange also listed four Exchange Traded Funds (ETFs) and one security on the Over the Counter (OTC) Board, which serves as a preparatory market for the main board. The bond market features a variety of instruments, including government, quasi-government, commercial paper, corporate, and sustainable bonds. The three stockbrokers recorded an average annual revenue of P6 million, with profits of up to P1 million.
115. There are 20 investment advisors and market makers operating in the sector. These entities are not permitted to hold customer assets and primarily offer advisory services. Consequently, their money laundering risks within the sector is considered minimal.
116. There are three Trustees and three custodians, all of which are subsidiaries of banking institutions. These entities safe keep a significant portion of the P80 billion AUMs managed by the asset and CIU management entities and also execute transactions on their behalf.
117. Overall, although the size and value of the sector is relatively small by international standards, it remains significant within the context of Botswana's economy. Given its scale, it is common for large volumes of funds to flow through the securities sector.

## Complexity and diversity of portfolio

118. Investment products in the Botswana securities sector are relatively simple and less sophisticated compared to those found in more developed markets. This limited product diversity previously justified allowing up to 70 percent of pension assets to be invested offshore. The straightforward nature of local investment offerings also makes regulatory easier and reduces their attractiveness for misuse. Overall, the sector's product complexity and diversity are assessed to be moderate.

## Customer profile

119. The securities sector is predominantly driven by institutional investors who hold segregated and pooled portfolios, as well as the majority of listed equities. Retail investors account for only 6.4 percent of the total AUMs, while institutional pension funds and institutional insurance customers contribute 88 percent and 6 percent, respectively. The securities sector is largely driven and dominated by institutional pension funds. Due to limited product diversity and low liquidity, participation remains largely domestic, with minimal involvement from foreign or non-resident investors.

## Portfolio liquidity

120. Liquidity in the securities market is largely influenced by the range of available products, stocks and instruments. In Botswana's securities sector, limited product diversity, combined with the dominance of institutional investors who generally adopt a buy-and-hold approach, results in markedly low market liquidity.
121. Consequently, and alongside the sector's relatively low size and lower product complexity, the securities sector is considered less attractive for money laundering purposes. Money market CIUs which are mostly attractive to retail customers, may be relatively more liquid due to their short-term investments nature (e.g money market funds) and therefore may elevate sector's vulnerability to money laundering. However, their overall money laundering exposure is moderated by the fact that they represent only 26 percent of total CIU AUMs, and thus do not significantly alter the sector's overall liquidity profile.

## Frequency of international transactions

122. International transactions in the sector are relatively infrequent. Most investments originate from local institutional customers, with limited appeal to foreign investors due to the sector's small size and low liquidity.

Table 15: Other vulnerability factor ratings

Vulnerability factor	Rating	Justification
Anonymous / omnibus use	Not available	Such accounts are prohibited in the sector, and strong customer due diligence are mandatory.
Existence of ML typologies	Exists	Only 4 reported alleged money laundering cases to date; overall risk is low.
Use in market manipulation	Exists but limited	Just 3 cases of trading during closed periods; considered minimal.
Record traceability	Easy to trace	Transactions are electronically recorded and are easily traced due to the sector's discouragement of the use of cash.
Non-face-to face use	Available but limited	Occurs through regulated intermediaries with mandatory customer due diligence requirements.
Level of cash activity	Low	Cash is generally discouraged.

123. While the above, mostly consist of vulnerabilities that are inherent to the sector, additional weaknesses relating but not limited to supervision were identified.

- The lack of a fully implemented sector-specific risk-based supervision (RBS) system for the review period has hindered the authority's ability to proactively identify non-compliance issues, including the three fraud and misappropriation cases mentioned in this report relating to the securities sector.
- Most of the reviewed risk assessments for the securities firms have yet to fully address the complexities associated with the sector's products and services, particularly the risks introduced through international customers and cross-border transactions.
- Additionally, most firms, particularly smaller ones by AUMs which are not part of a larger group, had not conducted independent reviews to evaluate the effectiveness of their compliance frameworks and this was largely due to the observed low commitment of leadership for the smaller firms with regards to cultivating a culture of compliance and adequately resourcing the compliance function.

#### AML Controls and Mitigation

124. Overall, the securities sector AML control capabilities were rated as Medium. The assessment of AML controls in the securities sector considered key indicators such as the quality of AML supervision, the commitment and leadership demonstrated by firms, the robustness of internal AML policies and procedures, and overall staff compliance. Securities firms have been progressively implementing measures to combat money laundering, and in most cases these measures were found to be proportionate to the size and risk profile of the respective institutions. Likewise, the supervisory authority's

ongoing efforts, particularly in providing guidance and enhancing sector-wide awareness, have contributed to improved compliance levels across the industry.

#### Quality of AML Supervision

125. The NBFIRA oversees AML compliance in the securities sector through its centralised AML/CFT Department, which is staffed by nine trained professionals. During the review period, the Department conducted 20 off-site inspections and issued several directives and guidance notes. One entity was fined P250,000, of which P230,000 was suspended. The Department also held regular capacity building workshops, focusing particularly on smaller entities with limited AML expertise. In 2023, the Department began piloting a sector-specific risk assessment tool, developed in line with its supervision manual, although its effectiveness has yet to be fully realised. Generally, the overall supervisory framework was found to be sound.

#### Commitment and Leadership of Securities Entities

126. The implementation of AML controls in the securities sector is to some extent shaped by the leadership of individual entities, though the degree of influence may vary. Well capitalised entities, i.e., investment firms tend to exhibit stronger governance and have dedicated substantial resources to bolster compliance. In addition, the majority of the investment firms are part of a larger group thereby leveraging the group wide controls.
127. Further, enhancements of the legal framework and directives/guidance notes issued by the NBFIRA appear to have prompted many securities firms to establish and resource their compliance functions. However, smaller entities with limited financial capacity such as stockbrokers and investment advisors are improving at a slower rate.
128. The NBFIRA observed increased awareness and engagement at governing body level, driven largely by the sector's desire to avoid punitive AML penalties and heightened sensitivity to reputational risk associated regulatory breaches and potential criminal exposure.

#### Quality of Internal AML Policies and Procedures

129. Due to the presence of comprehensive AML legislation in the country and guidance from NBFIRA, the documented controls within the sector are largely in line with international standards. This alignment is also supported by increased resourcing of compliance functions. The robustness of internal compliance frameworks appears to correlate with the size and complexity of firms within the securities subsector. Smaller entities such as advisory firms and brokers typically have simpler but proportionate policies and procedures, while larger firms integrate compliance within a broader enterprise risk management framework.

#### Compliance of Securities Companies' Staff

130. All securities firms were found to have established compliance functions, commensurate with the level of the perceived risk, with the quality and strength of the compliance

functions improving as the size and perceived risks increase. These better-positioned, specifically those that are part of a larger group showed evidence of senior management support and direct reporting lines to facilitate the management of regulatory risks.

131. Most firms demonstrated a basic understanding of key AML obligations, such as customer due diligence, and had documented controls in place. However, significant gaps remained in implementing more advanced requirements, particularly the adoption of a risk-based approach tailored to their size, risk exposure, suspicious activity/transaction monitoring and reporting. Only a small percentage of firms (30%), particularly investment institutions, had implemented systems for transaction monitoring and regularly carried out internal audits to assess the adequacy of their internal controls.

#### Residual Risk Rating

132. The money laundering risk in the securities sector has been assessed as Medium considering the sector's customer base, products, services, and overall control environment. Institutional investors, primarily domestic, account for 84.6 percent of AUMs. The sector has implemented adequate control measures, including dedicated compliance functions, and routine AML training. However, three cases involving fraud and money laundering by asset managers point to significant risks within the sub-sector. One case has resulted in a conviction, while the other two remain under investigation. Moreover, although investment firms typically use automated transaction monitoring systems, such systems are generally lacking among securities exchanges and brokerage firms, which poses a vulnerability given the high volume of transactions associated with listed equities.
133. Overall securities markets are inherently susceptible to money laundering due to factors such as large fund flows, high liquidity, international transactions, omnibus accounts, and rapid transaction speeds. However, the assessment highlights that Botswana's securities sector is relatively small, less liquid, and primarily composed of institutional investors who are subject to AML supervision. While gaps in supervision remain, oversight by NBFIRA has shown progressive improvement over time. The Authority had already started implementing a sector-specific risk-based supervision framework – albeit with some effectiveness concerns.

#### (c) Insurance Sector

134. The insurance sector comprises 23 insurers, 10 life insurers and 13 general insurers, together with seven re-insurers, five medical aid funds, and 216 intermediaries (including 147 corporate agents and 69 insurance brokers). Nineteen of the insurers are subsidiaries of international financial groups headquartered in South Africa. As at December 2024, the sector reported gross written premiums (GWP) of P7.4 billion and total assets of P20.9 billion, representing 2.8 percent and 7.9 percent of the country's GDP, respectively. The life insurance sub-sector dominates the market, contributing 85 percent of GWP and 81 percent of total assets, while the general insurance sub-sector accounts for the remaining 15 percent of GWP and 19 percent of assets.

## Main threats facing the Sector

135. The insurance sector was assessed as posing a **Medium-low** money laundering threat. The sector remained largely stable during the assessment period, with no significant threats reported. However, there were isolated incidents of fraud commission, where individual agents inflated the value of life insurance policies without customer consent to increase their commission payouts. Additionally, there has been a noticeable rise in attempted fraudulent claims involving falsified documents aimed at accessing life and funeral insurance benefits. Most of these attempts have been unsuccessful due to the sector's robust verification measures. Another growing concern among insurers is premium fraud, in which intermediaries fail to forward customer premiums to underwriters, ultimately leaving policyholders without coverage.

## Insurance Sector Vulnerability

136. The vulnerability of the insurance market was assessed based on inherent risk factors linked to the nature, design and characteristic of its products and services. Certain products are inherently more susceptible to money laundering abuse due to structural features. In Botswana, the insurance sector is composed of four main product categories being: life insurance, short-term (non-life) insurance, reinsurance and medical insurance, each offering a range of products tailored to different customer segments.
137. The assessment applied specific input variables to measure the inherent money laundering risk of these products. Certain risk factors such as cross-border exposure are most relevant to reinsurance, which caters both domestic and international insurers. Notably, insurance products are generally not offered to non-residents, except for individuals temporarily living abroad who maintain Botswana as their primary residence.
138. Reinsurance and retail life insurance products are assessed as having the highest potential for money laundering abuse. Vulnerabilities in reinsurance stem primarily from cross-border nature of the business, which increase exposure to imported jurisdictional risks. Retail life insurance, particularly high-value policies with investment add-ons, and savings components, also presents elevated risk due to their liquidity flexibility and presence of higher risk customer segments, including PIPs and high-net-worth individuals. In contrast, medical aid schemes and group life insurance products exhibit the lowest vulnerability because they are structured with limited transactional flexibility.

## Insurance Products Vulnerability Assessment

139. Botswana's insurance market comprises various products with differing structures and risk profiles. The overall assessment focused on the origin of funds, product features, target customer base, and AML/CFT controls in place. Below is a summary of the key product types:

### Annuities (Assured Retirement Income) – Low

140. Annuities involve a lump sum payment, (typically derived from regulated savings) in exchange for guaranteed stream of retirement income. These funds originate from

employer and employee contributions; their source is well documented and subject to regulatory oversight. The product does not include transactional or investment features that could be exploited for money laundering purposes. The high level of fund traceability, combined with supervision by NBFIRA, supports a low-risk rating.

#### Funeral Insurance – Low

141. These policies provide small sum-assured payout to beneficiaries upon the policyholder's death or their insured relative, typically to cover funeral expenses. With low premiums and benefits, and majority of customers being of low-income brackets, the product offers limited money laundering opportunities.

#### Credit Life Insurance (Retail) – Medium Low

142. This product is linked to loans and pays off outstanding debt upon the borrower's death or disability. Premiums are funded through the same loaned amount, and policies are typically bundled with bank loans. The risk is moderate due to the indirect nature of customer-initiated purchases and limited transparency in some customer risk ratings.

#### Group/Corporate Single-Premium Life Insurance – Medium Low

143. Provided to employees or members of legal entities, these policies are paid from corporate operational funds. The group nature of the product and its structured administration reduce money laundering exposure. However, moderate risk exists due to larger premium volumes and limited individual-level scrutiny.

#### Multiple-Premium Retail Life Insurance with Investment/Savings – Medium High

144. This personal insurance includes optional investment and borrowing components, enabling frequent deposits, withdrawals, and policy cessions. These transactional features heighten inherent ML vulnerability. The flexibility and liquidity of this product category warrant a medium-high risk rating.

#### Medical Aid Schemes - Low

145. Medical aid schemes provide financial coverage for members' medical expenses and typically operate as non-profit, membership-based societies, with administration outsourced to third parties. Most members are employees whose contributions are fully or partially funded by their employers and paid monthly. In 2024, total contributions reached P2.841 billion, with only 7.7 percent originating from individual members. Due to the traceable and legitimate nature of contributions, and the fact that funds are used exclusively for medical expenses, the sector is assessed as having a low vulnerability to money laundering abuse.

## Short-term insurance – Medium Low

146. General insurance contracts provide policyholders with financial protection against losses or damage to assets such as vehicles, homes, and business properties. These policies do not include cash-back, savings, or investment components. Coverage typically spans one year, with premiums payable monthly, quarterly, or annually. As of 2024, general insurance accounted for 22 percent of Botswana's gross written premiums, with property and motor insurance dominating the market at 32 percent and 29 percent, respectively. Other classes include liability, transport, and engineering insurance.
147. Since non-life insurance only disburses payments only upon a verified claim and does not involve cash accumulation, it is generally less attractive for money laundering abuse. However, the sector remains vulnerable to fraud through falsified or inflated claims. Consequently, both retail and corporate general insurance products carry a **Medium-Low** vulnerability rating.

## AML Controls & Mitigation AML Supervision

148. The insurance sector has experienced notable growth during the assessment period, reflected in both the increasing number of licensed entities and the rise in total assets and GWP. While AML supervision has strengthened in terms of quality of supervisory practices and the application of administrative sanctions, the number of supervisory staff and the scale of oversight activities have not kept pace with the sector's expanding market and increasing sophistication of products and services.
149. NBFIRA monitors AML compliance in the insurance sector through its centralised AML/CFT Department, which is staffed by nine trained professionals. During the review period, the Department carried out 18 on-site inspections and issued various directives and guidance notes. The Authority also held a limited number of bilateral supervisory meetings. As part of its enforcement efforts, the supervisory authority-imposed warnings and financial penalties ranging from P100,000 to P2.8 million on nine entities.
150. The Authority also conducted regular capacity-building workshops, with a particular focus on smaller entities that have limited AML capabilities. For much of the review period up to 2023, supervisory activities were guided by the broader 2017 National Risk Assessment (NRA). From 2024, the supervisory authority started using sector-specific risk assessment tools which improved targeted oversight based on risk profiles of individual entities.

## Commitment and Leadership of Insurance Companies' Management

151. A majority of the governing bodies of smaller insurance entities demonstrated limited understanding of ML risks specific to both the sector and their own institutions. This weakness is largely attributable to constrained financial resources, which limit the ability of these relatively new market entrants to provide management with adequate training and to translate such knowledge into actionable measures for managing ML and broader compliance risks. Although this vulnerability currently affects a small portion of the

market by GWP, it represents a growing risk given the sector's continued expansion in the number of licensed entities and the increasing market share of new entrants.

#### Quality of Internal AML Policies and Procedures

152. The quality of AML policies and procedures is directly dependent on the comprehensiveness of ML risk assessments, which should identify and evaluate risks to inform the design of internal controls. The insurance sector has demonstrated some improvement in developing internal AML frameworks underpinned by documented policies and procedures. However, for smaller insurance underwriters, control documents were not sufficiently tailored to risks relevant to their own operations and tended to remain generic, relying mainly on legislative and guidance requirements. Although these controls may be adequate in form, their application risks being inconsistent, either overly stringent or too lenient, due to the absence of risk-based tailoring stemming from inadequate institutional risk assessments. There remains scope for improvement in risk identification and assessment to ensure that controls are appropriately targeted.

#### Commitment and Leadership of Insurance Companies' Management

153. Insurance underwriters have generally demonstrated a willingness to enhance their compliance efforts, particularly in response to the supervisory authority's oversight and enforcement actions. The supervisory authority has made an observation through its monitoring reports that AML compliance has become a recurring topic at the board level, especially among larger underwriting entities which have been inspected. This has often been accompanied by increased investment in training and better resourcing of compliance functions, in contrast to smaller entities that continue to face resource constraints.

#### Quality of Internal AML Policies and Procedures

154. Driven by regulatory directives, all insurance underwriting entities have established compliance functions; however, the level of independence and resourcing varies across firms. The NBFIRA's requirement that compliance officers hold AML or compliance-related certifications has contributed to improved documentation of AML frameworks, bringing them more closely in line with legislative requirements and supervisory guidance. Larger insurance entities tend to employ more qualified compliance officers, and their internal control documents are generally more robust and well-informed to manage identified ML risks, reflecting the technical support and structured frameworks available within larger groups.

#### Compliance of Insurance Company Staff

155. Implementation of established controls remains inconsistent across insurance underwriters. Although some gaps may stem from legacy challenges associated with the late adoption of regulatory frameworks, they also reflect a generally limited compliance culture within certain organisations. Although the requirement for mandatory AML training for compliance officers has contributed to improvements in the

documentation of internal control frameworks, the implementation of these controls remains inconsistent across the sector. Monitoring reports issued by the supervisory authority have highlighted recurring instances of noncompliance, particularly in relation to risk assessments, CDD processes, transaction monitoring, and suspicious activity reporting. Weak implementation of CDD procedures is especially prevalent among customers on-boarded through intermediaries.

156. The assessment further noted a clear distinction in capability across the market; insurers with foreign parent companies generally benefit from more comprehensive training and demonstrate a stronger understanding of ML risks and control measures. In contrast, smaller entities continue to exhibit limited awareness and weaker control implementation, reflecting gaps in both resources and compliance culture.

#### Residual Risk Rating

157. The insurance sector's overall vulnerability to money laundering is assessed as **Medium**. This rating reflects several mitigating factors, including the low prevalence of cash transactions, minimal direct customer uptake of single premium life insurance, and limited cross-border usage of insurance products. Nonetheless, notable risks remain - particularly within the life insurance segment, where certain products include features such as cash-back options and investment or savings components that inherently increase exposure. Additionally, while regulatory oversight exists, there remains room for strengthening supervision and control measures across the sector.

#### (d) Other Financial Institutions Sector

158. Other financial institutions (OFIs) refer to financial institutions (Fis), operating outside the banking, securities and insurance sectors. For purposes of this assessment OFIs include FIs as defined by FATF that conduct activities such as lending, financial leasing, money or value transfer services, acceptance of deposits, and trading in foreign exchange. The categories of the OFIs assessed under this module are given under the table below.

Table 16: Categories of Other Financial Institutions and their supervisors

OFI Category	Total number of licensed/registered institutions	Supervisor
Micro Lending	282	NBFIRA
Pawnshops	52	
Financing Companies	68	
Leasing Companies	3	
Retirement Funds	91	
IFSC	60	NBFIRA other <sup>5</sup>
MVTS / EPS	24	BoB
Bureaux de Change	51	
Development Financial Institutions	2	FIA
SACCOS	100	DCD
Total	733	

<sup>5</sup> Other IFSCs without a designated Supervisory Authority

- (a) **Micro lenders** are authorised to provide loans exclusively to natural persons. As of 2023, the sub-sector served 208,713 customers, primarily salaried individuals. Most micro lenders utilize deduction codes that enable automatic repayment directly from the customer's income source.
- (b) **Pawnshops** serve individuals seeking short-term financial support by offering valuables—such as vehicles, jewellery, and electronics—as collateral. Their clientele mainly consists of residents including non-citizens living in Botswana. Transactions are generally of low monetary value.
- (c) **Financing and leasing companies** primarily serve both domestic and international institutional clients involved in public and private sector contracts and tenders. Many of these clients operate across multiple jurisdictions, including regional and overseas markets, which increases the sector's exposure to risk.
- (d) **Retirement funds** consist of fund administrators, pension funds, and provident funds, all supervised by the NBFIRA. As of December 2024, the sector comprised six retirement fund administrators and 85 retirement funds (seven provident funds and 78 pension funds). Among the pension funds, 73 are standalone, while five operate as umbrella funds. The sector has investment holdings totalling P139 billion, which are placed in a broad range of assets through a network of various investment managers in domestic and foreign markets.
- (e) **Money Value Transfer Service Providers (MVTs)/ Electronic Payment Service (EPS) Providers** are financial services that involve the transfer of money or value, locally and also across borders, outside of traditional banking systems. The MVTs include services that accept funds and deliver equivalent value through electronic communication or clearing networks. These service providers are authorized under the EPS Regulations, 2019.
- (f) **Development Finance Institutions (DFIs)** are entities established by the government to offer funding for development projects not typically financed by commercial banks. Botswana has two state-owned DFIs and these are: Citizen Entrepreneurial Development Agency (CEDA); which supports small and medium enterprises (SMEs) with funding and Botswana Development Corporation (BDC); which finances larger commercial, industrial, and agricultural ventures through debt and equity.
- (g) **Savings and Credit Cooperative Societies (SACCOS)** offer mainly savings products at attractive interest rates and loan accounts at affordable rates. The SACCOS are generally employer-based, and a few are community-based. They are further divided into financial and non-financial types. The sector also covers those in formal employment such as public officers and private sector employees. The SACCOS are registered and supervised by the Department for Co-operative Development (DCD) under the Co-operative Societies Act.

- (h) **Bureaux de change** are entities that exchange foreign currency. In Botswana, they are licensed and regulated by the Bank of Botswana. The Bureaux de change Regulations 2004 provides for licensing of Bureaux de change.
- (i) **International Financial Services Centre (IFSC)** are defined under section 137 of the Income Tax Act (Chapter 52:01) as a company incorporated to provide approved financial operations to its related or associated companies as stipulated under section 138 (7) of the Income Tax Act. The approved financial operations include: banking and financing operations; the broking and trading of securities; investment advice; management and custodial functions in relation to collective investment schemes; insurance and related activities; registrars and transfer agency services; accounting and financial administration; and other operations that the Minister of Finance may declare by Order from time to time to be approved financial operations. The IFSC regime primarily emanates from the array of tax benefits extended to companies operating within its framework. Notably, upon meeting the certification requisites, IFSC companies enjoy a preferential corporate tax rate of 15% on profits.

159. The overall money laundering vulnerability, threat and residual risk scores of each OFI category is summarized in the table below;

Table 17: Overall money laundering vulnerability, threat and residual risk scores of each OFI

Sector	Sector Vulnerability to ML	Sector ML Threats	Overall Sector Risk Score
Micro Lending	Medium	Low	Medium Low
Pawnshops	Medium low	Low	Medium low
Financing Companies	Medium	Low	Medium Low
Leasing Companies	Medium	Low	Medium Low
Retirement Funds	Medium low	Low	Medium low
IFSC	Medium high	Low	Medium
MVTS / EPS	Medium high	Low	Medium Low
Bureaux de Change	Medium	Low	Medium Low
DFI	Medium	Low	Medium Low
SACCOS	Medium low	Low	Medium low

#### Main Threats Facing OFIs

160. The threat assessment identified that the prevalent typologies within the OFI sectors were identity fraud, and cyber fraud (such as social engineering scams). Social engineering scams were reported to be committed mostly through the MVTS (mobile money) sector. In the micro-lending sector, the identified common fraud incidents were associated with impersonation scams, obtaining under false pretenses and identity theft where fraudsters used documents obtained from unsuspecting customers to illegally obtain loans and divert the funds to themselves. Other instances identified included customers using fraudulent or falsified documents to obtain credit facilities from micro lending institutions.

161. The threat associated with the IFSC sector emanated from the potential misuse of tax framework, whereby companies, often with limited or no substantive economic activity in Botswana may exploit IFSC status to benefit from preferential tax incentives. However, at a national level, there have been no significant cases linking IFSC to the top five predicate offences. As a result IFSC were therefore assessed to have a **low** overall money laundering threat.

#### OFIs Sector Inherent Vulnerability Assessment

162. As part of the inherent vulnerability assessment, four key variables were assessed: client base profile, level of cash activity, frequency of international transactions, and use of agents, all of which influence how attractive a sector may be to money launderers. Variables 5–10 further assess product and transaction related risks, including: potential for anonymity, traceability of transaction records, the presence of known money laundering typologies, sector’s susceptibility to fraud or tax evasion schemes, and the extent of non-face-to-face transactions. Collectively, these indicators provide a comprehensive understanding of each sector’s inherent exposure to money laundering risk.

Table 18: Inherent Vulnerability Factors (Variables 1-4)

Sector	1.Client base profile	2.Level of cash activity	3.Frequency of international transactions	4.Use of agents
<b>Micro Lending</b>	Medium	Medium High	Does not exist	Does not exist
<b>Pawnshops</b>	Medium	Medium High	Does not exist	Does not exist
<b>Financing Companies</b>	High	Does not exist	Medium High	Does not exist
<b>Leasing Companies</b>	High	Does not exist	Does not exist	Does not exist
<b>Retirement funds</b>	Low	Does not exist	Does not exist	Does not exist
<b>IFSC</b>	High	Does not exist	High	Does not exist
<b>MVTS / EPS</b>	High	High	High	High
<b>Bureaux de Change</b>	High	High	Does not exist	Does not exist
<b>DFI</b>	High	High	medium high	Does not exist
<b>SACCOS</b>	Medium	Low	Does not exist	Does not exist

Table 19: Inherent Vulnerability Factors (Variables 5-10)

Sector	5. Anonymous use of product	6. Difficulty in tracing transactions records	7. Existence of ML typologies	8. Use of business in fraud or tax evasion schemes	9. Non-face to face use of products
Micro Lending	Not available	Difficult/ time consuming	Exist	Exist and significant	Available but limited
Pawnshops	Not available	Difficult/ time consuming	Exist	Exist	Not available
Financing Companies	Not available	Easy to trace	Exist	Exist	Available but limited
Leasing Companies	Not available	Easy to trace	Exist	Does not exist	Not available
Retirement funds	Not available	Easy to trace	Exist	Exist but limited	Not available
IFSC	Not available	Easy to trace	Exist	Exist and significant	Not available
MVTS / EPS	Not available	Easy to trace	Exist	Exist and significant	Available but limited
Bureaux de Change	Not available	Easy to trace	Exist	Exist	Not available
DFI	Not available	Easy to trace	Does not exist	Exist	Not available
SACCOS	Not available	Difficult/time consuming	Does not exist	Exist	Available but limited

163. IFSCs and MVTS were assessed as having a medium high inherent money laundering vulnerability. This is primarily due to their client profiles, which includes foreign clients residing in jurisdictions under increased monitoring, and other clients having foreign business interests. Both sectors also service a notable number of domestic and international PIPs, further elevating their inherent risk exposure.
164. Further, the frequency of international transactions within the sectors was assessed to be high. The IFSC, in particular, conducts large volumes of inward and outward international transfers, including capital injections to different subsidiaries within the financial group. Similarly, the MVTS sector recorded a high volume of international transactions, with transfers amounting to P6.69 billion in 2024, as remittance payments. The sector is also characterised as fast paced, with transactions processed and received almost instantly. Moreover, the MVTS sector was assessed to have high level of cash activity, further elevating its vulnerability.
165. Micro lending, financing, leasing and DFI categories were assessed to have an inherent vulnerability rating of medium.
166. The micro-lending and DFI sectors were found to be cash intensive, as they frequently accept cash as a method of payment. Cash-based transactions significantly elevate money laundering risk because the origin of funds is often difficult to verify, making the scale of potential misuse higher compared to other payment channels.

167. Further, the DFI and financing sectors were assessed to have a medium-high frequency of international transactions with some transactions routed to high-risk countries, thereby increasing the money laundering vulnerability of these sectors. Additionally, the client base of financing, leasing and DFIs was assessed as high-risk, as the majority of customers are legal persons associated with PIPs.
168. In contrast, although the micro-lending sector provides loans to natural persons including PIPs, high-net-worth, and non-citizen residents, the majority of repayments are made through deduction at source. However, unlike other sectors rated as medium risk, most players in the micro-lending sector lack proper record keeping systems, making it difficult to monitor and trace transactions records and thereby increasing their vulnerability to abuse.

### AML Controls and Mitigation

169. As part of the AML control mitigation assessment, twelve key variables were evaluated across the sectors and grouped into two categories. Variables 1–6 assess the strength of the national AML environment, including the legal framework, supervisory effectiveness, enforcement of sanctions, entry controls, and staff integrity. Variables 7–12 assess institutional operational capacity, including staff AML knowledge, compliance functions, suspicious activity monitoring, access to beneficial ownership information, identification systems, and independent information sources. Together, these variables provide a concise view of how effectively the sector can prevent, detect, and respond to money laundering risks. The table below shows Quality of AML Controls (Variables 1-6).

Table 20: Quality of AML Controls (Variables 1-6)

Sector	1. Comprehensive ness of AML Legal Framework	2. Effectiveness of Supervision/ Oversight Activities	3. Availability and Enforcement of Administrative Sanctions	4. Availability and Enforcement of Criminal Sanctions	5. Availability and Effectiveness of Entry Controls	6. Integrity of Business/ Institution Staff
Micro Lending	Close to excellent	Medium high	Medium High	Medium High	High	Medium
Pawnshops	Close to excellent	Medium low	Medium High	Medium High	Medium High	Low
Financing Companies	Close to excellent	Medium	Medium High	Medium High	Medium High	High
Leasing Companies	Close to excellent	Medium	Medium High	Medium High	Medium High	High
Retirement Funds	Close to excellent	Medium High	Medium High	Medium High	High	High
IFSC	Close to excellent	Low	Medium High	Medium High	Medium High	Medium High
MVTS / EPS	Close to excellent	Medium High	Medium High	Medium High	Very High	Medium High
Bureaux de Change	Close to excellent	Medium	Medium High	Medium High	Very High	Medium High
DFI	Close to excellent	Medium	Medium High	Medium High	Very High	Medium Low
SACCOS	Close to excellent	Medium High	Medium High	Medium High	Medium High	Medium

Table 21 : Quality of AML Controls (Variables 7-12)

Sector	7. AML Knowledge of Business/Institution Staff	8. Effectiveness of Compliance Functions (Organization)	9. Effectiveness of Suspicious Activity Monitoring and Reporting	10. Availability and Access to Beneficial Ownership Information	11. Availability of Reliable Identification Infrastructure	12. Availability of Independent Information Sources.
Micro Lending	Medium Low	Medium Low	Medium Low	Medium	High	Very High
Pawnshops	Low	Low	Low	Medium	High	Very High
Financing Companies	Medium	Medium	Medium Low	Medium	High	Very High
Leasing Companies	High Low	Medium High	Medium Low	Medium	High	Very High
Retirement Funds	Medium High	Medium High	Very High	Medium	High	Very High
IFSC	Medium High	Medium High	Medium	Medium	High	Very High
MVTS / EPS	Medium High	Medium High	Medium High	Medium	High	Very High
Bureaux de Change	Medium Low	Medium Low	Low	Medium	High	Very High
DFI	Medium High	Medium High	Very High	Medium	High	Very High
SACCOS	Medium Low	Medium Low	Medium Low	Medium	High	Very High

### Quality of AML Supervision

170. The supervisory authorities responsible for OFI sectors have established units responsible for overseeing AML/CFT compliance in these sectors. During the period under review, sectors were subjected to regular onsite examinations and offsite monitoring to enhance risk based supervisory efforts. Furthermore, targeted awareness workshops were conducted, and various guidance notes were issued to entities. Supervisory authorities have imposed administrative sanctions from a wide range of available sanctions including monetary penalties, warnings, moral suasion and remedial action plans.

### Availability and Effectiveness of Entry Controls

171. Supervisory Authorities of OFIs have appropriate and effective entry controls in place. This is attributed to the fact that the supervisory authorities have sector specific legislation, procedures and rules that provide for the licensing and registration of OFIs. These entry controls provide for adequate fit and proper requirements applied on management and controllers of the OFIs.

### Quality of Internal AML Policies and Procedures

172. In general, the quality of AML compliance frameworks is closely tied to leadership commitment, adequate resourcing, and the presence of well-established compliance functions. Larger entities within the non-bank lending, MVTS, bureaux de change, IFSCs, DFIs, retirement fund and SACCOS sectors demonstrated a stronger

understanding of AML obligations, which were reflected in their documented frameworks aligned with AML legislation.

#### Compliance Level of Staff

173. It was observed that large non-bank lenders, bureaux de change and MVTs entities conduct employee integrity checks at onboarding, including verification of educational qualifications and criminal background screening. Additionally, staff within the leasing companies, retirement funds, IFSCs, MVTs and DFIs were assessed to possess high to medium high AML knowledge, supported by generally effective compliance functions.
174. However, it was noted that small micro-lending firms, pawnshops, financing companies, small bureaux de changes, and some SACCOS rarely provide AML/CFT training to their staff and Board members. Despite this gap, supervisory authorities have made concerted efforts to enhance sectoral understanding of AML/CFT obligations through awareness workshops, guidance notes and bilateral (one-on-one) engagements with each supervised entity.

#### Quality of Operations

175. Section 31 and 38 of the FI Act provides for AML/CFT records keeping and reporting of suspicious transactions. The MVTs, large bureau de change, retirement funds and DFI sectors have demonstrated effective and appropriate systems for record keeping and transactions monitoring that enhances the quality of their operations. Moreover, the leadership commitment and compliance levels of staff of these sectors were assessed to be adequate. However, the remaining OFIs have moderate to poor record keeping systems which affect their suspicious transaction monitoring and reporting capabilities.
176. A summary of the final Residual Risk Rating for the OFIs are presented on the table below.

Table 22: Final Residual Risk Rating for the OFIs

Sector	Final Risk
IFSC	Medium high
MVTS	Medium
DFI	Medium
Micro Lending	Medium
Financing Companies	Medium
Leasing Companies	Medium
Bureaux de Change	Medium
SACCOS	Medium low
Pawnshops	Medium low
Retirement Funds	Medium low

177. After consideration of the effectiveness of existing controls, the IFSC sector recorded a medium-high residual risk rating, primarily due to insufficient supervisory oversight. In contrast, the MVTS, DFIs, micro lenders, financing, leasing and bureaux de change sectors recorded a medium residual risk rating, reflecting the application of AML/CFT controls of moderate quality within these sectors.

178. The SACCOS, pawnshop and retirement funds sectors recorded a medium low residual risk rating due to the presence of adequate controls including effective supervisory oversight, robust market entry requirements and effective AML/CFT legal framework. These ratings also take into account the sector's medium low inherent vulnerability ratings.

(e) Designated Non-Financial Businesses and Professions

179. Designated non-financial businesses and professions (DNFBPs) are entities that while not classified as financial institutions, can be exploited for money laundering. Their services may enable criminals to move funds, obscure beneficial ownership, and give illegal activities an appearance of legitimacy. The DNFBPs sectors assessed in this report include :

- real estate,
- precious and semi-precious stones,
- gambling,
- legal practitioners,
- accountants,
- trust service providers and
- auditors

- (i) **The Real Estate Sector** in Botswana is made up of 4 categories namely; estate agency, property management, property valuations, and auctioneering; collectively referred to as real estate professionals. The sector has a total of 350 licensed real estate professionals. The real estate sector is regulated by the Real Estate Advisory Council (REAC), which is a regulatory body under the Ministry of Land Management, Water and Sanitation Services, mandated to regulate the activities of real estate professionals. REAC was established in terms of the Real Estate Professionals Act, 2003, to provide for the regulation of activities and conduct of the real estate profession in Botswana and other matters incidental thereto. Although REAC has licensed 350 real estate professionals, it supervises only 118 of them for AML purposes in accordance with the FATF guidance for the Real Estate Sector, which states that the focus of regulation and supervision should be on professionals involved in the buying and selling of real estate.
- (ii) **Precious and Semi-Precious Stones:** The term "dealer" according to the FATF, encompasses a wide range of persons (miners, intermediate buyers and brokers, precious stone cutters and polishers and precious metal refiners, jewellery manufacturers) who use precious metals and precious stones, retail sellers and buyers and sellers in the secondary and scrap markets. This supply chain is often defined in terms of the upstream (exploration, mining, sorting & valuing), midstream (rough trading, cutting and polishing, jewellery manufacturing), and downstream (jewellery wholesaling and retail) processes. In Botswana, dealing in precious stones requires authorisation or exemption under the Precious and Semi-Precious Stones (Protection) Act. Diamonds are central to Botswana's development and account for 80 percent of exports, one third of fiscal revenues, and one quarter of GDP. To manage diamond trade, Botswana in 2008 established the Diamond Hub. Diamond Hub was charged with a mission to transform Botswana into a competitive World Diamond Centre. The entities in the diamond industry in Botswana are categorized into three main groups: diamond producers, cutting and polishing/manufacturing, and diamond traders. In total, there are 99 supervised entities, consisting of 4 diamond producers, 50 cutting and polishing/manufacturing companies, and 45 diamond traders.
- (iii) **The Gambling Sector** is licensed and regulated by Gambling Authority ("the Authority") which is a corporate body established through an Act of Parliament. As of August 2024, the Gambling Sector had 8 casinos, 10 licensed betting operators and 6 limited payout machine operators. However, the assessment was limited to casinos as licensed betting operators and limited pay-out machine operators were not part of the scope of AML obligations for the assessed period, as they had recently been included in the supervised entities following the 2025 amendment of the Financial Intelligence Act.

- (iv) **The Legal Practitioners Sector** in Botswana has 384 law firms. The Law Society of Botswana ("The Society") regulates all the 384 law firms for purposes of AML/CFT compliance as mandated by the Financial Intelligence Act, 2022. It is important to note that the assessment of the legal professionals was compromised by the response rate of the sector which was not good representation of the sector population.
- (v) **The Accountancy Sector** comprises both citizens and non-citizens who are accounting technicians and professional accountants, operating primarily as sole practitioners, partnerships, or companies. Notably, non-audit firms managed by both accounting technicians and professional accountants form part of this diverse Sector. The Botswana Institute of Chartered Accountants (BICA), established under the Accountants Act of 2010, is mandated to regulate and develop the accountancy profession in Botswana. As at 31 December 2024, BICA had registered 276 accounting firms. Following the amendment of the Financial Intelligence Act in 2022, BICA's supervisory scope was refined to focus on AML/CFT supervision for accountants that carry out functions as stated in Schedule 1 of FI Act. Consequently, by the end of 2024, BICA supervised 181 member firms under this designation. Between 2022 and 2024, BICA conducted supervision of 169 firms to assess compliance with the Financial Intelligence Act.
- (vi) **The Audit Sector** in Botswana has a total of 31 audit firms which are regulated by Botswana Accountancy Oversight Authority (BAOA). BAOA was established by the Financial Reporting Act, 2010 as amended in 2020, as an independent oversight body of the accounting and auditing profession. The FI Act has designated BAOA as a supervisory authority for the audit sector for purposes of AML/CFT/CFP. For the period 2020- 2022 BAOA regulated all the 31 entities for AML/CFT/CPF compliance. The Financial Intelligence Act, 2022 introduced a limited scope of the auditors to be supervised for AML/CFT purposes and this reduced the number of specified parties falling under the audit sector to four audit firms. This change meant that audit firms that are not specified parties were no longer subjected to AML supervision.
- (vii) **Trust Service Provider Sector** is supervised by the Master of the High Court in terms of the Financial Intelligence Act. The Master of the High Court ("The Master") is an Office under the Administration of Justice which is established by the Administration of Estates Act, 1972. In addition, the Trust Property Control Act 2022 authorises The Master to keep a register for Trust Service Providers. The Master has 8 Trust Service Providers (TSPs) who are engaged in the arrangement and management of trusts. Of the 8 Trust and Company Service Providers (TCSPs), 7 are local companies, whilst one is based outside Botswana. The latest development is the Trust Control Property Act (Amendment of 2025), which came into effect on the 24th day of January 2025 and made provision for registration and fit and proper procedures for the TSPs by The Master. These complement the FI Act on preventing criminals and their associates from owning or controlling TSPs.

The registration process has not started pending regulations that will guide the registration process.

180. The individual money laundering vulnerability, threat and risk of each Sector is summarised in the table below.

Table 23: DNFBPs Sector Ratings

<b>Sector</b>	<b>Sectors ML Vulnerability</b>	<b>Sectors Threats</b>	<b>Sector Risk Score</b>
Precious Stones	Medium High	Low	Medium
Real Estate Professionals	Medium	Medium	Medium
Casinos	Medium	Low	Medium Low
Legal Practitioners	Medium	Low	Medium Low
Accountants	Medium	Low	Medium Low
Trusts Service Providers	Medium	Low	Medium Low
Auditors	Medium	Low	Medium Low

#### Main Threats facing the DNFBPs

181. As part of the threat assessment, law enforcement data and intelligence were sought to establish the extent, if any, of criminals using DNFBPs in their schemes to divert or launder proceeds of crime. Other than the real estate sector, all the other DNFBP sectors were assessed as having low ML threat, as there were no recorded cases nor any identified linkage to the prevalent predicate offences at a national level.
182. The real estate sector was assigned a medium ML threat rating, driven primarily by the existence of prevalent predicate offences recorded and the amount of proceeds linked to the sector compared to other sectors. Real estate was identified as one of principal channels through which criminal activities were facilitated, as out of the 126 recorded predicate offence cases amounting to P81, 187, 645.65 - 34 cases amounting to P1, 109,800,686.72, were associated with real estate transactions. The most common predicate offence linked to the sector is obtaining by false pretences.

#### DNFBPs Sector Vulnerability

183. The ML vulnerabilities common to DNFBPs sector vary depending on the nature of each business and the specific risks associated with their operations. Inherent characteristics include the complexity of transactions, potential for anonymity, and client base that may involve high-risk individuals or entities. Additional vulnerabilities arise from the nature of activities within the sector such as dealings in high-value goods, real estate transactions, and the use of nominee or intermediary arrangements—which can obscure the source of funds and conceal beneficial ownership. These vulnerabilities vary across the different entity types within the DNFBPs sector.

197. The table below, shows the varying levels of inherent vulnerability assessed for Botswana’s DNFBPs sector based on total size, client profiles, cash activity and other typologies with potential for abuse.

Table 24: DNFBPs Inherent Vulnerability Ratings

Sector	Gambling	Accountancy	Trust Service Provider	Precious Stone Dealers	Auditors	Legal Practitioners	Real Estate
Total size contribution to GDP (%)	Low	Low	Low	High	Low	Low	Medium Low
Client base profile	Medium	Medium	Medium	Medium	Medium	High	Medium
Level of cash activity	High	Does not exist	Does not exist	Low	Does not exist	Low	Low
Use of agents	Does not exist	Does not exist	Does not exist	Does not exist	Does not exist	Does not exist	Does not exist
Anonymous use of product	Not available	Not available	Not available	Not available	Not available	Not available	Not available
Difficulty in tracing transactions records	Easy to trace	Easy to trace	Easy to trace	Easy to trace	Easy to trace	Easy to trace	Easy to trace
Existence of ML typologies	Exists, but limited	Exist but limited	Exists	Exists	Does not exist	Exists& significant	Exists
Use of business in fraud or tax evasion schemes	Does not exist	Does not exist	Does not exist	Does not exist	Does not exist	Exists, but limited	Does not exist
Non- to face to face use of products	Not available	Available	Not available	Available	Not available	Available	Not available
<b>ML RATING</b>	<b>Medium</b>	<b>Medium</b>	<b>Medium</b>	<b>Medium High</b>	<b>Medium</b>	<b>Medium</b>	<b>Medium</b>

184. In determining the size of the sector, contribution to GDP was used as a key indicator. The precious stones sector makes a substantial contribution to the national economy, which in turn increases its attractiveness for large-scale illicit activity and heightens its vulnerability to money-laundering risks.

185. It was further observed that entities within the precious stones sector demonstrate varying levels of understanding regarding the identification of PIPs and the obligations associated with dealing with them. This knowledge gap increases the sector’s exposure to money laundering, as entities may unknowingly engage with PIPs without applying

the legally required enhanced due diligence (EDD), thereby creating opportunities for illicit funds to enter the financial system undetected.

186. **The legal practitioners sector** exhibits elevated ML vulnerability due to its customer profile, which includes PIPs, non-residents, and complex legal entities and arrangements. Lawyers' role in establishing legal structures and managing complex structures, such as trusts, companies, and partnerships heightens the sector's vulnerability to money laundering
187. A common typology highlighted by FATF as relevant to the legal profession include situations where legal professionals may overlook red flags in pursuit of financial gain.
188. The **Casino sector** is highly cash intensive as reflected by the high number of cash transaction reports submitted to FIA by the entities, therefore increasing vulnerability to criminal exploitation.
189. Other DNFBPs sector demonstrated lower ML vulnerabilities for other variables for several reasons.
  - they conduct very little business in cash, which limits opportunities for anonymous transactions,
  - they generally serve lower-risk customer profiles with minimal exposure to PIPs and legal arrangements, and
  - the businesses do not permit the use of agents, maintain easily traceable transaction records, and offer products and services that do not support anonymity.

#### AML Controls & Mitigation

190. In assessing the strength of AML/CFT controls across the sectors, consideration was given to a range of indicators aligned with the World Bank National Risk Assessment methodology. These indicators reflect the sector's overall control environment and its capacity to prevent, detect, and report money laundering. The assessment focused on the following key factors:
  - Quality of AML supervision, considering the effectiveness, frequency, and depth of supervisory activities and the regulator's ability to identify and address non-compliance.
  - Commitment and leadership of management and their involvement in setting the tone for compliance and the degree to which leadership prioritises AML/CFT obligations.
  - Quality of policies and procedures and whether entities have comprehensive, up-to-date, and risk-based AML/CFT policies and procedures that reflect legal and regulatory requirements.
  - Level of staff's capability, awareness, and their understanding of risks, ability to apply controls in order to reduce operational AML/CFT risks.

- Quality of the CDD framework, which measures the robustness of customer due diligence processes, verification of beneficial ownership, ongoing monitoring, and enhanced measures for high-risk customers.
- Quality of operations, which refers to the entity's operational systems and capacity to implement AML/CFT controls effectively

191. Together, these indicators form the basis for evaluating each sector's AML/CFT control environment and determining its overall resilience against money laundering risks. The table below, shows the individual ratings of the key indicators which in overall give a measure of the quality of AML Controls for DNFBPs.

Table 25: DNFBPs Ratings for Quality of AML of Controls

Intermediate variables	Real estate sector	Precious stones sector	Gambling sector	Legal practitioner	Accountant	Trust service providers	Auditors
Quality of AML supervision	Medium	Medium low	Medium high	Low	Medium high	Medium low	Medium high
Commitment and leadership of managements	Medium	Medium	Medium high	Medium low	High	Medium low	Medium high
Quality of policies and procedures	Medium high	Medium	Medium high	Medium	Medium high	Medium	Medium high
Compliance level of staff	Medium high	Medium low	Medium	Low	Medium low	Medium low	Medium
Quality of CDD framework <sup>6</sup>	Medium high	Medium high	Medium high	Medium high	Medium high	Medium high	Medium high
Quality of operations	Medium	Medium low	Medium	Low	Medium low	Medium low	Medium
Quality of AML controls	<b>Medium</b>	<b>Medium low</b>	<b>Medium</b>	<b>Low</b>	<b>Medium low</b>	<b>Medium low</b>	<b>Medium</b>

192. The quality of controls across the different sectors ranged from medium, medium-low, to low, indicating an overall moderate level of effectiveness, with notable weaknesses in several areas which may hinder the sectors' ability to adequately mitigate money laundering risks.

<sup>6</sup> The quality of the CDD framework depends on Availability and Access to Beneficial Ownership Information, Availability of Reliable Identification Infrastructure, and Availability of Independent Information Sources which were analysed and rated under National Vulnerabilities Module. On the basis of these ratings, the quality of CDD Framework was rated Medium High for all the DNFBPs.

## Quality of AML Supervision

193. BICA demonstrates the strongest AML/CFT/CPF supervision, supported by a structured risk-based framework, a dedicated AML division, and risk informed inspections. Ongoing sector engagement and the 2021 establishment of an independent AML Committee have further strengthened accountability and enforcement.
194. BAOA applies a risk-based supervisory approach, conducting inspections, issuing guidance, and providing awareness training. It uses moral suasion before escalating to disciplinary action. However, the absence of a dedicated AML budget and formal staff training programme limits its operational capacity.
195. Since adopting a risk-based approach in 2019, the Gambling Authority has strengthened supervision through inspections, awareness initiatives, guidance, a structured framework, and a dedicated AML/CFT/CPF budget, with an Enforcement Unit recently established. However, limited staffing and the absence of administrative fines despite identified deficiencies weaken overall effectiveness.
196. Similarly, REAC has conducted risk assessments, inspections, guidance, and awareness sessions, with moral suasion positively influencing compliance. However, insufficient staff, limited training, and a lack of a dedicated AML/CFT/CPF budget restrict effective risk-based supervision.
197. The Diamond Hub faces significant supervisory weaknesses. Despite a sectoral risk assessment and the development of a Risk-Based Supervision Manual, effectiveness is limited due to insufficient resources, no dedicated AML unit, and competing priorities. No administrative sanctions were issued, and moral suasion lacked follow-up. Although the Diamond Hub is prescribed as a supervisory authority in Schedule II of the Financial Intelligence Act, its supervisory powers are exercised through the Minister including licensing and administrative sanctions. This deficiency impacts its ability to effectively apply supervision measures including dissuasive sanctions.
198. The Master of the High Court had conducted a sectoral risk assessment and developed a supervisory manual in 2020. Outreach activities and guidance on risk assessments were delivered during the review period. However, the Master did not conduct inspections or impose sanctions on Trust Service Providers, despite having the legal authority to enforce compliance through fines, imprisonment, or deregistration of trustees.
199. The Law Society shows the lowest supervisory effectiveness. While it issues guidance, conducts trainings, and carries out inspections, its capacity is limited, with no dedicated AML/CFT budget, no internal training plan, and no administrative sanctions imposed.

## Availability and Enforcement of Entry Controls

200. REAC demonstrates strong controls when processing licence applications and management has maintained sound entry requirements, including minimum educational qualifications, police clearance, and annual fit-and-proper assessments. Weaknesses

persist due to the limited scope of regulation, as current laws require only individuals, not firms, to be licensed. The informal arrangement with Companies and Intellectual Properties Authority (CIPA) does not sufficiently capture general dealership companies acting as real estate agents. Furthermore, REAC lacks formal mechanisms to prevent criminals or their associates from holding beneficial ownership or management roles in real estate firms.

201. The precious stones and metals sector is regulated under multiple pieces of legislation, providing some structural safeguards for entry into mining and trading activities. Trading of precious stones requires a Precious Stones Dealer Licence (PSDL), and regulatory oversight exists along various stages of the value chain. However, mining houses are exempt from holding a PSDL and therefore fall outside the scope of the Financial Intelligence Act, creating a major regulatory gap. The Department of Mines does not assess applicants using AML/CFT or FATF-aligned standards, and penalties for non-compliance or unlawful entry are not sufficiently dissuasive.
202. The gambling sector exhibits strong entry controls supported by the Gambling Act, which requires thorough due diligence on applicants, shareholders, directors, beneficial owners including criminal clearance, tax compliance checks, ID verification, credit assessments, and security vetting. Fit-and-proper requirements apply both to operators and employees, who must renew their licences annually. AML/CFT obligations are clearly communicated, and establishments are required to appoint qualified compliance staff. Oversight has been effective, demonstrated by enforcement actions against illegal operators, including seizure and destruction of illegal gambling machines, and the revocation of a casino licence in 2023. The sector requires targeted AML/CFT training for its licensing personnel to strengthen fit-and-proper processes.
203. The accountancy sector demonstrates strong entry controls, supported by a clear registration framework under the Accountants Act. Individuals and firms must meet qualification and experience requirements and undergo annual renewal, including fit and proper tests for key personnel and beneficial owners. The BICA verifies applications for compliance with both the Accountants Act and the Financial Intelligence Act. AML/CFT capacity is strengthened by annual training covering beneficial ownership, customer due diligence, the risk-based approach, and ML/TF typologies. Only 22 suspensions were recorded across 276 member firms, with no criminal activity or convictions reported. These strong controls support a high rating for the sector.
204. Entry into the legal practitioners profession is clearly regulated under the Legal Practitioners Act, which sets out the requirements for admission and issuance of practising licences. Continued oversight is supported by provisions allowing the Law Society to conduct spot checks on trust accounts, and the Society has skilled personnel to monitor compliance. However, no cases were referred to law enforcement during the period under review, and no criminal sanctions were imposed, raising concerns about the effectiveness of monitoring and enforcement.
205. The Trust Property Control Act, amended in 2022, strengthened the sector by aligning the definition of beneficial ownership with the FI Act and introducing registration requirements for Trust Service Providers. The Master now maintains a register and has

enrolled eight TSPs, with fit-and-proper requirements incorporated into the amended legislation. There were no criminal sanctions recorded during the review period. Nonetheless, the sector faces notable weaknesses due to the absence of formalised regulatory provisions outlining TSP registration requirements. In the interim, the Master relies on a self-developed form that includes criminal declarations, and full implementation awaits finalisation of supporting regulations.

206. The audit sector has strong foundations, with the BAOA required by law to register auditors and conduct fit-and-proper assessments during both initial registration and annual renewals. No illegal operators or licence suspensions were recorded during the period, and only 4 applications were rejected in 2024 for failing to meet requirements. No criminal sanctions or convictions were recorded during the review period. However, the sector faces resource constraints, particularly budget limitations that restrict the number of skilled personnel available to enforce AML/CFT compliance during onboarding. Additionally, the registration requirements do not explicitly incorporate AML-specific entry controls.

#### Quality of Policies and Procedures

207. Diamond producers and manufacturers demonstrate stronger AML controls than traders, many of whom are dormant and therefore vulnerable to misuse. Policies, risk assessments, and Compliance Officers are in place. However, there are infrequent updates of risk assessments, and inconsistent independent audits.

208. All eight licensed casinos have AML/CFT policies, guidelines, Compliance Officers, staff training, and some independent audits. However, some Compliance Officers often carry multiple responsibilities, resources are not always commensurate with operational complexity relative to the size of the institution, irregular risk-assessment updates, and inconsistent AML audits.

209. Legal practitioners maintain AML/CFT programmes and conduct annual risk assessments, with Compliance Officers appointed at management level. Despite this, most Compliance Officers are not dedicated, which compromises independence, and most entities do not perform internal AML/CFT audits.

210. The real estate entities have designated Compliance Officers, AML programmes, CDD/EDD for PIPs and high-net-worth clients, trained staff, and institutional risk assessments. However, there is no clear AML budget, few independent audits are conducted, and low transaction volumes reduce the perceived urgency of AML reviews.

211. Accounting firms have appointed Compliance Officers at various seniority levels, and often adopt integrated compliance structures. However, most of the firms have not conducted independent AML/CFT audits, and many sole practitioners rely heavily on BICA training.

212. Most audit firms appoint Compliance Officers, conduct annual risk assessments, and comply with the FI Act. Smaller firms, however, lack dedicated Compliance Officers,

internal AML/CFT audits limiting the assessment of the adequacy and effectiveness of their AML/CFT controls, and PIP-risk awareness is insufficient.

213. Most TSPs have AML/CFT policies, perform annual risk assessments, and maintain AML units. Nevertheless, 5 out of 8 have not appointed Compliance Officers at management level, reducing their independence and weakening the compliance function.

#### Compliance Level of Staff

214. The real estate sector demonstrates structured AML/CFT practices, including staff vetting at on-boarding, fit and proper tests conducted by REAC during on-boarding and license renewals, designation of compliance officers at management level, implementation of AML programmes, institutional risk assessments, and application of a risk-based approach. Staff have received training, either internally or through REAC, However, ongoing staff vetting is limited, there are no formal mechanisms to protect staff reporting suspicious activities, training is not continuous, AML compliance budgets are ad hoc, and independent AML/CFT audits are rare.
215. Diamond Hub and precious stone dealers indicate that while some entities conduct criminal background checks and fit and proper tests are performed for all key persons, employee vetting across the sector is generally inconsistent. AML training is limited in most dealers, primarily restricted to compliance personnel, with minimal capacity building, whereas diamond producers demonstrate stronger practices by providing training to all staff across departments. Overall, sector-wide AML knowledge and implementation remain inadequate, limiting employees' ability to fully understand and apply compliance obligations.
216. All casinos have employee recruitment and vetting procedures, including police and past employment checks, and conduct fit and proper tests before license issuance and renewal. Policies protect staff reporting suspicious transactions, and disciplinary measures for breaches, particularly fraud, are generally robust. AML/CFT training is provided sector-wide, covering legal frameworks and ML/TF typologies. However, inconsistencies in ongoing vetting and in the implementation and frequency of AML/CFT training persist.
217. The Law Society conducts fit and proper tests for all entrants, and some firms perform initial staff vetting including employment history and criminal checks, with AML/CFT training and refresher programs provided across the sector. However, ongoing vetting is rare, anonymous STR reporting mechanisms are limited, most firms lack protections for staff reporting STRs, and training is inconsistent and insufficient for full sector coverage.
218. The accounting sector demonstrates structured oversight through BICA's fit and proper tests at registration and annual renewals, adherence to a professional code of ethics, and enforcement by the Disciplinary Committee. All firms provide general AML/CFT training at least annually, ensuring baseline awareness of regulatory obligations. However, only 20 percent of firms conduct pre-employment screening of key personnel, ongoing vetting is largely absent, safeguards for staff filing STRs are inadequate, and

55 percent of firms do not provide role-specific training for customer-facing staff, limiting practical AML/CFT application.

219. The TSP sector demonstrates structured staff vetting, with most entities conducting integrity screening at on-boarding and continuously throughout employment, and a fair level of AML/CFT/CPF knowledge. Some firms provide continuous internal training, while the majority rely on external training from FIA or the Master. However, gaps exist in targeted and ongoing internal training, and a few TSPs lack adequate employee screening, increasing the risk of employing staff susceptible to facilitating money laundering.
220. The audit sector demonstrates structured oversight, with staff vetting conducted at on-boarding and supplemented by BAOA's fit and proper tests during registration and renewals, while disciplinary procedures address the few integrity breaches reported. Most firms provide AML/CFT/CFP training and participate in regulator-led sessions, positively impacting staff knowledge. However, ongoing vetting is limited, and refresher training particularly for staff responsible for on-boarding clients remains insufficient.

#### Quality of Operations

221. The real estate sector has basic systems in place for monitoring transactions and client profiles, and record-keeping practices exist. Entities demonstrated some awareness of PIP screening and the need for enhanced due diligence for high-net-worth clients. A total of 103 out of 118 entities registered on the goAML platform; however, only two STRs were filed due to limited understanding of reporting obligations. This low reporting rate weakens the sector's ability to detect and respond to suspicious activity, ultimately reducing operational effectiveness.
222. The precious stones and metals sector did not submit any STRs during the review period, largely due to insufficient monitoring systems and weak operational controls among reporting entities. Deficiencies were noted in record-keeping, client and transaction monitoring, and the screening of high-risk clients, including PIPs, high-net-worth individuals, and clients from high-risk jurisdictions. These shortcomings undermine the sector's ability to implement effective AML/CFT measures.
223. The gambling sector shows comparatively strong operational controls. All the casinos have a central electronic monitoring system (CEMS) in place for monitoring play and transactions and client profiles. All casinos have policies to guide STR identification and reporting, and are registered on goAML, and use gaming systems and closed-circuit television (CCTV) to monitor staff and customer behaviour. Records are kept electronically for 20 years, and casinos actively monitor PIPs, clients from high-risk jurisdictions, and high-net-worth clients, although most conduct screening manually, with only some using commercial databases. The sector submitted nine STRs during the review period, and eight were rejected due to missing mandatory information. Ongoing refresher training is being provided by the Financial Intelligence Agency to improve reporting quality.

224. The legal practitioners sector relies heavily on manual processes for PIP screening, transaction monitoring, and suspicious activity detection. Although systems for transaction recording exist, the use of automated monitoring tools remains limited. Several firms are still not registered on the goAML platform, and no STRs were filed during the review period.
225. Most accountancy sector firms maintain manual controls for identifying and escalating suspicious activity, but actual STR reporting remains very low. While 97 percent of sampled firms are registered on goAML, fewer than 10 percent submitted STRs despite the sector’s significant client base and exposure to ML/TF risks. This low reporting level heightens vulnerabilities and highlights the need for strengthened BICA guidance and sectoral awareness.
226. Audit firms maintain CDD and transaction records for 20 years and make use of both automated and manual systems for PIP screening, monitoring, and reporting. All firms are registered on goAML, yet only one STR was submitted during the review period, and this was pointed out during an inspection. Despite systems being present, the limited reporting points to gaps in understanding or implementation.
227. Operational quality within the Trust and Company Service Provider sector is limited and inconsistent. Only half of the TSPs have systems for PIP screening, while the remainder conduct no screening at all. Suspicious transaction detection is extremely limited, with only one TSP having any system in place to support this function.

#### Residual Risk Rating

228. Based on the assessment, the residual ML vulnerability was determined as in the below table.

Table 26: Residual Money Laundering Vulnerability Rating for DNFBPs

Sector	Gambling	Accountancy	Trust Service Providers	Precious Stone Dealers	Auditors	Legal Practitioners	Real Estate Professionals
Inherent Vulnerability	Medium	Medium	Medium	Medium High	Medium	Medium	Medium
Quality of AML Control	Medium	Medium Low	Medium Low	Medium Low	Medium	Low	Medium
Residual Vulnerability Rating	<b>Medium</b>	<b>Medium</b>	<b>Medium</b>	<b>Medium High</b>	<b>Medium</b>	<b>Medium</b>	<b>Medium</b>

## CHAPTER 5: TERRORIST FINANCING RISK ASSESSMENT

### Overview of Global Terrorism Financing Landscape

229. Terrorism threat is constantly evolving because perpetrators continue to change their tactics and adopt new ways, which are difficult to detect. Global trends indicate that over the last two decades, the epicenter of terrorism has shifted from the Middle East and North Africa into the Sahel Region of Africa. The Sahel accounted for 51 percent of global terrorism deaths in 2024.<sup>7</sup> Islamic states operate as a decentralized network of affiliates, encompassing nine Jihadist groups and affiliated entities.<sup>8</sup> It maintains an enduring global enterprise, promoting a large-scale terrorism campaign across Africa, the Middle East and Asia. It expanded its recruitment and operations across key locals within regions and grew its global networks to approximately 20 branches and affiliates.<sup>9</sup> In 2024, these affiliates were responsible for attacks across the Middle East, Africa, Asia and Europe, whereas Syria and DRC were the most affected by IS activities in 2024, experiencing the highest number of fatalities.
230. Classical terroristic groups found to be operating in the African region include the Islamic State, Boko Haram and Al Shabaab. Reports have shown that the impact of terrorism is far higher in Sub-Saharan Africa, the Middle East and North Africa (MENA) and South Asia than any other region in the world. These three regions accounted for 94 percent of deaths from terrorism in 2023, with Sub Saharan Africa alone accounting for just under 59 percent of all fatalities.<sup>10</sup> Burkina Faso, Mali, and Niger account for most of the terrorism deaths in the region.<sup>11</sup> Several factors have fuelled the current crisis in the Sahel region including climate change, poor governance, ethnic polarisation, abuse by state security, pastoral conflict, the growth of transnational Salafi-Islam ideology, conflict over natural resource extraction (particularly gold), and the presence of external actors.<sup>12</sup> Salafi-Jihadis and Bandits have looked to exploit socio-economic, political vacuums as well as grievances. Terrorism usually occurs as a tactic within a conflict setting, used by groups looking to bring about political change.
231. The remainder of sub-Saharan Africa has also seen steady increase in terrorism during the period under review, with the largest increase in terrorist attacks being reported in Mozambique, Somalia and DRC. Terrorist attacks in Mozambique are reported to have increased forty-fold since 2013.<sup>13</sup> In Southern Africa, there are growing security concerns over the attacks carried out by Al Sunnah Wa Jama'ah (ASWJ) in northern Mozambique, many of which have been claimed by the Islamic State Central Africa Province (ISCAP). Despite the counter terrorism operations by the Southern African

---

<sup>7</sup> Global Terrorism Index, 2025.

<sup>8</sup> US Country Report on Terrorism, 2023.

<sup>9</sup> US Country Report on Terrorism, 2023.

<sup>10</sup> Global Terrorism Index, 2025.

<sup>11</sup> Global Terrorism Index (GTI), 2023 pg. 2

<sup>12</sup> GTI, pg. 62

<sup>13</sup> GTI, pg. 60

Development Community (SADC) Mission in Mozambique (SAMIM), the group remains active.

232. The insecurity in the eastern DRC, continues to fuel a long-standing humanitarian crisis. These devastating atrocities were caused by several armed groups including Allied Democratic Forces (ADF)/Islamic State Central Africa Provinces (ISCAP), Congo Development Corporative (CODECO) and March 23 Movement (M23). Despite the deployment of the SADC Mission in DRC (SAMIDRC), and repeated cease fire arrangements, heavy fighting between the Congolese Army and the M23 Armed Group remains active resulting in loss of lives for civilians and security officers in the DRC.

#### Botswana TF Context

233. During the period under review, Botswana had not recorded any terrorist attack but had one (1) case<sup>14</sup> of terrorism financing which was registered in 2019. The case was withdrawn without prejudice in 2020. Notwithstanding the reported case, the opinion of officials and law enforcement agencies is that Botswana has no known exposure to any terrorist group or individuals. However, Botswana's proximity and involvement in SAMIM makes the country a potential target due to retaliatory attacks by ASWJ<sup>15</sup>.
234. Botswana's overall ranking in the 2024 Global Terrorism Index is 89,<sup>16</sup> and its score is 0. In relation to the impact of terrorism between 2020 and 2024, Botswana has been consistent with no changes in its rankings.

#### Terrorist Financing Risk Assessment Methodology

235. The assessment relied on the World Bank's methodology to identify and assess TF risks. This was augmented by the Terrorist Financing Risk Assessment Guidance issued by the FATF, the International Monetary Fund (IMF) guidance, and the National Terrorism Financing Risk Assessment of other countries such as South Africa.
236. The World Bank tool recommends that TF threat assessment be performed separately from the ML threat assessment.<sup>16</sup> Likewise International Monetary Fund<sup>17</sup>, considers it good practice to assess, and thus understand, terrorist financing risk separately from ML risk. This is on the grounds that while ML and TF share some common attributes, their threats and consequences are sufficiently different to require assessing terrorist financing risk separately. Moreover, the TF threat only overlaps with the ML threat when

---

<sup>14</sup> *State v. Weleminah Maswabi* (Maswabi case/reported case). In October 2019, the DPP registered a criminal case against the accused, Ms Maswabi, on charges that included TF. The case was on the basis of information shared during inter agency cooperation by LEA's. On 17th November 2020, the TF charge was withdrawn without prejudice. See DPP update, Botswana's ICRG Progress Report, April 2021 [pg. 183]

<sup>15</sup> <https://www.facebook.com/TheGazettebw/posts/the-botswana-defence-force-bdf-has-warned-of-the-possibility-of-terrorists-strik/10159321947092620/> <sup>16</sup> Global Terrorism Index 2024 [pg. 7]

<sup>16</sup> See third paragraph on page 5 of the World Bank Guidance Manual, Terrorist Financing Risk - National Risk Assessment Tool.

<sup>17</sup> Countering the Financing of Terrorism Good Practices to Enhance Effectiveness

terrorist funding comes from criminal activity. Vulnerability analysis shares some features but also deals with aspects that are unique to the financing of terrorism. Due to the distinct nature of TF, the TF threat assessment was thus performed separately from the ML threat assessment. The ML and TF assessments were, however, conducted in parallel and working groups benefitted from interacting with each other and exchanging inputs and views.

#### National TF Threat Assessment

237. The overall national TF threat was determined to be very low on account of the very low cross-border threat posed by sympathizers transiting through Botswana and the incoming threat due to Botswana's exposure to threats from neighbours with active terrorism due to the country's intervention in Mozambique as part of the SAMIM. Both domestic TF threat and the international TF threat were determined to be very low.

238. The national TF threat assessment examines the raising, moving, storing, and use of funds to finance terrorists, terrorist organisations, or their operations. It considers the country's TF threat profile, including exposure to terrorism and contextual factors such as demographic composition and geographic location. The assessment also evaluates potential TF exposure through the provision of strategic goods or services, such as machinery, vehicles, equipment, or weapons that could be used for terrorist purposes. The following variables were also assessed:

- Active terrorist threat within the country;
- Terrorists persons or organisations; risks posed by individuals or organisations that may support or facilitate terrorism;
- Threat from sympathisers who could provide financial or logistical assistance;
- Terrorist activity in neighbouring countries and potential spillover effects;
- Risks linked to the country's role as an international and trade hub, which may be exploited to move funds or goods; and
- Potential misuse of strategic goods, such as machinery or equipment, for terrorist purposes.

Table 27: Terrorist financing variables risk rating

<b>Active Terrorist Threat</b>		
<b>Variable</b>	<b>Rating</b>	<b>Motivation</b>
<b>A. Domestic Active Terrorist Threat</b>	<b>None and Constant</b>	Botswana has not recorded any presence of terrorist organisations/individuals and terrorist activity. Further, Botswana’s overall rank in the 2024 Global Terrorism Index is 89, <sup>18</sup> and its score is 0. In relation to the impact of terrorism between 2020 and 2024, Botswana has been consistent with no changes in its rankings.
<b>B. Cross-Border Terrorist Threat</b>	<b>None and Constant</b>	Botswana remains on high alert from potential attacks due to spill overs from countries with active terrorist activity in the region such as Mozambique and the Democratic Republic of Congo. Botswana’s proximity and past involvement in the SADC Mission in Mozambique (SAMIM) makes the country a potential target. The possibility of retaliatory attacks in response to military deployment by SADC countries was announced by the terrorist organisations.
<b>Terrorist Persons and Organisations</b>		
<b>Variable</b>	<b>Rating</b>	<b>Motivation</b>
<b>A. Domestic TF Threat arising from Terrorist Persons and Organisations</b>	<b>None and Constant</b>	There were no convictions related to terrorism or terrorism financing. Further, there were no reasonable grounds to believe that a person or group in Botswana were engaged in terrorism, owned, controlled or acting on behalf of a designated terrorist or terrorist group. However, one case of terrorist financing was registered before courts in 2019 and was withdrawn before the court without prejudice in 2020. The Government’s official position is that the case lacked merit and was withdrawn. Therefore, the risk assessment determined that there are no terrorist organisations/persons active in Botswana nor any fundraising activity. Consequently, it was found that the criteria on level of funding, sources of funding, types of assets used or channels of transfer as not applicable.
<b>B. Cross-Border TF Threat arising from Terrorist Persons and Organisations</b>	<b>None and Constant</b>	<p>Given the absence of known or suspected terrorism or TF cases, the assessment considered how terrorist organizations that are active in the region may raise, use or move funds and other assets in Botswana. In this regard, the assessment considered the incoming threat as the outgoing threat was found inapplicable.</p> <p>Notwithstanding the expressed intention by ASWJ to launch terrorism activities in countries that participated in the SADC mission as a retaliatory measure, there is no detected TF incident of ASWJ moving or using funds for TF in Botswana. Similarly, there were no detected incidents for inward TF threats by other terrorist persons or groups to Botswana.</p>

<sup>18</sup> Global Terrorism Index 2024 [pg. 7]

<b>Sympathizers</b>		
<b>Variable</b>	<b>Rating</b>	<b>Motivation</b>
<b>A. TF threat associated with persons that may be sympathetic to terrorist organizations, persons, or ideology</b>	<b>None and Constant</b>	Threat not been identified in Botswana. Consequently, there are no convictions, prosecutions, investigations or MLAs relating to terrorist financing by persons sympathetic to terrorist organizations.
<b>B. Cross-border threat of sympathizers</b>	<b>Very-Low and Decreasing</b>	In 2022, Botswana received a foreign request for information regarding a suspected ISIS sympathizer that had transited through Botswana. The matter was followed up and it was established that the individual transited through Botswana from Zambia to South Africa in 2018 and there was no evidence of the subject raising, moving or using funds for TF through Botswana. Further, there are no incidences (intelligence, STR, request for information) of outgoing remittances with active terrorist threat locations with links to TF.
<b>Neighbours</b>		
<b>Variable</b>	<b>Rating</b>	<b>Motivation</b>
<b>A. Active terrorist threat in the neighbouring jurisdictions</b>	<b>Very-Low and Constant</b> for both domestic and cross-border threat.	<p>There were no reported incidents of terrorism activity during the review period in countries where border is shared presence of IS sleeper cells (sympathizers) and extremist right-wing groups in South Africa were considered. Proceeds of crime generated by IS supporters in South Africa through kidnapping for ransom, extortion and smuggling activities (commodities, drugs, etc.) are largely used for sustaining activities of IS cells active in the country. Further, IS sympathizers in South Africa are considered to redirect terror finance generated in other countries in the region through informal and cash-based channels back to originating countries.<sup>19</sup></p> <p>Further, ASWJ terrorist activity in Mozambique were considered due to close regional proximity. From 2020-2023 Islamic terrorist attacks in Mozambique resulted in over 2100 civilian deaths. The violence saw a peak in 2021 with a total of 2080 deaths.<sup>20</sup> After escalating rapidly through 2021, northern Mozambique saw a nearly six fold decline in deaths over the next 3 years. This decline is linked with the arrival of the SADC and Rwandan security forces in July 2021. However there has been a rebounding of violent events and fatalities linked to the militant Islamists in 2024.<sup>21</sup></p> <p>There are no recorded incidents of funds transfer between Botswana, South Africa Mozambique related to terrorism financing.</p>

<sup>19</sup> South African National Terrorism Financing Risk Assessment, 24 June 2024.

<sup>20</sup> <https://africacenter.org/spotlight/mig-2024-africa-constantly-evolving-militant-islamist-threat/>

<sup>21</sup> <https://africacenter.org/spotlight/mig-2024-africa-constantly-evolving-militant-islamist-threat/>

Finance and Trade Hub Function of Jurisdiction		
Variable	Rating	Motivation
<b>Is Botswana an international or regional trading hub/transshipment hub/ major trading hub</b>	<b>none and the trend is constant</b> both domestic and cross-border threat	Whilst Botswana has ambitions to be a finance and trade hub through pronouncements made by the political leadership and the setting up of institutions like Botswana Investment and Trade Centre (BITC). Analysis indicates that Botswana does not function as an international or regional financial hub, nor a major transshipment hub and neither a major trading jurisdiction. It is against this background that is unlikely to be abused for terrorist financing flows.
Strategic goods and services		
Variable	Rating	Motivation
<b>Does Government/businesses/NPO provide or transfer strategic goods or services to areas with active terrorist threat</b>	<b>none and the trend is constant</b>	Botswana does not export financial aid, military equipment, strategic goods, and other economic resources to areas with an active terrorist threat. This variable is therefore rated none and the trend is constant, for both domestic and cross border threat.

#### Sectoral TF Risk

239. The significance of the TF risk borne by the various sectors in Botswana was assessed to fully understand the national TF risk. In this regard, banking, MVTs, DNFBPs and other FIs were assessed.
240. The sector TF risk was assessed as a product of two main components: threat and vulnerability. In relation to threats, the assessment considered the applicability of TF typologies, suitability of the sector to TF, geographic, demographic and other threat factors specific to the sector including their cross-border elements. For vulnerability, inherent vulnerabilities and CFT controls were considered. As many of the assessment variables and criteria in ML and TF risk assessment are similar, the assessment synergized and built on the assessment done for ML.

#### Banking

241. The banking sector was assessed to have a **Low** TF residual risk. Of note, was the banking sector's exposure arising from cross border business activities in areas with active terrorist such as South Africa and Mozambique. The high use of cash in the sector was noted however existing CFT controls were found to adequately mitigate the risk posed by the use of cash.

#### MVTs

242. The assessment noted high levels of use of cash and use of agents in the sector, moderate transfer of funds to high-risk jurisdictions such as South Africa, the suitability of the sector being exploited by transit sympathizers and that most of the transactions

for the sector were destined outside Botswana, the residual TF risk for the sector was determined to be **Low**

243. The assessment determined suspicious activity monitoring and reporting, compliance functions and CFT knowledge and awareness among the staff as priority areas.

#### Other FIs and DNFBPs

244. Securities, insurance and other FIs were grouped together for the assessment. The residual TF risk for the combined sector was judged to be **Very Low**. With respect to DNFBPs the residual TF risk was determined to also be **Very Low**.

245. Consequently, the TF risk posed by IS sleeper cells, transit sympathizers, terrorist organizations in active terrorism areas including Mozambique and extremist such as white supremacist in South Africa, were found to be more likely to abuse MVTS and banking more than other sectors.

#### National TF vulnerability

246. The overall national TF vulnerability was assessed to be low. This step assesses the level of national TF vulnerability, which stems from the gaps and weaknesses in the national measures for the prevention and detection of TF and the enforcement of counter-financing of terrorism (CFT). Vulnerabilities may include weaknesses in dedicated CFT measures, the overarching AML/CFT framework, or contextual features of a jurisdiction that may be exploited for TF, such as suboptimal border controls or a large informal economy.

247. A total of 23 input variables were assessed in order to determine the outcomes for 13 intermediary variables and the overall national vulnerability in four categories of vulnerability to internal TF, incoming TF, outgoing TF and transit TF.

#### Quality of CFT Policy and Strategy

248. Following the 2017 national risk assessment an AML/CFT Strategy was developed. However, it was observed that not all relevant sectors were included in the risk assessment including NPOs. Similarly, the dissemination of the National AML/CFT Strategy was not widely circulated with key AML/CFT stakeholders. Further, it was observed that the strategy was not adequately monitored for implementation. **Rating: Medium-High**

#### Effectiveness of TF Crime Definition

249. The Counter-Terrorism Act criminalises and specifies penalties for terrorism and terrorist financing. The penalties apply to both legal and natural persons and are dissuasive and proportionate. **Rating: Excellent**

## Effectiveness of TF Customs & Border Controls

250. The overall rating for quality of TF customs and border controls is **Medium**. Resource constraints on customs authority (limited human deployment, screening equipment including currency sniffer dogs) negatively affects the effectiveness to detect and deter any unauthorized physical cross-border transportation of cash, bearer negotiable instruments (BNI), and precious metals and stones (PMS). Botswana has comprehensive laws relating to trade on strategic goods and criminalises the development, acquisition, trafficking, or use of WMDs; their means of delivery; and related materials, equipment, and technology.
251. Limited detectors and inadequate human capacity affect Botswana's ability to effectively detect unauthorized or illegal trade and transfer of strategic goods. The responsible authority, CBRNWA, is still at an early stage to identify strategic goods and materials. In addition, a comprehensive list of dual use goods is not available. Botswana has long porous borders with limited natural barriers and hence compromised immigration controls.

## Quality of TF Intelligence Gathering and Processing

252. The overall rating for the quality of TF intelligence gathering and processing is **medium**. This variable assesses the quality of the Financial Intelligence Unit (FIU) and other intelligence agencies for TF intelligence gathering and processing. FIA has the mandate under the FI Act to collect, store, analyse and disseminate intelligence reports as well as threshold transaction reports effectively and is a member of EGMONT Group. However, there are limited human resources and requisite analytical tools.
253. The Directorate of Intelligence and Security (DIS) is empowered to gather intelligence on national security including terrorism and terrorism financing. The Fusion Division established under the Counter Terrorism Act is mandated to receive, analyse and disseminate TF and terrorism information to relevant law enforcement agencies. The amendment of the Counter Terrorism Act in 2022 redesignated the fusion agency as a Division under the Directorate of Intelligence and Security affecting its ability to independently receive, analyze and disseminate TF information. Similarly, some of the agencies required by law to second staff to the fusion agency are not doing so, hence limiting its capacity.

## Quality of TF investigation

254. The overall rating for quality of TF investigations is medium. This variable considers Capacity/Resources for financial crime investigations and integrity/independence of investigators amongst others.

## Capacity & resources for financial crime investigations

255. The Counter Terrorism CT Act empowers Botswana Police Service (BPS) to investigate terrorism, terrorist financing and other financial crimes. BPS has established a specialized AML/CFT unit however it is inadequately staffed. The AML/CFT Unit of BPS

is based in Gaborone. Given the threat of transit sympathizers, the centralisation of CTF investigator skills and expertise in Gaborone affects its capacity to adequately detect TF cases and assets at borders. There are no established Standard Operating Procedures (SOP) on identifying and tracing assets for TF which could compromise detection, disruption and investigation of TF.

#### Integrity and Independence of Financial Crime Investigators

256. There are measures to safeguard the integrity of financial investigators. However, there was a failure by existing institutional safeguards to adequately deter and react to a breach on one matter. The matter culminated with a Consent Order with government undertaking to publicly apologise for the integrity lapse.<sup>22</sup>

#### Quality of TF Prosecution

257. The overall rating for quality of TF prosecutors is medium low. This variable considers capacity/resources for prosecutors and the integrity/independence of TF prosecution. The DPP is not adequately structured as it falls within the AGC and lacks operational independence including funding and staffing.

#### Integrity and Independence of Financial Crime Prosecutors

258. DPP as the department mandated to prosecute cases in Botswana does so without fear and favour. It deals with the prosecution of all criminal matters including ML/TF cases. However, the High Court found the integrity of a prosecutor in one particular case to be lacking.
259. International cooperation through MoUs in relation to mutual legal assistance, through the Ministry of International Relations and the DPP. It is however observed that in a number of cases there was delay in response for information and the extradition process

#### Quality of TF adjudication

260. The overall rating for quality of TF adjudication is medium low on account of the cascading deficiencies noted at variable for quality of intelligence gathering, TF investigations and prosecutions above. The Judiciary in Botswana is capacitated and informed to deal with TF cases. The lack of Judicial Training institution and research assistants contributes to inadequate training in specialized financial crimes and delayed conclusion of matters. The Judicial officers in Botswana are independent and impartial in presiding over cases and there are no reported cases of integrity lapses involving the judicial officers.

#### Availability and Effectiveness of TF Asset Forfeiture and Confiscation

261. The overall rating for Availability and Effectiveness of TF Asset Forfeiture and Confiscation is rated **Excellent**. The PICA comprehensively enables competent

---

<sup>22</sup> Motsepe v AG.

authorities to seize, freeze and forfeit proceeds and instrumentalities of TF. It has been established that Competent Authorities are able to seize, freeze and forfeit proceeds and instrumentalities of crime.

#### Quality of Targeted Financial Sanction (TFS)

262. The overall rating for quality of TFS is **Medium**. This variable assesses (a) comprehensiveness of TFS legislation, procedures and mechanisms, (b) access to reliable information/data/records, (c) effectiveness of domestic cooperation and (d) effectiveness of TFS implementation.
263. The Financial Intelligence Regulations of 2022 provides for the implementation of United Nations Security Council Resolutions and successor Resolutions; however, it has been determined that the regulations are not covered under the primary law (FI Act).
264. The Act establishes the NCCFI which is mandated to domesticate United Nations Security Council (UNSC) Resolution 1267, whilst the Minister of Finance has the responsibility to propose persons and organisations that meet the designation criteria to the UN in accordance with UNSC Resolutions 1373. All natural and legal persons within the country are required by the Financial Intelligence Regulations (Implementation of United Nations Security Council Resolutions) to freeze, without delay and without prior notice, or to make available, the funds or other assets of designated persons and entities.
265. Upon receipt of the UNSC list the FIA disseminates to specified parties /accountable institutions whilst CTFD is responsible for the Competent authorities. The Banking and the MVTS sectors have automated monitoring systems which has demonstrated a high level of effectiveness. Sectors that rely on manual screening have demonstrated a moderate level of effectiveness.

#### Access to Reliable Information/Data/Records

266. Botswana is found to have close to excellent access to reliable information/data/records as it has a highly formalized economy (the informal economy contributes an estimate 5.3% to the GDP<sup>23</sup>) and good quality of CDD framework (reliable ID infrastructure, independence information sources and access to BO information).

#### Controls on Provision of Strategic Equipment, Goods & Services to Conflict Zones

267. Variables deemed inapplicable as the national TF threat assessment did not find any provision of such strategic goods and services to risky jurisdictions. **Rating: Not applicable**

---

<sup>23</sup> Botswana National Informal Sector Recovery Plan, page 12.

Table 28: Overall Terrorist Financing Risk Rating

<b>CATEGORY</b>	<b>TF THREAT</b>	<b>VULNERABILITY TO TF</b>	<b>TF RISK LEVEL</b>
<b>Domestic TF Risk</b>	0,0	0,53	Low
<b>Outgoing TF Risk</b>	0,02	0,57	Low
<b>Incoming TF Risk</b>	0,10	0,57	Low
<b>Transit TF Risk</b>	0,00	0,57	Low

## CHAPTER 6: NON-PROFIT ORGANISATIONS RISK ASSESSMENT

268. FATF defines the term NPO to cover “a legal person or arrangement or organization that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of “good works.”
269. Global typologies have highlighted that certain features and operational characteristics of non-profit organizations (NPOs) can make them vulnerable to terrorist financing (TF) abuse. In response, the FATF, under Recommendation 8, calls on countries to identify the nature and extent of TF risks to their NPO sectors and to implement targeted, proportionate, and risk-based measures to mitigate those risks.
270. The NPO risk assessment aimed to:
- Identify all NPOs in the country that meet the FATF definition;
  - Evaluate the level of TF risk exposure among the identified FATF-defined NPOs;
  - Examine and assess the existing national and sectoral controls designed to mitigate these risks; and
  - Provide recommendations for ongoing and adaptive measures to address emerging TF threats.
271. There are four legal types of NPOs in Botswana, namely, Societies, Trusts, Companies Limited by Guarantee (CLGs) and statutory. These entities fall under the supervision of the Master of the High Court, Companies and Intellectual Authority and the Registrar of Societies as the supervisory authorities for AML/CFT compliance.
272. There are 11 657 registered NPOs in Botswana. This comprises of 9 973 societies under ROS, 259 CLGs under CIPA, 1 424 trust under Master and one statutory **NPOs** registered through the Red Cross Act.
273. The NRA identified 400 FATF-defined NPOs as represented per category in Table 2.

Table 29: Classification of FATF NPOS

CLASSIFICATION TYPE	SOCIETIES	CLGs	TRUSTS	STATUT ORY NPO	Total
Charitable Organizations	21	80	6	1	108
Community Based Organizations	18	17	177	0	212
Religious Organizations	41	0	0	0	41
Cultural Organizations	0	0	2	0	2
Educational Organisations	0	37	0	0	37
<b>Total</b>	<b>80</b>	<b>134</b>	<b>185</b>	<b>1</b>	<b>400</b>

## Main Threats Facing the Sector

274. Assessing the inherent TF risk posed to NPOs by terrorist and terrorist organisations requires an understanding of the environment that NPOs operate in, the vulnerabilities present in the sector, how terrorist entities seek to exploit these vulnerabilities, and how threats to the sector have been detected and managed.
275. The analysis of enforcement data revealed that there were no STRs, intelligence reports, investigations, prosecutions and convictions involving the abuse of NPOs for TF. Consequently, the variable on evidence of TF abuse for NPOs was rated DOES NOT EXIST.
276. In determining TF threats to NPOs, two key factors were assessed: the presence of known typologies involving NPO misuse and the organisation's proximity to active terrorism threats.
277. Common TF threat typologies relevant to assessing NPO vulnerability included:
- Diversion of funds,
  - Affiliation with a terrorist organization,
  - Support for recruitment efforts,
  - Abuse of programming, and
  - False representation/sham NPOs.

### Diversions of funds

278. This is a method where funds raised by NPOs for humanitarian programmes (disaster relief, humanitarian relief, cultural centres, relief of poverty, advancement of education, advancement of religion) are diverted to support terrorism activities. Based on enforcement data, there is no evidence to support that NPOs (inclusive of employees, volunteers, or other individuals acting in an official capacity as representative of an NPO) in Botswana have diverted or are diverting funds to terrorism, a known or suspected terrorist entity, terrorist individual or supporter of terrorism. Accordingly, this typology is not present in Botswana.

### Affiliation with a terrorist organization

279. This typology refers to NPOs or their officials, either knowingly or unknowingly, being affiliated to terrorist entities. In this regard, NPOs are misused for various purposes, including providing logistical support to the terrorist entities. Based on the enforcement data, there is no evidence that NPOs in Botswana, their employees, volunteers, or any of their official representatives maintain operational ties with known or suspected terrorist entities, individuals, or supporters. Where NPOs engage in cross-border activities, they are primarily related to affiliations by religious organisations to the parent body in jurisdictions such as: South Africa, United Kingdom and Nigeria. Although Nigeria is considered a high-risk jurisdiction<sup>24</sup> to TF, there is no evidence of financial transactions that would suggest TF. Consequently, the typology was found not to exist.

---

<sup>24</sup> Institute of Economics and Peace Global Terrorism Index 2025

### Support for recruitment efforts

280. This typology refers to where NPOs provide support to recruitment efforts by terrorist entities. There is no evidence that Botswana's NPOs are used to create an environment that supports or promotes terrorism recruitment-related activities. Hence, the typology is not applicable.

### Abuse of programming

281. This entails where programs meant to support legitimate NPO purposes are manipulated at the point of delivery to support terrorism. Based on enforcement data there is no evidence that NPOs in Botswana are manipulated to support terrorism, a known or suspected terrorist entity, terrorist individual or supporter of terrorism. The assessment has revealed that NPOs deliver their programs locally where it has been established that there is no active terrorism or evidence of TF in Botswana. Consequently, this typology was also found not to be applicable to Botswana context.

### False representation /Sham NPOs.

282. This is a situation whereby an NPO that, under the guise of charitable activity, raises funds or carries out other activities in support of terrorism, a known or suspected terrorist entity, terrorist individual, or supporter of terrorism. There is no evidence of false representation/sham NPOs in Botswana. Accordingly, this variable is determined not to be applicable.

### Proximity to active terrorist threat

283. In assessing this variable, three parameters were interrogated: collection of funds, transfer of funds and expenditure of funds (disbursing funds or delivery of programs) in areas where or near:

- an established presence of terrorism,
- conflict in which there is an active terrorist threat or from collecting funds or operating,
- a known or suspected terrorist entity or terrorist individual,
- a population that is actively targeted by a terrorist movement for support and cover, or
- entities (including financial institutions) and individuals known to be supportive of or sympathetic toward terrorist entities, terrorist individuals, terrorist ideology, or radical beliefs.

284. The reported presence of Al-Shabaab and the Islamic State terrorist cells in South Africa and presence of ISCAP/ISIS, ASWJ in Mozambique and ISIS in the Democratic Republic of Congo (DRC) was noted as having proximity to Botswana. Notwithstanding the above, there was no evidence to suggest that NPOs in Botswana collected, transferred or expend funds from terrorists or terrorist groups or these jurisdictions. Further, none of the NPOs have shown financial control connections to high-risk jurisdictions and no

evidence of funds were disbursed to terrorist groups or to deliver programs to areas with active terrorism.

#### Overall TF threat

285. The above noted assessment was applied across all categories of NPOs in Botswana. The assessment determined that there were no incidents related to the variables of typologies and proximity to active terrorist areas of South Africa, Mozambique and DRC. Consequently, the overall TF threat per category of NPOs was determined as **DOES NOT EXIST**

#### Sector Vulnerability

286. To assess the inherent vulnerabilities of the FATF NPOs in Botswana, three variables were considered; NPO Profile, Operational Features and Methods to Transfer Funds.

##### NPO Profile

287. For NPO profile, the tool considers NPO size, activity, offshore/complex structures, level of accountability, level of verifiability of fundraising methods, level of cash transfers and valuable in kind goods.

##### NPO Size

288. Cultural, Community Based Organisations and Religious were all found to be **small** in relation to the value of income, (they operated with an average income less than P15 million per year). Charitable and educational organisations were determined to be medium. The rating scale where P0- P15m represented small, P15.1-P30m represented medium and P30.1 million and above representing large was adopted for the assessment.

##### Activity Type

289. NPOs in Botswana were found to be mostly engages more in service activities than expressive activities. It was observed that 78 percent of NPOs engage in service activities, 10 percent engage in expressive activities while 12 percent engage in both expressive and service.

##### Offshore/ Complex Control Structures

290. A rating of "**does not have (does not exist)**" was given to foreign controls of complex control structure for the NPOs. While some of the NPOs were found to have international links, it was established that the links were not related to TF. It was determined that some charitable as well as some religious NPOs were founded on the principle of universality meaning that they operate internationally but guided by local frameworks.

## Level of Accountability Required by Funding Sources

291. The assessment found the level of accountability for NPOs to be **high** across all categories. This is because accountability mechanisms such as audited reports, due diligence and oversight were constant.

## Level of Verifiability of Fundraising Methods

292. From the data collected, community-based organisations and cultural organisations were rated '**medium**' because NPOs in these categories have an equal mix of formal and informal methods of fundraising. Charitable, religious and educational NPOs were rated '**high**' because of heavy reliance on formal fundraising methods with electronic transactions being the mostly used.

## Level of Cash Transfers or Valuable in-Kind Goods

293. The assessment revealed that all NPOs under review had little appetite for use of cash and valuable in-kind goods. The finding is that they predominantly used electronic transfer. The rating of this vulnerability across the different categories was determined as **low**.

Table 30: Summary of NPO Profile

ININHERENT RISK RATING						
VARIABLE	INPUT VARIABLE	Charitable	Community Based	Cultural	Religious	Educational
<b>NPO Profile</b>	Activity Type	Service	service	service	service	service
	Offshore complex control structure	low	Does not exist	Does not exist	Does not exist	Does not exist
	Level of accountability required by funding sources	High	High	High	High	low
	Level of verifiability of fund-raising methods	High	Medium	medium	High	high
	Level of cash transfers, valuable in-kind goods	low	low	low	low	high

## Operational Features

294. NPOs were assessed against the following operational features.

### Level of Risk Appetite

295. All NPOs except for Educational were rated '**low**' because they had adequate control measures for accepting funding or valuable in-kind goods but in some instances, they can lower their control measures. Education was rated **High**.

### Complexity/ Length of Operational Chains

296. Due to their nature of having fewer players in the operational chain, all NPOs were **found not to have** (does not exist) long and complex operational chains.

### Reliance on Transitory or Informal Workforce

297. Charitable, CBOs and cultural were found to have low reliance on transitory or informal work force, while religious organisations were found to have a high reliance on transitory or informal workforce. Educational organisations were found not to rely on transitory or informal workforce.

### Level of Professionalism

298. All NPOs were all rated '**high**'. NPOs were found to have governance manuals that consisted of ethics and code of conduct, financial management policies and condition of service. The table below shows a summary of Operational features rating.

Table 31: summary of Operational Features Rating

VARIABLE	Input variable	INHERENT RISK RATING				
		Charitable	CBO	Cultural	Religious	Educational
Operational Features	Level of risk appetite	low	Low	Low	low	High
	Complexity level of operational chains	Does not exist	Does not exist	Does not exist	Does not exist	Does Not Exist
	Reliance on transitory or informal workforce	low	low	low	High	Does not exist
	Level Of Professionalism	High	high	high	High	high

## Methods of Fund Transfer

299. This variable is assessed on the extent of which NPOs use cash, virtual currency and use of informal money transfers. This variable is rated medium. The following factors were used to establish methods used by NPOs to transfer funds.

### Use of cash

300. The use of cash in all NPOs was rated low. The main source of funding for religion tithing, membership/subscription fees mostly collected through cash transactions. However, these NPOs deposit monies collected into bank accounts and disburse through the banking system.

### Use of virtual currency

301. No NPO used any virtual currency for the period under review. The variable is rated does not exist.

### Use of informal money transfers

302. No NPO used informal money transfer systems for the period under review. The variable is rated does not exist.

### Overall inherent vulnerability

303. The inherent TF vulnerability for all NPOs was found to be **low**.

## CFT Controls & Mitigation

304. Societies, Trusts, CLGs and the statutory NPOs were all assessed to be at low risk of TF abuse hence the quality of mitigating measures were not assessed. However, controls in place include filing annual returns, legal obligations of TFS and requirement to transact through the banking sector.

### Effectiveness of Legislation

305. While the world bank tool does not prescribe the assessment of adequacy of laws. The adequacy of laws governing NPOs were briefly assessed and the following inadequacies were identified;

- (a) Supervisory Authorities are not legally empowered to promptly exchange information with LEAs in order to facilitate preventive or investigative action.
- (b) The process of registration of trusts and information management is manual and therefore information retrieval, processing and analysis becomes difficult, making the whole process inefficient. Promptness of information sharing therefore becomes close to impossible.
- (c) There is no legal requirement for CLGs to submit annual returns for purposes of monitoring financial and operational activities.

## Residual Risk Rating

306. TF threat and vulnerability were assessed to be low, therefore, the overall TF risk was rated as low meaning that there is no evidence of terrorist financing abuse of NPOs in Botswana.

## CHAPTER 7: LEGAL PERSONS, LEGAL ARRANGEMENTS AND BENEFICIAL OWNERSHIP RELATED RISKS

307. Legal structures<sup>26</sup> in Botswana are created either through statutory provisions or common law. Those created through statutory provisions are required to comply with the specific laws including the requirement to register and disclose ownership details to the relevant registry body. There are four registries responsible for registering legal structures in Botswana being;

- Companies and Intellectual Property Authority (CIPA) – registration of companies
- Register of Societies (ROS) – registration of societies
- Department for Co-operatives Development (DCD) – registration of cooperative societies, and
- the Master of the High Court – registration of trusts

308. Legal persons also include foundations and foreign companies identified through banks. On the other hand, common law legal arrangements consist of partnerships and trusts. There is no legal requirement for registration of partnerships, therefore, this lapse pose an inherent risk for abuse of money laundering as they have no regulatory authority to monitor their dealing.

309. Exposure to foreign ownership also existed in different types of structures such as private limited companies, public limited companies, external companies, trusts and partnerships. Public Limited companies had the highest level of foreign ownership.

Table 32: Total number of all categories of legal structures and legal arrangements operating in Botswana

Registry Body & the Law	Statutory Legal Structures	Registration requirement	Total number
CIPA - Companies	Private limited companies	Yes	129835
	Public Companies		185
	Companies Limited by Guarantee		259
	Close companies		140
	External companies		137
	Foreign companies		1
N/A	Foreign companies (Identified through banks)	No	88
ROS Societies	Societies	Yes	10145
DCD - Cooperatives	Financial Cooperatives	Yes	101
	Non-Financial Cooperatives		292
None	Foundations (Identified through banks)	No	69
<b>Total</b>			<b>141 252</b>
Master	Trusts	Yes	1424
None	Partnerships (identified through banks)	No	547
TOTAL			1971

310. The legal structures sector plays a crucial role in the integrity and transparency of the financial system but also present vulnerabilities for misuse by criminals seeking to conceal the true origin and ownership of illicit proceeds. As a result, legal structures can be instrumentalised as vehicles for laundering proceeds from a wide range of criminal conduct.
311. The legal structures sector plays a critical role in supporting the integrity and transparency of the financial system. However, it also presents vulnerabilities that can be exploited by criminals seeking to obscure the true origin and ownership of illicit funds. Consequently, legal structures are often instrumentalised as vehicles for laundering proceeds derived from a broad range of criminal activities.
312. This risk assessment aimed to understand the nature and extent of these risks by analysing the ML/TF threats posed by legal structures based on enforcement data, threat perceptions and open sources.
313. The enforcement data provides evidence of actual misuse of legal structures; perceptions and open-source information, offers insight into emerging risks and broader context where statistical data is limited; and public and expert opinion, contributes practical knowledge from professionals who directly observe vulnerabilities in the sector.

*ML abuse based on enforcement data, perceptions & open sources*

Enforcement Data	perceptions & open sources	Public Experts Opinion
Medium	Low	Medium

#### Enforcement Data

314. During the review period, there was no enforcement data for TF, however, there were 14 SARs/STRs related to ML linked to legal structures. Following their analysis, FIA disseminated nine intelligence reports to LEA. According to the FIA, the types of legal structures that have been abused for money laundering purposes were private limited companies. Furthermore, the FIA had received 6 international requests for information on private limited companies including BO information.
315. LEAs have conducted 22 criminal investigations where legal structures were suspected to be abused by criminals for money laundering. Of these three are pending before courts, 12 are still under investigation with six awaiting MLA. Five cases are pending assessment of evidence by the DPP whilst one case has been closed for insufficient evidence. One case involving a PEP was completed before court resulting in a conviction. The Politically Exposed Persons (PEP) had used a legal person to receive proceeds of crime but the company involved was acquitted of the money laundering and corruption charges. A criminal forfeiture order of P640, 000.00 was granted against the PEP.

316. The enforcement data rating considered the **extent, nature and actors** involved. The extent of the amount of the proceeds generated was found to be considerably high with sophisticated methods applied to launder the money. The actors were well organised with technology used in some cases to transfer money across the borders. Therefore, this led to the medium risk for rating of the enforcement data.

#### Perceptions and open

317. With regards to the perceptions and information held by open sources, there was no local information that existed whereas limited international sources existed. They mainly talked to the ranking of Botswana in corruption cases compared to other countries in the region. Due to this limited information, perceptions by open sources was considered to be low.

#### Public expert opinion

318. The sector risk assessments that exist for legal persons were considered as part of the public expert opinion. All of them considered risks associated with legal persons as medium.

319. The overall ML threat for legal structures was assessed as **medium**, driven primarily by the medium ratings assigned to enforcement data and public expert opinion, which outweighed the lower threat rating derived from perceptions and open-source information.

#### Sector Vulnerability

320. The vulnerability of the sector was assessed using a set of key variables designed to identify structural weaknesses and exposure to misuse. These variables included the scale and size of the sector, its cross-border risk exposure, and the ease, speed, and cost of forming or registering entities. The assessment also considered the sector's attractiveness to non-residents, the quality and accessibility of both basic and beneficial ownership information, the sector's incidence in analysed ML/TF cases, and the existence of known ML/TF typologies linked to its activities. Together, these factors provided a comprehensive understanding of the sector's susceptibility to money laundering

Table 33: Detailed assessment of the sector vulnerability

Legal structure type	ML/TF Risk Assessment rating		Intermediate Variables and Score							
			Scale	Cross Border Risk Exposure	Ease, speed & costs of forming	Attractiveness for non-resident use	Quality & Accessibility of Basic Info	Quality & Accessibility of BO Info	Incidence in analysed ML/TF cases	Existence of ML/TF Typology
Private limited companies	ML	Medium	High	Low	High	Low	Low	Low	High	Medium
	TF	Low	High	Low	Low	Low	Low	Low	Low	Low
Public Companies	ML	Low	High	Low	Medium	Low	Low	Low	Medium	Low
	TF	Low	High	Low	Low	Low	Low	Low	Low	Low
Companies Limited by Guarantee	ML	Low	Low	Low	Low	Low	Low	Low	Low	Low
Close companies	ML	Low	Low	Low	High	Low	Low	Low	Low	Low
	TF	Low	Low	Low	Low	Low	Low	Low	Low	Low
External companies	ML	Low	Low	High	Low	Low	Low	Low	Low	Low
	TF	Low	Medium	Low	Low	Low	Low	Low	Low	Low
Societies	ML	Low	Medium	Low	Medium	Low	Low	Low	Low	Low
	TF	Low	Medium	Low	Low	Low	Low	Medium	Low	Low
Financial Cooperatives	ML	Low	Medium	Low	medium	Low	Medium	Medium	Low	Low
	TF	Low	Medium	Low	Low	Low	Low	Medium	Low	Low
Registered Trusts	ML	Low	Low	Low	High	Medium	Low	Medium	Low	Low
	TF	Low	Low	Low	Low	Low	Low	Medium	Low	Low
Partnerships	ML	Medium	Medium	High	High	Low	Medium	Medium	Low	Low
	TF	Low	Medium	Low	Low	Low	Medium	Medium	Low	Low

321. The table indicates that, overall, money laundering risk for private limited companies and partnerships is rated as medium, whereas for all other legal structures it is rated low. In contrast, terrorist financing risk is rated low across all legal structures. These results show that the country is moderately vulnerable to money laundering risks associated with private limited companies and partnerships. Accordingly, resources and supervisory attention should prioritise these legal structures.

322. Notwithstanding the above, several intermediate variables were assessed as high or medium and therefore require ongoing monitoring:

#### Scale of Activity

323. The intermediate variable on "scale" assesses (i) the total number of registered legal structures and (ii) the value of pass-through financial flows/assets.

- Both components were rated **high** for private limited companies.

- They were rated **medium** for external companies, societies, financial cooperatives, and partnerships.

#### Cross-Border Risk Exposure

324. Cross-border exposure was found to be significant for:

- External companies, which originate in foreign jurisdictions and register in Botswana using incorporation documents. Their dual presence increases their cross-border ML exposure which has been rated high.
- Partnerships, which are unregistered and typically identified through banking activity, also face high cross-border ML risk.

#### Ease, Speed and Cost of Formation/Registration

325. This variable was rated:

- High for private limited companies, close companies, and trusts.
- Followed by public limited companies, societies, and financial cooperatives. High ease, speed, and low cost of formation can increase vulnerability if key checks necessary for mitigating ML/TF risks are weakened or bypassed.

#### Attractiveness for Non-Resident Use

326. This factor was rated medium for trusts, largely due to the high proportion (32.54%) of trusts with foreign natural and juristic persons.

#### Quality and Accessibility of Beneficial Ownership (BO) Information

327. Risk related to BO information was rated medium for societies, financial cooperatives, trusts, and partnerships. TF risk was also rated medium for financial cooperatives and partnerships. These ratings highlight the need to improve the completeness, quality, and accessibility of BO information for these entities.

#### Incidence in Analysed ML Cases

328. The incidence of ML cases was high for private limited companies and medium for public companies. ML typologies involving private limited companies were rated medium. These findings demonstrate that both private and public limited companies remain vulnerable to ML risks, as evidenced by case analyses and typology trends.

329. A typology analysis identified several typologies of money laundering abuse across domestic and foreign legal structures. The most prevalent of these typologies included the following which makes legal persons and arrangements vulnerable;

- Multi-jurisdiction Splitting - splitting of company formation, asset ownership/administration, location of professional intermediaries, and location of bank accounts across different countries in order to evade regulations.

- Foreign ownership/control - ownership/control of domestic legal structures by foreign-registered legal structures.

330. Use of nominee directors and shareholders exists in the formation and management of legal persons. This creates a significant vulnerability, as nominees can be used to conceal the individuals who exercise actual control over companies. Such arrangements enable the manipulation of legal structures and hinder the identification of true beneficial owners.

331. The following case studies illustrate the practical application of these typologies, showcasing how they were implemented and adapted in different contexts.

**Case 1-typologies identified: multi-jurisdiction splitting, foreign ownership & Anomalous complex ownership/control**

A foreign national registered and operated a micro-lending business in Botswana, which functioned as a subsidiary of a Frankfurt-listed company with affiliated entities in Zimbabwe, Zambia, Eswatini, South Africa, and Mauritius. The Botswana subsidiary subsequently listed a bond on the Botswana Stock Exchange (BSE) to raise capital for the expansion of its micro-lending operations. Following the successful capital raise, the director of the Botswana entity misappropriated a substantial portion of the investor funds to related companies based in Mauritius and South Africa. A total of P258,882,979 was laundered.

**Case 2- typologies identified: multi-jurisdiction splitting, foreign ownership, nominee directors/nominee shareholders/front men**

A company owned by Chinese nationals and purportedly engaged in the import and export of seafood opened a bank account with a local financial institution. Shortly after account activation, the account began receiving high-value cash deposits, which were promptly followed by transfers to China. This transaction pattern persisted over time, with no observable business-related expenditures apart from routine bank charges. Within six months of opening the account, approximately BWP18.9 million in cash deposits and BWP 5 million in electronic transfers were received. Notably, the electronic transfer originated from a company previously investigated for receiving proceeds linked to a pyramid scheme. Of the total funds received, approximately BWP22 million was subsequently transferred to China. The conductor making the deposits was not linked to the ownership/management of the company.

**Case 3 typologies identified: multi-jurisdiction splitting & foreign ownership**

Company A was registered by an employee of Company B, with the Managing Director (MD) of Company B appointed as the sole signatory to Company A's bank account. At the time, Company B was engaged as a bond advisor for a foreign entity seeking to list a bond on the Botswana Stock Exchange (BSE). During the period surrounding the bond listing, Company B began transferring funds into Company A's account. These funds were subsequently transferred to a savings account belonging to an individual known to the MD of Company B, from which large cash withdrawals were made. The use of cash in this context raises red flags, as it lacks clear economic justification and is inconsistent with the known business profile of Company B. This pattern of behavior suggests a potential attempt to obscure the financial trail. Notably, both the MD and the ultimate beneficial owner of Company B have a history of financial misconduct. The owner has previously been deemed not fit and proper in Zambia and is currently under investigation in Eswatini.

The company is 100% owned by a Motswana. The signatory to the account is another Motswana, who is neither shareholder or Director. The entity has a transactional relationship with several other entities within Southern Africa that have been linked to under hand dealings that caused investors to lose their funds, such as in Eswatini, South Africa, Malawi.

**Case 4 typologies identified: foreign ownership & nominee director's/nominee shareholder's/front men**

Chinese nationals approached various Botswana to set up companies. The Chinese nationals would then request the account holders to handover account login credential and would control the bank accounts of these various Botswana owned companies and received funds from a pyramid scheme before laundering the funds abroad to China.

**Case 5- typologies identified: Use of large professional firms**

Fund Managers connived with some board members to divert public funds for personal gain. Some of the funds were transferred to large professional firms under the color of payment of fees.

332. Based on the vulnerabilities and typologies discussed above, the overall vulnerability for legal structures was found to be **medium**.

**AML Controls & Mitigation**

333. AML controls and mitigations are used to assist in reducing and or minimizing the effects of risks associated with the threats and vulnerabilities of this sector. The following are key AML controls and mitigations identified during the stated review period.

- BO information is accessible through various sources mainly through the CIPA Online Business Registration System (OBRS) for companies and upon request for other registries.
- Routine verification of identification is done through interfacing civil and national registration databases for CIPA and through certification of copies of ID/passports by commissioner of oaths for other registries. Further, routine verification is done to ensure the existence of those registering legal persons and to deter the existence of ghost companies.

- A legal framework for sanctions for non-compliance with disclosure requirements for BO exists.
- Mechanisms for exchange of information amongst domestic competent authorities occurs without impediments
- Botswana is a member of the Egmont Group and therefore able to informally exchange BO information informally prior to mutual legal assistance processes.
- The FIs are obligated to comply with the FI Act when onboarding or concluding a transaction with a customer. This provides mitigation for challenges associated with the use of partnerships.

#### Residual Risk Rating

334. The ML risk for private limited companies and partnerships was assessed as Medium relative to other legal structures. This rating reflects existing statistics and typologies showing moderate ML exposure among private limited companies, as well as the lack of mechanisms to monitor the quality of information for partnerships. The final rating also takes into account the effectiveness of controls in place to mitigate these threats.
335. Therefore, the overall ML threat and vulnerability facing legal structures were both rated **medium**.

## **CHAPTER 8: VIRTUAL ASSETS AND VIRTUAL ASSETS SERVICE PROVIDERS RISK ASSESSMENT**

336. This section presents a structured and summarized version of Botswana's ML/TF risk assessment of Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs). With the global rise in use of cryptocurrencies, this assessment evaluates the emerging threats and vulnerabilities specific to Botswana's context. It draws from data collected through surveys, stakeholder engagements, regulatory reviews, and international best practices. The goal is to inform a risk-based approach to supervision, mitigation, and enforcement in the VA/VASP space.
337. Botswana enacted the Virtual Assets Act in 2022, revised in 2025, empowering NBFIRA to supervise and license VASPs. Under Section 2 of the Virtual Assets Act, 2025 Virtual Asset means a digital representation of value that (a) may be digitally traded or transferred, and may be used for payment or investment purposes, or (b) is distributed through a distributed ledger technology where value is embedded or in which there is a contractual right of use, and includes virtual tokens; and excludes (i) a digital representation of legal tender as provided for under the Bank of Botswana Act, and (ii) securities and other financial assets that are regulated under the Securities Act.
338. Virtual asset service provider (VASP) means a person who (a) under an agreement, as part of a business, undertakes a virtual asset service or any of the following activities for or on behalf of another person— (i) the exchange between virtual assets and fiat currencies, (ii) the exchange between one or more forms of virtual assets, (iii) the transfer of virtual assets, (iv) the safekeeping or administration of virtual assets or instruments enabling control over virtual assets, and (v) the participation in and provision of financial services related to an issuer's offer or sale of a virtual asset; or (b) is a dealer or is willing to deal, on own account, by buying and selling virtual assets at prices set by that person, and includes a— (i) market maker or liquidity provider, (ii) system that provides virtual liquidity, allowing traders to buy and sell derivatives on the blockchain, or (iii) virtually automated market maker. These definitions align closely with FATF standards.
339. VASPs have been designated as non-bank financial institutions under the Financial Intelligence Act, making them subject to full AML/CFT requirements. As of 2024, there a total of six VASPs had been licensed by the NBFIRA to operate in Botswana. However, only two, Yellow Card and Express Minds, had commenced operations. Yellow Card dominated the market accounting for more than 85% of the market share.
340. Yellow Card Botswana is a regional and continental virtual asset exchange with a presence across Africa, offering services that includes the buying, selling, transfer and safekeeping of virtual assets. In contrast, Express Minds is a smaller, domestic operator primarily engaged virtual assets ATM operations, facilitating the buying of virtual assets, mainly stablecoins such as USDT and limited trading capabilities, as it only allows for purchasing VAs and not selling. In addition, Express minds allows for over-the-counter purchase of large volume Virtual Assets (VA) orders.

341. The VASP sector remains small but growing. As of December 2024, over BWP169 million in transaction volume was recorded. The sector remains highly concentrated and dominated by one major exchange. Other licensed VASPs have not commenced operations.

#### Features of the Product & common typologies

342. VA products/services in Botswana, as assessed in the report, include cryptocurrencies (e.g., Bitcoin, USD Tether, Ethereum, Solana), exchange services, custodial wallets, ATMs, and initial token offerings (e.g., Temtum's Pula-backed stablecoin). VA products carry several inherent ML/TF vulnerabilities. Their pseudonymous nature allows transactions to be linked to wallet addresses rather than real identities, although KYC controls help reduce this risk. Cross-border, peer-to-peer transferability and the ease of storing VAs on mobile or hardware wallets enable fast and borderless movement of value. Most activities occur non-face-to-face, relying on digital verification measures, while travel-rule compliance helps strengthen identity assurance.

343. Although block-chains provide transaction traceability, anonymity tools such as mixers or chain-hopping remain potential risks, even though they were not observed among licensed VASPs. The speed of transactions, operating instantly and 24/7, further increases inherent ML/TF exposure due to limited intervention time.

344. Additional features—such as the use of stablecoins, custodial or omnibus wallets, and Bitcoin ATMs—add convenience and liquidity but may introduce vulnerabilities related to regulatory arbitrage, cash conversion, and reduced transparency.

#### Target Groups of the Product

345. In Botswana, the primary target customers for virtual assets appear to be individual retail clients interested in buying, selling, sending, or receiving cryptocurrencies. For example, Yellow Card and Kalahari Exchange cater to clients trading Bitcoin, USD Tether, Ethereum, and other coins. Express Minds operates a BTM at Airport Junction shopping mall, targeting walk-in users for convenient crypto transactions. The combined active customer base across operational VASPs (Yellow Card and Express Minds) exceeds 1,200 users, reflecting growing interest among everyday consumers, including those seeking faster payment mechanisms or speculative trading.

#### Conditions or Thresholds for Eligibility

346. Eligibility to use VA products and services in Botswana is centred on robust user onboarding and AML/CFT compliance rather than financial entry barriers, requiring all clients of licensed VASPs to undergo CDD and KYC checks, including verified ID and proof of address, with beneficial ownership disclosure for business accounts; users assessed as higher risk—such as PIPs, non-residents, or individuals from high-risk or sanctioned jurisdictions, must undergo EDD, and VASPs must also verify source of funds for suspicious or high-value transactions to mitigate ML/TF risks.

## VA/VASP Sector vulnerability

347. Despite the small scale of operations, the sector exhibits Medium-High vulnerability to ML/TF risks due to several factors:

- The ecosystem is still maturing, with relatively low levels of institutional expertise and limited industry-wide understanding of ML/TF risk typologies.
- AML/CFT controls among VASPs remain uneven, with some entities lacking adequate internal controls, CDD processes, and AML/CFT training.
- The de-risking posture of traditional financial institutions — which results in minimal to no engagement between VASPs and technology operators exposed to significant risk (traditionally obliged entities i.e. TOEs) such as banks and payment processors — hinders transparency and effective supervision.
- The use of overseas platforms and decentralized exchanges (DEXs) remains a potential blind spot, given the cross-border nature of VA transactions.
- Nevertheless, vulnerabilities are partially offset by the fact that VASPs currently do not support privacy coins or high-anonymity features, reducing the risk of concealment of illicit finance flows.

## Product/channel Vulnerabilities in Sector

348. Botswana's regulatory framework, anchored in the Virtual Assets Act of 2022 and updated in 2025, empowers NBFIRA to license and supervise VASPs, covering key types including virtual asset exchange, virtual asset advisory, virtual asset broker-dealer, virtual asset custodian and issuers of initial token offering. However, emerging models such as decentralized finance (DeFi) platforms and non-custodial services fall into regulatory gaps as they are not explicitly addressed in the law, potentially allowing unlicensed foreign entities to engage with local users without clear restrictions.

349. This creates vulnerabilities where criminal interest could exploit weak oversight, making it easier for illicit actors to access the sector and layer funds through unregulated channels. Overall, this aspect contributes to a medium vulnerability, as foundational licensing exists but enforcement on cross-border and novel models remains underdeveloped.

350. VASPs in Botswana are newly licensed, with simple ownership structures and low transaction volumes, primarily offering major cryptocurrencies like Bitcoin and Ethereum. VASPs operating in the country do not offer complex products such as derivatives, Non-Fungible Token (NFTs), or DeFi services. However, their integration with global networks exposes them to cross-border risks from high-risk jurisdictions, where criminals might find profitability in exploiting limited local VASPs risk awareness and basic AML/CFT frameworks.

351. The small scale reduces immediate criminal involvement, but inadequate tools for monitoring geographic origins heighten detection challenges. This results in a medium rated vulnerability, balancing modest domestic operations against growing international exposures that could facilitate ease of use for illicit purposes. Licensed VASPs focus on

basic spot trading and custodial wallets for assets like BTC, ETH, and USDT, avoiding complex offerings like Non-Fungible Token (NFTs) or derivatives.

352. However, support for stablecoins and potential indirect access to obfuscation tools via foreign platforms increase risks, as these can enable reduced transparency and profitable layering for criminals. Variance in AML/CFT controls, often generic rather than product-specific, complicates detection, while under-resourced governance limits disruption. This leads to a medium rated vulnerability, where limited local products temper risks but gaps in oversight allow exploitation.
353. Delivery occurs predominantly through online platforms and mobile apps, enabling non-face-to-face interactions that heighten pseudonymity and rapid settlements. This borderless setup makes it accessible for criminals to move funds swiftly, bypassing traditional checks and increasing profitability for evasion schemes. Without robust real-time monitoring or threshold-based triggers, detection becomes challenging, particularly for peer-to-peer transfers. Vulnerability here is rated high, as the digital methods facilitate ease of use and hinder effective disruption in a nascent regulatory environment.
354. The customer base is mostly retail and modest in scale but includes foreign users and potential PIPs, with inconsistent enhanced due diligence and travel rule implementation. This exposes the sector to obfuscation risks, where criminals could conceal beneficial ownership through complex structures or high-risk jurisdictions, drawing on the sector's accessibility. Notwithstanding, section 26 of the Virtual Assets Act, 2025, which requires licensed VASPs to implement travel rule compliance mandating the sharing of data between originator and beneficiary VASPs. Limited screening for geographic ties further complicates detection. The vulnerability is medium, reflecting a small base offset by low barriers to access foreign unlicensed platforms that could enable criminal involvement.
355. VA transactions' borderless nature links Botswana's VASPs to customers from jurisdictions with lax AML/CFT regimes, often without geofencing or sanctions screening. This amplifies risks from sanctioned areas or non-resident clients, where criminals exploit profitability through unmonitored flows. Inadequate geographic profiling hinders detection and disruption. Vulnerability is medium because while Botswana has demonstrated a concerted effort to comply with FATF recommendations at a national level, VASPs currently lack the technical capacity to effectively manage cross-border risks and detect high-risk jurisdictions.
356. Interactions with international VASPs, including for liquidity, expose Botswana's sector to unlicensed or lightly regulated counterparts, a potential for the use of mixers or DeFi. Without risk classification frameworks or sanctions filtering, this heightens criminal interest in using such channels for obfuscation, making detection difficult amid pseudonymous arrangements. Vulnerability is high, due to the absence of tools for effective risk-based screening of counterparties, combined with the growing exposure to DeFi and pseudonymous arrangements, necessitates a high risk rating for this variable, as unlicensed counterparties with weak AML/CFT frameworks could facilitate ease of involvement in illicit networks.

357. Local VASPs offer coins like Bitcoin, USDT, Ethereum, and Solana, which lack enhanced anonymity features, but no policy bans riskier assets like privacy coins. This pseudonymity attracts criminals seeking to evade detection, enhancing profitability for layering without face-to-face controls. Vulnerability is high, as inherent tech features enable concealment, challenging traceability and detection in an emerging market.
358. While this feature increases financial efficiency due to near-instant settlement, it also removes layers of oversight and AML/CFT filtering, making it easier for illicit actors to move funds discreetly and swiftly across jurisdictions allowing quick cross-border moves that appeal to organized actors for efficient laundering. Absent robust fiat-VA monitoring or CDD triggers by some VASPs hinders the ability to monitor the entry and exit points of fiat in the virtual asset ecosystem, which is critical in identifying suspicious patterns, layering, or movement of illicit proceeds.
359. Consequently, this eases criminal use while complicating detection. Vulnerability is high, given the speed's role in disrupting traditional controls, leaving the country highly vulnerable to the abuse of rapid settlement features of VAs for financial crime.
360. Due to the borderless and digital nature of VAs, users in Botswana can easily access VA services from foreign VASPs that operate without being registered or licensed either locally or abroad, bypassing oversight and exposing the sector to fraud or illicit flows from grey zones. Limited detection tools and inter-agency coordination hinder identification, making it accessible for criminals to exploit regulatory arbitrage.
361. These risks are further amplified by the non-face-to-face, instant, and anonymity enhanced features of many foreign VASP operations. The lack of detection tools despite the regulatory effort leaves Botswana highly exposed to unregistered foreign VASPs, which pose elevated risks of ML/TF, fraud, and abuse. Vulnerability is rated medium, as some alerts exist, but gaps in enforcement and awareness when dealing with unregistered offshore VASPs heighten risks.

#### Main threats facing the Sector

362. While domestic VA adoption remains modest, the global environment demonstrates increasing exploitation of VAs by criminal networks.
363. The threat level for the VA/VASP sector is assessed as **Medium**. The following threat drivers are notable:

Threat drivers	Botswana context & justification
International exploitation of VAs for ML/TF	Global intelligence reports consistently demonstrate the use of VAs in predicate offences, including online fraud, cyber-enabled scams, drug trafficking, and extortion. Although Botswana has not recorded major ML/TF cases involving VAs, the international trend creates a realistic exposure risk, given the inherently borderless nature of VA transactions

Potential to bypass traditional monitoring mechanisms	Cross-border peer-to-peer (P2P) transfers, stablecoin conversions, and decentralized platforms enable value movement outside regulated channels. In the matrix, P2P cross-border transfer and portability was rated Very High Risk due to ease of transmission and the absence of real-time controls.
Anonymity and pseudonymity	While local VASPs do not list privacy coins or mixers, the underlying features of public blockchains—pseudonymous identifiers, wallet portability, and limited face-to-face contact—create a moderate exposure to ML/TF misuse. The matrix reflects this with Medium Risk ratings for anonymity, traceability, and absence of face-to-face controls.
Technological obfuscation tools	Mixers, tumblers, and decentralized exchanges (DEXs) were assessed as latent external threats. Their availability globally poses risks for cross-border transactions initiated or terminated outside Botswana’s regulated environment.
Limited detection capacity	Law enforcement agencies possess the legal authority to investigate and seize virtual assets, but current operational capacity remains developing. The matrix rates trace and seize difficulty and circumvention of exchange control as High Risk, acknowledging real constraints in blockchain analytics capability.
Growing regional usage	Neighbouring jurisdictions have experienced rising VA-related scams and social engineering schemes, some involving remittances and illicit value transfers. These regional trends increase the probability of spill-over into Botswana’s small but expanding market.

364. Collectively, these considerations justify a Medium threat rating, acknowledging that while domestic activity remains relatively controlled, external exposure continues to grow.

- The emerging interest of organized criminal groups globally in exploiting VAs for illicit finance.
- The potential for cross-border transactions to circumvent existing monitoring mechanisms.
- Although no major VA-related ML/TF cases have been reported in Botswana, the regional and international context indicates growing misuse of VAs for predicate offences such as fraud, scams, and drug trafficking.
- Anonymity and pseudonymity of VAs facilitate potential criminal misuse. VAs can be easily transferred across borders without regulatory oversight.
- Tools such as mixers, tumblers, and decentralized platforms may obscure illicit flows.
- Limited face-to-face verification and lack of advanced monitoring tools raise traceability concerns.

#### AML Controls & Mitigation

365. Botswana has established a sound legal and supervisory framework for the licensing and regulation of VASPs, largely aligned with FATF Recommendation 15. The regulatory oversight by NBFIRA, in collaboration with the FIU, provides a credible foundation for managing sectoral risks. Additionally, the non-engagement of TOEs, while currently limiting VASP functionality, also serves as a temporary barrier against uncontrolled exposure. Periodic inspections and licensing reviews provide further layers of assurance,

albeit requiring enhancement in the areas of data collection, enforcement of AML/CFT training, and risk-based supervision. These controls demonstrate proactive strengths in aligning with international standards, such as FATF Recommendations. Below are key areas highlighting their strengths:

#### Comprehensive AML/CFT Legal Framework

366. Botswana’s legal framework for virtual assets rests on a well-constructed foundation, anchored by the Virtual Assets Act—first enacted in 2022 and strengthened further in 2025, alongside targeted amendments to the Financial Intelligence Act. Together, these instruments fully integrate VASPs into the national AML/CFT system. They set out clear obligations around licensing, risk management programs, customer due diligence, enhanced measures for politically influential persons and high-risk jurisdictions, Travel Rule compliance, recordkeeping, STR filing, beneficial ownership transparency, and prohibitions on tipping-off. The Act also provides for civil and administrative sanctions, enabling NBFIRA to respond swiftly where non-compliance is identified.

#### Availability and effectiveness of entry controls

367. Entry controls under the Virtual Assets Act, 2025, serve as an early line of defence against criminal infiltration. All VASPs must be licensed or registered, and operating without a licence is expressly prohibited, an offence that carries sanctions. The licensing process is rigorous, requiring fit-and-proper assessments of beneficial owners, shareholders, and key management to ensure that only individuals of integrity can enter or influence the sector. VASPs are also required to maintain AML/CFT compliance structures, manuals, and trained personnel, and any changes in ownership or control must be pre-approved by the regulator. Enforcement actions taken against illegal operators illustrate that the system is not merely symbolic.

#### Adequate supervision and monitoring mechanisms

368. Supervision of VASPs rests within the regulatory scope of NBFIRA, which is empowered by the Virtual Assets Act, 2025, to conduct on-site inspections, carry out off-site reviews, compel records, and impose a range of sanctions, including licence suspensions or revocations. The supervisory mandate is reinforced by the accompanying regulations, manuals and guidelines that help translate the law into practice and give regulated entities clarity around expectations. As the sector evolves, the supervisory program is also expanding its lens to new risks, including DeFi-related exposures and innovations such as stablecoins. While the authority’s legal grounding is strong, the supervisory function is still refining its technical capability and deepening its risk-based approach. Staff training in AML/CFT is increasing, and each inspection incrementally strengthens market discipline.

#### Regulation of CDD, Source of Funds, and Reliable Identification Infrastructure

369. Customer due diligence obligations for VASPs are comprehensive and follow FATF standards closely. Operators must verify the identities of customers and beneficial owners using independent sources, understand the nature and purpose of business

relationships, monitor transactions on an ongoing basis, and apply enhanced measures where risk indicators are present. The source of funds must be scrutinized, and Travel Rule data must accompany transfers as required.

370. Botswana's national identity system and corporate registry (CIPA) provide strong foundational infrastructure for reliable verification. These systems give VASPs access to credible and authoritative information, strengthening their capacity to conduct proper CDD. Although these measures meet the required international thresholds, the system is still evolving toward more seamless and integrated verification mechanisms

#### Legal and Human Resource Capacity of Law Enforcement to Investigate, Trace, Seize, and Secure Virtual Assets

371. Law enforcement agencies have a clear legal mandate to investigate and act on virtual asset-related crimes. The VA Act, the FI Act, and the Proceeds and Instruments of Crime Act provide authorities with powers to trace, seize, and confiscate virtual assets and related proceeds. Agencies can compel information from VASPs, obtain records, and pursue confiscation orders. The FIA processes STRs involving virtual assets, supplying intelligence that supports investigations.
372. Capacity is steadily expanding through specialised training offered regionally and internationally, including via Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) and the World Bank. Officers are gaining familiarity with blockchain tracing, investigative techniques, and asset-handling procedures. While this capability is still maturing, the legal basis for action is strong, and the trajectory of skill development suggests a system moving in the right direction. This remains a functional, growing, and increasingly prepared for VA-related cases.

#### Effectiveness of Domestic Cooperation

373. Botswana's ability to engage internationally is supported by its membership in INTERPOL, ESAAMLG, and global UN conventions, providing multiple channels for mutual legal assistance, intelligence exchange, and cross-border collaboration. These mechanisms have historically been reliable for traditional financial crimes and are gradually being extended to issues involving virtual assets. NBFIRA's MOUs with foreign counterparts facilitate supervisory information sharing, helping to close gaps around cross-border risks.
374. While VA-specific cooperation protocols are still emerging globally, Botswana's existing treaty-based networks give it a meaningful platform for managing transnational exposures.

#### Interaction with Other Sectors

375. Limited interaction exists between VASPs and other TOEs, such as banks and insurance firms. De-risking strategies are in place, with most TOEs avoiding deep engagement with VA ecosystems.

## Residual Rating

376. The overall money laundering and terrorist financing ML/TF risk level of the VAs and VASPs sector in Botswana is assessed as **Medium-Low**. This assessment reflects the sector's early stage of development and the currently limited scale and complexity of VA-related activities within the country.

## Key considerations for High and Very High-Risk Areas

377. Several areas emerged as consistently high to very high risk throughout the assessment, forming a clear narrative of where Botswana's virtual asset ecosystem is most exposed. The sector's heavy reliance on digital onboarding presents significant identity-related vulnerabilities, particularly the potential misuse of synthetic identities and weak KYC points. Cross-border activity further amplifies these weaknesses, as most VA transactions occur through unregistered foreign platforms operating outside the domestic supervisory perimeter, creating substantial exposure to high-risk jurisdictions and international layering schemes.

378. Limited availability of transactional data and gaps in blockchain-analytics capability hinder the regulator's ability to detect emerging threats, while supervisory resourcing and specialised technical expertise remain insufficient for the pace at which the technology evolves. These structural characteristics, combined with growing regional trends in cyber-enabled offences, collectively underpin the conclusion that several inherent vulnerabilities in the VA ecosystem remain at a high level and require proactive strengthening before market expansion intensifies these risks.

379. Taking into account the sector's threat level, vulnerability factors, and existing legal and supervisory controls, the residual ML/TF risk is rated Medium-Low. However, this rating should not be interpreted as permanent — it is dynamic and contingent on how the sector evolves.

## Emerging Risks and Considerations

380. Looking ahead, several emerging risks and trends warrant proactive attention:

- **Entry of Privacy-Enhancing Technologies:** As the sector matures, privacy coins and mixing/tumbling services may be adopted, increasing anonymity and complicating transaction monitoring.
- **Decentralized Finance (DeFi):** Growth in decentralized platforms and peer-to-peer services may pose supervisory blind spots, especially when operators are unlicensed or foreign-based.
- **Cross-Border Risks:** With VAs inherently borderless, there is a growing need for international cooperation, information exchange, and adoption of the travel rule.
- **Digital onboarding and identity fraud:** As VASPs expand services digitally, there is heightened risk of identity fraud, necessitating strong Know Your Customer (KYC) mechanisms and the use of digital identity verification tools.

- Cybercrime and Ransomware: VAs are increasingly exploited in ransomware payments and cyber extortion, and while this is not yet prevalent in Botswana, early detection systems must be put in place.
- Regulatory Arbitrage: As global rules diverge, unregulated or poorly regulated jurisdictions may become channels for VA abuse, and Botswana must prepare for spill-over effects.

## **CHAPTER 9: TAX CRIMES RISK ASSESSMENT**

381. The purpose of this assessment is to identify, assess and understand tax crimes prevalent in Botswana, and further assess whether tax crimes are detected, investigated and successfully prosecuted. Tax-related offences were added to the FATF list of predicate offences in 2012, meaning that from that point onward countries were required to apply the ML offense to proceeds generated from tax related offenses.
382. Tax crimes refer to illegal activities related to the evasion or fraudulently misrepresentation of tax obligations. This may involve failure to submit returns, failure to register for Value added tax (VAT), VAT refund fraud, failure to maintain proper records, submitting false or misleading tax returns, false declaration and non-declaration of goods. These crimes undermine the confidence in the economy and government institutions. Botswana has taken significant steps to combat tax-related crimes in order to safeguard the integrity, stability, and fairness of its financial system.
383. The Botswana Unified Revenue Service (BURS), a semi-autonomous body under the Ministry of Finance, mandated to administer and enforce revenue laws as provided under the Botswana Unified Revenue Service Act (Cap 53:03). Legal instruments that empower BURS to execute its mandate are; the Income Tax Act (Cap. 52:01), Customs Act of 2018 (Cap. 50:01) and Value Added Tax Act (Cap 50:03).
384. The assessment approach drew on guidance from international standards and good practices, from the World Bank and OECD which were then adapted to the local context of the TCRA process which included;
- Identification of risks by developing a list of threats from law enforcement agencies/intelligence and potential vulnerabilities based on law enforcement, data analysis and/or emerging trends already observed.
  - Analysis of risks by analysing the threats and vulnerabilities, considering their nature, sources or origins, likelihood, and impact, to gain a complete overview and understanding of the risk.
  - Assessing risk mitigation measures put in place to determine residual risk based on inherent risk and mitigation measures

### Money Laundering Threats

385. Tax offence encompasses any violation of tax laws that results in the infringement of a government's right to collect tax revenue. These offences range from relatively minor administrative breaches to more severe acts of fraud or tax evasion. Tax evasion means the use of illegal methods by taxpayers to avoid paying tax or reduce tax payable. The assessment identified various tax crimes for the period under review as listed in the table below.

Table 34: Statistics of Tax Crimes (2020-2024)

TAX OFFENCES	Number	Amount Involved
Under declaration of income	1451	1,580,112,395.39
Non remittance of PAYE	61	70,882,787.79
Non/under declaration of cash	62	6,504,282.40
Non declaration of goods (Smuggling of goods)	1936	5,296,239.00
Falsified records and self-invoicing	99	44,274,583.00
Under valuation	2032	6,839,060.30

386. Under declaration of income was identified as one of the main crimes when considering number of incidents and the amount involved. Non-remittance of PAYE also posed a significant, in one case over P60 million of non-remitted PAYE was detected.
387. This illustrates that failure to enforce compliance on withholding tax (WHT) has a big impact hence a need for commensurate measures to deter the offence. Cross border offences incidences (non-declaration of goods and undervaluation) were found to be the most prevalent although amounts involved were relatively low as compared to other offences mentioned above. While this may be attributed to effective detection mechanisms as empowered by the existing legal and regulatory framework. The trend was also seen as a threat which necessitated strengthening of controls to detect and minimize possible incidents due to porous borders.
388. According to the FIA Trends Report of January-June 2024, tax evasion remained one of the most prevalent predicate offences in Botswana, a trend that was fully corroborated by the findings of this risk assessment. Based on both the volume of reported cases and the significant monetary values involved, the overall money laundering threat associated with tax crime is assessed as **high**.

#### Tax Crimes Vulnerability

389. The main focus of this chapter was factors that were seen to expose the country to tax crimes as discussed below. This assessment on tax crime vulnerabilities considered the weaknesses identified in Botswana's anti-tax evasion framework as it relates to; the country's Legal framework, institutional framework, organizational structure, operational practices and processes.
390. The risk assessment found that Botswana remains vulnerable to money laundering stemming from limited tax-crime detection and weak enforcement mechanisms. These gaps create opportunities for criminal actors to exploit deficiencies within the tax system to evade taxes or conceal illicit proceeds. The assessment also identified instances of inadequate integrity controls within the tax administration, which further enable offenders to bypass compliance measures. Additionally, a lack of sufficient

understanding and appreciation of tax-related offences among other law enforcement agencies and prosecutors may result in tax-related ML cases going undetected, allowing criminal networks to repeatedly exploit tax offences as a channel for laundering illicit funds.

391. The absence of tax compliance checks during licensing renewal by most supervisory authorities represent a significant weakness, as it allows tax offences and other illicit proceeds to enter and circulate within the formal economy with minimal risk of detection.

#### Vulnerabilities associated with of Prosecutions

392. During the period under review, no tax-related offences were successfully prosecuted, even though other predicate offences, including several high-profile cases, having been successfully prosecuted. The assessment identified only two tax crimes cases recorded during the period under review, in which the DPP restrained assets worth P28.2 million for the cases. In 2023, the DPP participated in one Prosecutor Guided Investigation alongside DCEC where P22.9-million worth of assets were restrained. In the second case, illicit proceeds amounting to P5.3 million were laundered from Botswana to several countries, including Tanzania, South Africa, Lesotho, the USA, and Nigeria.
393. In an effort to facilitate prosecution through effective investigation of tax crimes, BURS seconded two officers to the DPP during the period under review, with an objective of gaining insights into legal procedures and prosecution strategies and ultimately enhance capacity for prosecuting tax related crimes.
394. The low number of prosecutions was believed to be attributable to the capacity and financial constraints faced by the unit.

#### Integrity of Tax Officials

395. BURS also recorded incidents of compromised integrity of tax officials in performing their duties. The table below shows the number of integrity breach cases investigated over the review period and breakdown by Units within BURS, respectively. The BURS had drafted a Whistleblowing policy which had not yet been approved for implementation.
396. As at December 2024, only 40 out of the 75 recorded cases underwent the disciplinary process. The remaining 35 could be that the investigations were still on-going or that the evidence was not sufficient to support initiation of a disciplinary process. Further breakdown is provided in the table below.

Table 35: number of integrity breach cases investigated over the review period

Units	No. of Cases	Disciplinary Outcome/Status			
		Final Written Warning	Summary Dismissal	Acquitted	Investigations, Rec & report ongoing
Customs	29	10	13	4	2
Audit	2	1	1	0	0
TSC	1	0	1	0	0
Investigations	1	1	0	0	0
Large Taxpayer Unit (LTU)	2	0	0	1	1 (awaiting hearing outcome)
Return Processing	5	1	1	1	2 (awaiting court outcome)
<b>Total</b>	<b>40</b>	<b>13</b>	<b>16</b>	<b>6</b>	<b>5</b>

**Case Study: State vs. Ronald Kgano (2022)**

An intelligence report revealed that a BURS official collaborated with companies to fraudulently claim tax refunds. The officer received kickbacks, which were used to acquire assets. Assets worth P4.6 million were restrained by court order.

397. Considering the prevalence of integrity breaches and the number of hearing outcomes (final written warning and summary dismissal), the integrity of tax officials was deemed poor.

**Tax Audits of Private Sector**

398. BURS operates four dedicated tax audit Units namely; Small and Medium Taxpayer (SMTU), Inspectorate, Refunds Audit and Large Taxpayer (LTU) with a total staff complement of 41 tax auditors. Although these Units apply risk-based compliance programmes and auditors possess the requisite technical skills, the assessment established that the human resource capacity remains insufficient, resulting in fewer than one percent of taxpayers being audited annually.

Table 36: Number of tax audits conducted during the review period

Tax Year	No of Audits	Total Tax assessed (BWP)
2020	288	998,012,605.00
2021	185	132,375,047.00
2022	372	724,532,335.00
2023	424	1,262,251,209.01
2024	540	103,436,116.52
<b>Total</b>	<b>1,809</b>	<b>3,220,607,312.53</b>

399. The overall ML Vulnerability for Tax Crime was rated as Medium

#### AML Control & Mitigation

400. The assessment on the AML control environment considered several key factors to determine the country's ability to prevent, detect, and respond to tax-related money laundering. Together, these variables provide a clear picture of the robustness of AML controls related to tax crimes.

- the **tax legal framework** — including information access, investigative powers, and sanctions was examined to determine whether authorities have the necessary tools to address tax offences.
- **effectiveness of domestic and international cooperation** was assessed to understand the extent of information sharing and coordination on both local and cross-border tax matters.
- **capacity and resources** of tax and law enforcement agencies were reviewed to gauge whether staffing, skills, and systems are sufficient to support investigations.
- **effectiveness of prosecutions** and the **integrity of tax officials** were assessed, given their influence on enforcement credibility.
- **completeness of registration and licensing systems**, along with the **volume and quality of private-sector tax audits**, were evaluated to determine oversight coverage and the ability to detect non-compliance

#### Comprehensiveness of Tax Legal Framework

401. Botswana has enacted tax laws which empowers tax officials to obtain information, detect non-compliance, investigate offences and apply sanctions in accordance with legislations such as the Income Tax Act, the Value Added Tax Act, and Customs Act. The OECD 2023 report affirmed the adequacy of these powers, noting that BURS is authorised to access information even where such information is requested for criminal tax investigations. The report further concluded "no material deficiencies were identified in Botswana's legislation in relation to the access powers of the competent authority". The assessment established that the tax laws provided for both administrative and criminal sanctions

402. BURS Revenue Officers were designated as prescribed investigators under the Proceeds and Instruments of Crime (Amendment) Act of 2022.

Table 37: Administration and Criminal Sanction

<b>Tax Law</b>	<b>Administrative Sanction</b>	<b>Criminal Sanction</b>
Income Tax Act	sections 117 to 119	sections 120 to 129A
VAT Act	section 16(9)- non-registration section 26(6)-failure to lodge a VAT return section 33(5)-failure to pay VAT	section16(8)-non-registration section 26(4)-failure to lodge a VAT return section24(8)-non-conforming tax credit or debit notes.
Customs Act	N/A	section 96(8)- failure to lodge customs declaration section 16(2)- submission of fraudulent information section 34(3)-failure to provide information upon request

Effectiveness of the Inter-Agency Cooperation (Domestic)

403. BURS signed a number of MoUs, including with Supervisory Authorities, to strengthen information exchange on tax-related matters. During the review period, law enforcement agencies undertook various joint activities to enhance to enhance information sharing and coordinated enforcement. The case studies below illustrate positive outcomes achieved through these collaborative efforts.

**Case study 1**

In 2020 BPS and BURS had a joint operation after receiving an information that there were some locals who were in possession of foreign and local currencies (USD 64,400.00, ZAR 913,910.00, SZL 50, BWP 328,090.00). The suspects were arrested and failed to account for currencies in their possession. The money was subsequently confiscated to the state through administrative forfeiture.

**Case Study 2**

In 2022, information was received that there were locals who were in possession of money and drugs (Meth-cathinone and dagga). An operation was conducted by LEAs (BURS, BPS and DIS) where the team recovered drugs and BWP103 500.70 in cash. BURS ultimately seized the money through administrative forfeiture, while BPS continue with the case of drug trafficking as a predicate offence.

Table 38: The number of joint activities conducted (2020 to 2024)

<b>Type of Activity</b>	<b>2020</b>	<b>2021</b>	<b>2022</b>	<b>2023</b>	<b>2024</b>
Joint operations	21	36	25	9	6
Joint investigations	30	60	27	0	0
Joint Border patrols	17	16	31	0	0

404. The information shared with BURS has produced significant results, including the issuance of additional tax assessments, the application of penalties up to 200% of the value, collection of unpaid debts and accumulated interests, enhanced risk profiling and the seizure of illicit consignments. The table below presents information sharing statistics and the corresponding assessment value (BWP) raised by BURS for non-compliance each year.

Table 39: Information sharing statistics and the resulting assessment value (BWP)

<b>Intel. From</b>	<b>2020</b>	<b>2021</b>	<b>2022</b>	<b>2023</b>	<b>2024</b>
BPS	8	14	2	8	11
DIS	0	0	4	17	5
FIA	10	14	18	3	17
DCEC	0	0	22	1	3
<b>Total (BWP)</b>	<b>379,094,793.40</b>	<b>67,999,822.40</b>	<b>83,986,335.38</b>	<b>43,328,835.40</b>	<b>233,064,380.21</b>

405. During the period under review, BURS seconded two Officers to the DISS- Counter Terrorism Analysis and Fusion Agency (CTAFA) for a period of 3 years to enhance cooperation and strengthen the effectiveness of joint engagements.

406. Domestic inter-agency cooperation is rated medium high, reflecting strong collaborative structures and frequent joint operations, but also noting delays and uneven capacity.

#### Effectiveness of International Cooperation

407. Botswana signed bi-lateral agreements with the OECD and African Tax Administrators Forum (ATAF) and has also signed Double Taxation Avoidance Agreements (DTAAs) with about 24 jurisdictions. The agreements are meant to increase tax transparency, mainly to deter tax evasion and money laundering.

408. Botswana shares tax information with any other country, despite provisions of other laws, particularly intercountry tax agreements which may provide for the non-sharing of tax information.

409. LEAs had mechanisms in place for providing/requesting assistance internationally e.g. through INTERPOL, MLA, agreements with other revenue administrations under SADC Protocol on Trade, treaties provided by World Customs Organisation and other tax related authorities. There were frequent joint international operations initiated by the World Customs Organisation or INTERPOL on matters relating to tax crime that Botswana participated in. These operations resulted in few investigation cases. The table below demonstrates Botswana's utilization of international law enforcement networks such as Customs Enforcement Networks (CEN) that provides for the exchange of information related to tax crimes trends.

Table 40: Requests made to other tax administrators by BURS.

<b>Year</b>	<b>No. of Requests</b>	<b>No. of Responses</b>	<b>Responding Administration</b>
2020	1	1	NAMRA-Namibia
2021	1	1	KRA-Kenya
2022	5	4	SARS-South Africa
	1	1	ZIMRA-Zimbabwe
	1	1	ATM-Mozambique
	1	1	KRA-Kenya
2023	3	3	SARS-South Africa
	2	2	ZRA-Zambia
	3	1	ZIMRA-Zimbabwe
	1	1	NAMRA-Namibia
	1	1	KRA-Kenya
	1	1	GRA-Ghana
2024	3	0	SARS-South Africa
	2	2	ZRA-Zambia
	1	1	ZIMRA-Zimbabwe
<b>Total</b>	<b>27</b>	<b>21</b>	

Table 41: Requests made to other regional and international bodies

<b>SOURCE</b>	<b>2020</b>	<b>2021</b>	<b>2022</b>	<b>2023</b>	<b>2024</b>
Interpol	2	5	4	0	0
ARINSA	0	0	0	0	0
W.C.O	2	0	3	0	0

Table 42: Requests received by BURS from other tax administrators.

Year	No. of Requests	No. of Responses	Requesting Administration
2020	1	1	SARS-South Africa
	1	1	ZIMRA-Zimbabwe
2021	1	1	Isle of Man
	1	1	NAMRA-Namibia
	1	0	RLS-Lesotho
2022	3	3	SARS-South Africa
	1	1	ATM-Mozambique
	2	2	NAMRA-Namibia
	1	1	NCS-Nigeria
2023	4	4	SARS-South Africa
	2	2	ZIMRA-Zimbabwe
	1	1	ATM-Mozambique
Year	No. of Requests	No. of Responses	Requesting Administration
	1	1	NAMRA-Namibia
	1	1	CHINA
	1	1	TRA-Tanzania
2024	2	0	SARS-South Africa
	1	1	NAMRA-Namibia
	1	0	ZRA-Zambia
	1	1	TRA-Tanzania
Total	27	23	

410. The country's strong mechanisms for fostering international cooperation—through well-established agreements, active engagements, and transparent tax-information sharing—demonstrate a highly effective framework that aims to deter tax evasion and money laundering, but the delays in responses leaves a room for improvement. Therefore, this variable was rated **medium high**

## Capacity and Resources at Tax Policy Unit (TPU) & Law Enforcement Agencies

411. The TPU, which is mandated to draft, amend and ratify tax laws, had only nine officers at the time of assessment and is complemented by 31 officers from the General Investigation Unit. While the team possesses substantial policy experience, additional capacity building initiatives are required to further strengthen their technical competencies. The unit is supported by the Legal Services and Domestic Tax Departments which are adequately resourced and actively contribute to the legislative development process.
412. BURS, BPS and DCEC have established specialised units mandated with investigation of money laundering and assets forfeiture. The authorities are empowered under the PICA and other legislations, to investigate, seize and restrain assets.
413. Botswana has established a range of measures to safeguard its borders against illicit activities, however recent assessments highlighted the need to place greater focus on high-risk ports of entry, where vulnerabilities are more likely to be exploited.
414. While the Tax Policy Unit and the LEAs possess adequate resources and staff complements to carry out their mandate, additional capacity-building initiatives have been identified to further strengthen technical and related competencies. As a result of these gaps, **the rating is medium.**

## Comprehensiveness of Registration and Licensing Authority

415. The assessment established that Supervisory Authorities in Botswana required a tax clearance certificate from entities as part of the entry level registration process for licensing. However, most Authorities did not require their regulated entities to present a tax clearance certificate upon renewal of their licences, save for NBFIRA and Gambling Authority.
416. The Overall rating for the effectiveness of Control was rated as Medium.

## Residual Rating

417. The overall ML risk rating for Tax crimes was Medium high looking at the gaps identified in the legal framework, the insufficient staffing levels and the need of more capacity building programmes.

## CHAPTER 10: ENVIRONMENTAL AND NATURAL RESOURCES CRIMES RISK ASSESSMENT

418. The Environment and Natural Resources (ENR) sectors comprising forestry, wildlife, mining, and waste management, plays a pivotal role in economic development, rural livelihoods and biodiversity conservation. Botswana’s management of natural resources is both a national economic priority and a global ecological responsibility. The four sectors have been assessed independently and their ratings are as shown in the below table;

Table 43: Money Laundering Risk Level of the ENR Sector

ENR SECTOR	ML THREAT	ML VULNERABILITY	ML RISK
Wildlife	Medium	Medium High	High
Mining	Low	Medium High	Medium
Forestry	Low	Medium High	Medium
Waste	Low	Medium High	Medium

### Main Threats facing ENR Sector

#### (a) Wildlife Sector

419. The wildlife sector is one of the country’s most significant natural and economic assets supporting the tourism industry and contributing to biodiversity conservation. Roughly 40% of the land in Botswana is under conservation as national parks, game reserves, wildlife management areas (WMAs) making it one of the leading countries in Africa for biodiversity conservation.

420. The country hosts one of the largest elephant populations in Africa (approx. 130,000+), representing nearly one-third of the continental population. Wildlife tourism contributes significantly to GDP and employment: in 2023, tourism contributed around 5% of GDP (pre-COVID levels reached 13-14%), with wildlife resource as the main attraction. The sector is crucial for rural development through the community-based natural resource management (CBNRM), a program aimed at improving livelihood of communities through utilisation of wildlife resources particularly through trophy hunting, photographic safaris, eco-tourism, etc.

421. Botswana’s conservation approach is globally comparable to countries like Costa Rica, though the latter has more advanced ecotourism models and high-income contribution to GDP. When compared to the USA and United Kingdom, Botswana’s wildlife sector contribution to GDP is higher.

### Environmental and Social Impact of Wildlife Crimes

422. Wildlife crime drives many species to extinction as it reduces their population. The reduction of animal population, including key species, can disrupt the balance of the

ecosystems. For example, predators control the population of herbivores thus preventing overgrazing and allowing vegetation to thrive.

423. Environmental crime has potential to fuel organised crime networks involved in the illegal harvesting and trafficking of wildlife resources and this ultimately weakens the rule of law. A reduction in the population of wildlife resources leads to loss of livelihood opportunities for communities engaged in cultural tourism. Most communities derive value from utilising wildlife resources, for example; The DWNP issues hunting quotas for citizens, community trusts etc. to benefit from wildlife resources through the community based natural resource programme (CBNRM).
424. Community based organisations are allowed to enter into agreements with potential partners to better utilise wildlife resources. It is through this programme that potential investors/partners invest financially with the organizations. Mostly these investors are safari hunting companies who hunt for animal trophies (e.g. elephant tusks).
425. Often, this citizen economic empowerment initiative is abused by the investors. A typical example of community exploitation was noted through social media where a local newspaper (Sunday Standard) article 'Community trusts in global mafia network' reported that a community trust entered into an agreement with a notorious rhino poaching syndicate and an international trafficker raising concern of infiltration by criminal syndicates. The article, published on the 16<sup>th</sup> December 2024, disclosed that local communities are used as 'grey' nodes (legal players who participate in illegal activities) in criminal hunting schemes by the international wildlife mafia. The article further disclosed that the criminal syndicate member who is currently facing over (one thousand) 1000 counts of racketeering, money laundering, fraud, intimidation and illegal hunting infiltrated Botswana since 2017. This presents a high risk to money laundering activities in the wildlife sector in Botswana.
426. The alleged criminal has not committed any registered illegal activity in Botswana, his criminal activities are registered in the United States of America and South Africa. In addition, he is also partnering with a Botswana registered company (through suspected fronting) to access the community resources. The findings were supported by Prince William during the Global Summit (October 2022) - ESAAMLAG and United for Wildlife, where he reported the damaging impact of illegal wildlife trade, estimated at up to \$20 billion annually, and was associated with violent crime, corruption and robbed countries of their natural resources, funded organised crime, and harmed the most vulnerable communities.

(b) Mining Sector

427. The Mining Sector in Botswana is dominated by diamonds. Diamonds contributed +25 per cent of GDP and over 80 per cent of export revenue in the review period. Botswana is the world's largest producer of diamonds by value and the second largest by volume. Diamond sales are the main engine for foreign exchange, government revenue, and infrastructure development. Botswana, like Namibia, has more stable governance and better revenue management compared to her regional peers. Globally, Botswana's

mining GDP share is far above that of high-income nations like Canada or Australia, which have diversified economies.

428. The risk assessment identified two (2) predicate offences in the mining sector; illegal trade of mining products (Diamonds and Gold) and illegal mining. A total of sixty-five (65) cases of gold mining were recorded by Botswana Police Service (BPS) from 2020 to 2024 with the value of the confiscated proceeds amounting to P9 890.35. The illegal mining of gold occurred in the northern region of Botswana<sup>25</sup> (Matsiloje, Kalakamati, and Francistown). Ninety percent (90%) of the suspects were foreigners (mostly Zimbabweans) while ten percent (10%) were Botswana. Only one money laundering (ML) case was registered by the BPS in 2020, a case that was also referenced by an ESAAMLG typology on Illicit Dealings in Gold, Diamond, Rubies and Associated Money Laundering and Terrorist Financing<sup>28</sup>, Sept 2022.
429. A notable rise in illegal mining of Gold operations was observed from 2022 to 2023 and a decline in 2024 due to government interventions through joint operations and community sensitization. The modus operandi observed was the use of minors in these illegal mining activities as well as use of metal detectors to explore untouched land for gold. Only one (1) case of polished diamonds (12 units) was recorded during the period under review and the value of the confiscated diamonds was P22, 499.50.
430. The total value of confiscated proceeds from these predicate offences during the period under review was P32, 389.85 which was considered insignificant relative to Botswana's economy.

#### Environmental and Social Impact of Mining Crimes

431. According to information from open sources, residents of the affected areas raised concerns that the surge in illegal mining has led to environmental degradation, including pollution of indigenous lands and water sources, posing health risks to residents and livestock. Communities have reported living in fear due to the presence of criminals, who often operate in large numbers with dangerous tools. Another source highlighted the environmental risk that comes with illegal mining due to the use of hazardous chemicals<sup>26</sup>.
432. According to Botswana Daily News newspaper dated 27 May 2024<sup>27</sup>, some residents of Shashe ward in Maun expressed displeasure about illegal sand mining in the Shashe channel that forms part of Thamalakane River. The residents were worried of the negative impact on the environment, a situation that has been going on for several years.

---

<sup>25</sup> <https://www.sundaystandard.info/francistown-gold-rush-illegal-miners-exploit-lenient-mining-laws/> <sup>28</sup> ESAAMLG typology of [Illicit Dealings in Gold, Diamond, Rubies and Associated Money Laundering and Terrorist Financing](#)

<sup>26</sup> <https://www.mmegi.bw/news/matsiloje-police-face-uphill-battle-against-illegal-mining/news>

<sup>27</sup> <https://www.dailynews.gov.bw/news-detail/79750>

433. These findings were supported by the latest report by the Wildlife Justice Commission (WJC) under the report titled, "Convergence of wildlife crime with other forms of organised crime: A 2023 review"<sup>28</sup>. The review indicated that sand mining in these environments can cause erosion threatening communities and livelihoods at both the point of extraction and further downstream in the affected system, as well as the salination of aquifers and groundwater reserves, loss of protection against storm surges, land-use changes, shrinking deltas, and threats to freshwater and marine fisheries and biodiversity. Therefore, the mining sector ML threat was rated **low**.

(c) Waste Management Sector

434. Waste streams include household, e-waste, industrial and mining waste. Waste sector is crucial for urban environmental management, especially in cities. The sector is still emerging with significant environmental and health risks. Poorly managed waste threatens water resources, human health, and biodiversity. The country generates over 500,000 tons of waste annually, with less than 10 per cent recycled which is far below those of high-income countries (>30–40 per cent in European Union (EU) and OECD countries).

435. The waste sector faced challenges with illegal waste transportation possibly attributed to intended illegal disposal. During the period under review, Department of Environmental Protection (DEP) recorded nine (9) incidents of 'illegal dumping/disposal'<sup>32</sup> and 14 incidents of 'transportation of waste without a waste license'. The DEP applied administrative fines on all the twenty-three (23) offences. The assessment established that these violations were not proceeds generating for money laundering.

Environmental and Social Impact of Waste crimes

436. On the Botswana Daily News Newspaper<sup>29</sup> dated 8 August 2022, an environmental officer expressed that issues of illegal dumping of waste were worrisome and that waste could cause a variety of issues beginning with environmental impact which may lead to disruption of community's good health and quality lifestyle. It was revealed that 103 people have been charged for illegal dumping of waste and faced administrative charges of P86 800. Considering the low reported incidences the waste sector ML threat was rated **low**.

(d) Forestry Sector

437. The Forestry Sector plays a role in Botswana's economy and ecosystem. Forests play a major role in carbon sequestration and mitigating desertification. The country has about 29 million hectares of forest area, largely in the north and eastern parts of the country.

---

<sup>28</sup> <https://wildlifejustice.org/wp-content/uploads/2023/10/Crime-Convergence-Report-2023-pages-V07.pdf>

<sup>32</sup> <https://dailynews.gov.bw/news-detail/55713>

<sup>29</sup> <https://dailynews.gov.bw/news-detail/68502>

438. The country has six (6) main forest reserves located in the Chobe District which provide vital habitats for threatened and endangered wildlife species. The reserves are also essential for water catchment, supporting the Chobe river, which is a significant source of water for both wildlife and local communities. Approximately 50 per cent of Botswana's forests are affected by land degradation due to unsustainable grazing, cultivation, fuel wood harvesting and uncontrolled fires.
439. Botswana has two key initiatives being Botswana Sustainable Miombo-Mopane Landscape Management Project and Forest Conservation Botswana. The sector is not a large formal economic contributor (per cent of GDP), but it's critical for fuelwood, charcoal, construction materials, and traditional medicine. Over 70 per cent of rural households depend on forests for energy and livelihoods.
440. During the period under review, there were 2 428 incidents which included illegal harvesting of veld products, taking of forest resources (thatching grass and firewood) and dealing in veld products. The mopane worm is considered an important resource from the mopane woodlands and has been classified as a non-timber forest product. The harvesting and commercialisation of mopane worms contribute to the local economy and provide food security. According to the open sources, there has been rising incidences of illegal mopane harvesting<sup>30</sup>. The waste sector ML threat was rated Low.

#### Financial Impact of Wildlife crime

441. Among all ENR crimes assessed, wildlife crime posed a significant threat to ML considering its extent, nature and actors involved. The working group could not assess the financial impact per predicate offence because the country has not yet quantified the financial value of species targeted in wildlife crime.
442. The country identified significant challenges in assessing the scale and estimated value of criminal proceeds generated by wildlife crime. These challenges were largely due to the absence of a standardised approach for quantifying the financial impact, including determining the life-value of the targeted species and the value of the poached animal products such as horns or tusks. Limitations in law enforcement seizure or recovery of poached products further compounded the challenges in estimating the value of the products in the absence of the poached products.
443. To address the gap, the assessment considered three valuation methods:
- CITES valuation (current country approach): This method is found to be limited as it involves that weighing of products which may not be available due to low detection and recovery of the concerned wildlife product. FATF aligned valuation approach: Based on the June 2020 report on Money Laundering and Illegal Wildlife Trade.

---

<sup>30</sup> <https://www.ngamitimes.co.bw/mother-sons-escape-p300-000-phane-heist-imprisonment/>

- Research-based methodology: Utilising lifetime valuations from studies conducted by international independent researchers and organizations.

Extent of the crime

Scenario 1

Table 44: Predicate Offences Amounts Involved (LEAs data reported to CITES)

Year	Unlawful Possession of Elephant Tusks		Unlawful Killing of Rhinos	
	No of Cases	Total Estimated Value(BWP)	No of Cases	Total Estimated Value (BWP)
2020	24	549,631.75	59	0.00
2021	32	581,506.99	22	0.00
2022	25	594,289.27	6	0.00
2023	13	266,051.52	11	0.00
2024	15	852,617.33	0	0.00
	<b>109</b>	<b>2,844,096.85</b>	<b>88</b>	<b>0.00</b>
<b>Total</b>	<b>2,844,096.85</b>			

444. In assessing the economic scale of wildlife-related offences, the Working Group applied value estimates for elephant ivory derived from the Elephants Trade System (ETIS) which is an online primary tool for monitoring the illegal trade of ivory and other elephant products managed by Trade Records Analysis of Flora and Fauna in Commerce (TRAFFIC), a strategic alliance (International NGO) that works with Convention On CITES to ensure that Trade in wild plants and animals is not a threat to the conservation of nature.

445. These estimates enabled a more consistent and internationally aligned evaluation of offences involving elephant tusks. However, it is important to note that CITES did not provide comparable value estimates for rhino horn. As a result, the assessment of rhino-related crimes could not draw on standardized CITES valuation data hence the findings of no financial value of rhino horns. As such, the working group relied on alternative information sources for valuation of the two predicate crimes as detailed on scenario 2 and 3.

Rating: Low due to number of cases and estimated domestic proceeds.

Scenario 2

446. Considering the fact that the CITES did not have a standard estimation of rhino horn value, the working group opted to use the estimations of the black-market value of the rhino horn based on the Financial Action Task Force (FATF) report on Money Laundering and Illegal Wildlife Trade of June 2020.

Table 45: Black-market value of the rhino horn based FATF report on Money Laundering and Illegal Wildlife Trade of June 2020

		Unlawful Killing of Rhinos			
YEAR	Av. USD rate per Year	BWP per Kg@USD37,000.00	Estimated Weight(Kg)	No of Cases	Total Estimated Value
2020	10.9125	403,763.87	4	59	23,822,068.27
2021	11.7353	434,205.66	4	22	9,552,524.43
2022	12.8832	476,678.51	4	6	2,860,071.07
2023	13.4894	499,107.95	4	11	5,490,187.43
2024	13.6574	505,323.50	4	0	0.00
<b>Total</b>				<b>88</b>	<b>41,724,851.20</b>

### Scenario 3

447. The assessment applied the resource lifetime valuations by studies conducted by several international independent researchers/organisations that advocate for conservation and natural resource management - the lifetime valuations are adopted by United Nations Office on Drugs and Crime (UNODC).

Table 46: Predicate Offences Amounts Involved (Lifetime Value)

	Unlawful possession of elephant tusk		Unlawful killing of Rhinos	
YEAR	No of Cases	Total Estimated Value	No of Cases	Total Estimated Value
2020	24	1,143,720,000.00	59	4,380,750,000.00
2021	32	1,524,960,000.00	22	1,633,500,000.00
2022	25	1,191,375,000.00	6	445,500,000.00
2023	13	619,515,000.00	11	816,750,000.00
2024	15	714,825,000.00	0	0.00
<b>Total</b>	<b>109</b>	<b>5,194,395,000.00</b>	<b>88</b>	<b>7,276,500,000.00</b>
<b>TOTAL</b>	<b>12,470,895,000.00</b>			

Rating: Low considering the amounts of proceeds generated domestically

Nature of the crime

448. Wildlife crimes are Transnational, offences for elephant and rhino poaching are mostly committed in Botswana and animal products are trafficked outside. Sophisticated concealment of poaching such travelling by foot and through difficult to transverse areas such as swamps. The poachers have demonstrated capability to killing of tracked animals without. There is also suspect information leakages from insiders

449. **Criminal Actors** – typically known to be organised transnational criminal syndicates. The local actors are low actors in the value chain whilst major proceeds are laundered externally. There is also suspicion of involvement of professionals - former agents previously involved in anti-poaching activities.

450. The overall threat for Wildlife crime threat was rated: Medium

AML Control & Mitigation

451. The rise in environmental crimes, along with its links to bribery and corruption, its strong connection to money laundering, and its broader environmental impact—have required

increased efforts to strengthen the financial crime prevention and detection measures of the country, in order to safeguard the environment. Botswana had a comprehensive legal framework for seizing, freezing, and confiscating proceeds and instruments of environmental and natural resource (ENR) crimes.

#### Legal framework for environmental crime

452. The country has aligned its legislative framework with FATF's definition of environmental crimes. And has defined environmental and natural resource offenses in both legal and regulatory instruments, such as Convention on International Trade on Endangered Species of Fauna and Flora (CITES) and Convention on Biological Diversity which are domesticated by the Wildlife Conservation and National Parks Act 28 of 1992, Forest Act 23 of 1968. The Basel Convention is domesticated under the Waste Management Act of 1998 and the Kimberly Process is domesticated under the Mines and Minerals Act, 17 of 1999.
453. The statutes listed above criminalised offences that facilitate the commission of ENR crimes.

#### Financial Intelligence Agency (FIA)

454. The Financial Intelligence Agency (FIA) plays a central role in gathering, analysing, and disseminating financial intelligence to support investigations into environmental and ENR-related crimes. In addition to the FIA, several inter-agency structures such as the Botswana Defence Force (BDF), Botswana Police Service (BPS), Directorate on Intelligence and Security (DIS), Botswana Unified Revenue Service (BURS), and the Department of Wildlife and National Parks (DWNP) have set up dedicated intelligence units that are mandated to collect, analyse, and share intelligence specific to ENR offences. While these bodies operate independently, they maintain structured channels for coordinated information-sharing, ensuring that relevant intelligence is effectively communicated to support operational and investigative efforts.

#### Preventive law enforcement & Designated Authorities

455. The DWNP, Department of Environmental Protection (DEP) and Department of Forestry and Range Resources (DFRR) under the Ministry of Environment (MET) and Department of Mines (DoM) under the Ministry of Mines and Energy (MME) are preventative authorities (bodies) established to coordinate and develop strategies and measures for preventing environmental and ENR-related crimes, and they work closely with specialised law enforcement units under existing legal frameworks.
456. Although Botswana did not have a combined national strategy to address all ENR crimes, all the designated Authorities developed independent strategies tailored to promote conservation and sustainable utilisation of natural resources. More precisely, the DoM had the Minerals and Energy Strategy, DEP had the Botswana Strategy for Waste Management while the DWNP developed and launched a National Anti-Poaching Strategy (2025-2030) in April 2025. Launched by the Minister of Environment and Tourism, the strategy was aimed at combatting wildlife crimes.

457. Other joint preventive activities enabled through these agencies included antipoaching patrols, intelligence gathering, and public outreach initiatives.
458. Preventative measures such as patrol intensification, rhino dehorning, and translocation of rhinos from the wild led to reductions in illegal killing of rhinos in the wildlife sector i.e. in 2020, 61 rhinos were poached and since the translocation in 2022 the numbers declined to zero in 2024.

#### Anti-corruption efforts

459. As environmental crimes are at times motivated by the substantial illegal profits generated, it often relies on corrupt practices such as bribery and undue influence both in private and public sectors.
460. As such, the country had a dedicated anti-corruption investigative body, the DCEC, which was complemented by anti-corruption units across government ministries. The National Anti-Corruption Strategy (2021-2026) provided a structured approach to addressing corruption, with regular reviews every five years.

#### Reporting and Whistleblowing

461. The country has adopted laws such as the Whistle-blowers Protection Act of 2016, the Corruption and Economic Act of 1994 enable whistle-blowers and witnesses to report offenses thus strengthening the fight against environmental crime. These efforts have strengthened the community participation in the form of whistle blowing and sustainable management of resources through the Community Based Natural Resource Management (CBNRM) program. CBNRM in Botswana focuses on providing incentives for communities to take responsibility for managing natural resources sustainably, and on actively building community capacity to do this. The community participation was evident also in the tip-offs received from the general public which had led to most of the arrests on ENR crimes.

#### Quality of Judicial Evidence

462. To support and enable authorities in the investigation and prosecution of ENR crimes, information is gathered from various sources including experts, NPOs, reports from the public and intelligence preventative bodies. DWNP also had trained biologists to conduct DNA analysis and morphology (trophy identification) analysis. Additionally, the DEP operated a functional forensic testing laboratory, providing key support for case work.

#### Sanctions

463. ENR legislation for the wildlife and mining sectors provided for both administrative and criminal sanctions for ENR violations, albeit enhancements in respect of the effectiveness and proportionality of sanctions is required. In instances where administrative fines were not imposed, cases were forwarded to the DPP for

prosecutions. Below are criminal sanctions for the most prevalent predicate offences in the wildlife sector, as provided under the WCNP Act.

Offence	Criminal Sanctions
Unlawful possession of elephant tusk	A fine of P50 000.00 and ten (10) years imprisonment. (Section 67)
Unlawful possession of government trophy	A fine of P5 000.00 and five (5) years imprisonment. (Section 71)
Unlawful killing of Rhinoceros	A fine of P100 000.00 and fifteen (15) years imprisonment. (Section 67)

### Customs and Border Controls & Regional collaboration

464. Botswana's border and customs forces (BURS, BDF, BPS, DIS, DWNP and Department of Immigration, Department of Veterinary Services) played a crucial role in combating border control violations, including ENR crimes, with structured efforts in place to monitor, detect, and respond to these offences at points of entry and exit.
465. Assessment reflected that Botswana strategically deployed LEAs (BURS, BPS, DIS, BDF) and DWNP in borders and hotspot areas to combat ENR crimes. A specialized Border Management Unit (under BDF) operates 21 base camps to prevent illegal crossings, DWNP, DIS and BPS has several Forward Operating Bases (FOBs) in an effort to augment areas where there were no permanent offices mandated to combat ENR crimes. Additionally, there were instances where extended patrols were conducted to cover the vast areas. Through the KAZA-TFC and KTC, the DWNP coordinated bilateral patrols involving neighbouring countries such as South Africa, Zambia, Zimbabwe, and Namibia. The vastness of Botswana's geographical area and porous borders make Botswana susceptible to illegal ENR trafficking. Control measures such as use of drones, aerial surveillance, GPS systems, canine (search) dogs, and vehicle scanners were used to monitor inaccessible terrains and detect illegally obtained ENR products, however, the controls were assessed to be inadequate.

### Regional collaborations

466. Joint investigative efforts are supported through regional collaborations such as the Trans Kalahari Corridor (TKC) and Kavango Zambezi Transfrontier Conservation Area (KAZA-TFCA). Through these cooperation, Botswana has successfully conducted several cases-such as the arrest of several cross border nationals who entered Botswana illegally to poach elephants for the period under review as shown in the table below.

YEAR	No. of Investigated Cases (Joint)	Country	Details
2020	1	Botswana & Zambia	Investigation of suspects intercepted in Botswana for smuggling 270 rifle, 19 live rounds of .270 ammunition, 3 live rounds of .270 ammunition and 89 live rounds of 9mm ammunition into Botswana from Zambia.
2021	-	--	-
2022	-	-	-
2023	3	Botswana & Namibia	Unlawful possession of elephant tusks. Both tusks were intercepted in Namibia and alleged to be originating from Botswana. 1st consignment (24 tusks), 2nd consignment (15 tusks) and 3rd consignment (18 tusks). Thus making a total of 57 tusks altogether. Poachers alleged they poached 5 elephants in Botswana while some tusks were picked from the forest.
2024	1	Botswana and Zimbabwe	Arrest for unlawful possession of 15 elephant tusks alleged to be originating from Botswana
Total	5	Total number of cross border criminals arrested: 17, in total 72 Tusks were seized.	

The table below shows the number of joint operations during the review period.

Number of joint operations					
2020	2021	2022	2023	2024	Total
322	188	213	151	205	1079

467. The following case studies demonstrate the effectiveness of domestic cooperation.

Unlawful Possession of Government Trophy- Elephant Tusks
<p><b>Case Study 1:</b> On 21/06/2021, information was received that there is a person in possession of an elephant tusk looking for a buyer in Gaborone. A joint team consisting of BPS, DWNP, BDF and DIS executed an operation in which 3 Batswana were arrested in possession of one elephant tusk. The case was successfully completed and Accused 1 and 2 were fined P10 000.00 each or 4 years' imprisonment in default of payment. 3rd accused was discharged and acquitted.</p> <p><b>Case Study 2:</b> A joint operation consisting of DIS, BPS, BDF and DWNP led to an arrest of 11 Batswana on 14/03/2023 for possession of 1 pair of elephant tusks at Grand Palm in Gaborone. The 11 were convicted to 5 years imprisonment, wholly suspended and ordered to pay P10 000 each.</p>

## Environment and Natural Resources (ENR) Sector Vulnerabilities

468. In overall Botswana was rated medium high vulnerability to ENR crime and related ML. This rating was mainly attributed to the following factors.
469. Despite having a legislation that provides for administrative and criminal sanctions on ENR, the penalties for most offences were not proportionate and dissuasive considering the consequences/impact to the country hence not deterrent.
470. Although ENR crimes fall within the scope of predicate offenses to money laundering, the legislation did not provide for a minimum monetary and prison term fines thereby giving Judges liberty to use their own discretion to charge suspects below the prescribed fines, as shown in the following case studies:

Case 1:

Unlawful Possession of Government Trophy- Elephant Tusks

Case Study 1: On 08/01/2020 Two Batswana men were fined Seven Thousand Pula (P7000.00) each by the magistrate court after they were found in possession of an elephant tusk in Semolale.

Case 2: One Motswana man was arrested on 07/11/2020 for possession of four elephant tusks in Nata village. The suspect was verbally warned and released the same day. The exhibit (4 Tusks) were seized and forfeited to the state.

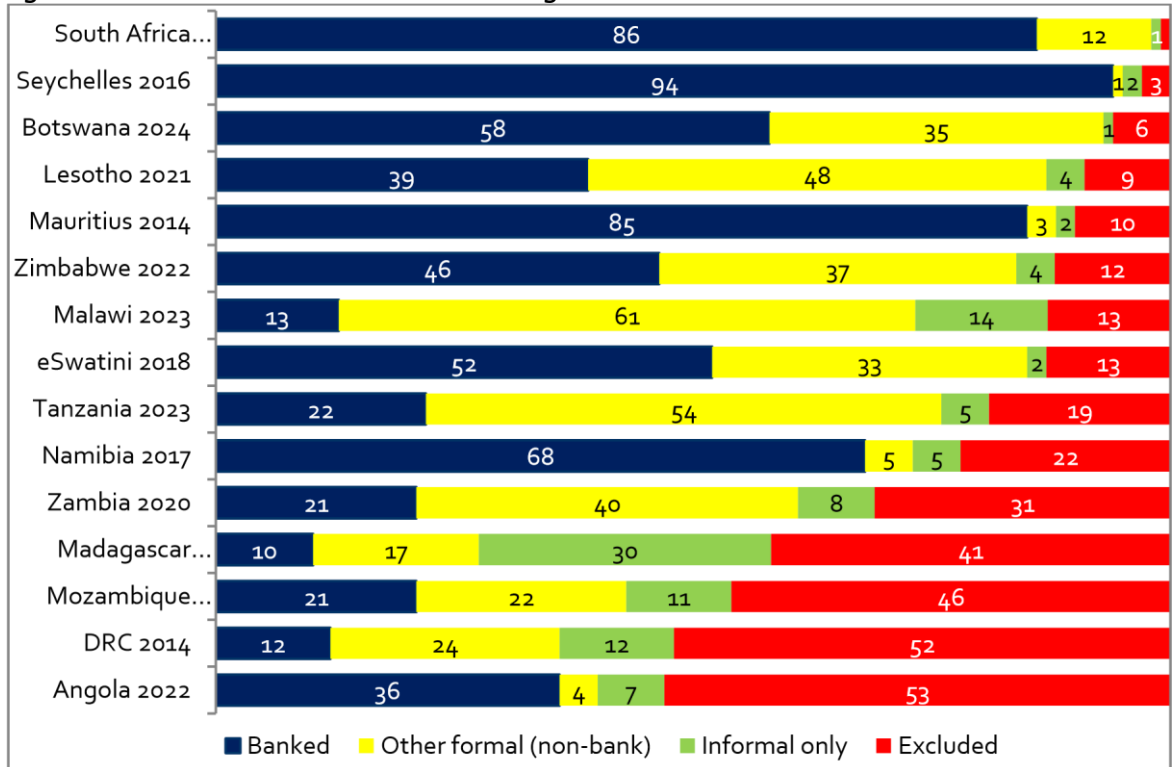
471. Lack of dedicated units to investigate ENR crimes at the designated authorities (DWNP, DEP, DFRR, DoM) limited interpretation, understanding and application of legal frameworks for ENR sectors.
472. There was inconsistency in deployment of wildlife officials at ports of entry and limited knowledge on identification of ENR products by personnel deployed at ports of entry. This made it easy for ENR crimes to go undetected at ports of entry and eventually making it difficult to disrupt smuggling of environmental products.
473. Inadequate storage facilities for seized properties and lack of storage and rehabilitation facilities for live animals whilst waiting for court orders affected the quality of evidence and subsequently resulting in prosecutors losing tangible evidence of proceeds of crime.
474. Shortage of financial resources to facilitate acquisition of control measures/equipment such as vehicles, air crafts, boats and special tools to identify ENR crimes at border posts or inland reduced capacity for monitoring and enforcement.
475. The absence of due diligence measures for investors, donors and beneficiaries of natural resource products created a potential avenue for money laundering, as illicit funds may be placed into, layered or integrated through ENR sector.
476. Lack of typologies and trend reports by FIA in relation to ENR crimes limits the understanding of ML risks existent in the ENR sectors leading to low awareness by reporting entities and lack of specialised/technical skills to analyse ENR crimes.

477. There was limited understanding of the economic, environmental and social impacts of ENR crimes by key stakeholders therefore limiting the prosecution prospects.
478. Delays in extradition process and intelligence sharing due to lengthy protocols resulted in prosecution delays of ENR crimes.

## CHAPTER 11: FINANCIAL INCLUSION PRODUCTS RISK ASSESSMENT

479. Botswana ranks third in terms of financial inclusion within SADC, at 94% inclusion rate, meaning that only 6% of the adult population remain excluded. It is surpassed only by South Africa and Seychelles.

Figure X: SADC Financial Inclusion Rankings



480. For this risk assessment, the products considered for financial inclusion were money or value transfer services/ electronic payment services (MVTs/EPS), savings, micro loans, insurance and virtual assets. Mobile money was identified as the main driver of the high financial inclusion rate.

481. Although a separate risk assessment of financial inclusion products was conducted, a decision was made not to make a separate report on the module as the products fall within the various sectors assessed being banking, insurance, new technologies and other financial institutions.