



AML/CFT/CPF FINANCIAL SYSTEM INTEGRITY REPORT

2026



Disclaimer

This report has been prepared by the Financial Intelligence Centre (FIC) for informational, analytical and policy-support purposes. The information and analysis presented are based on data and inputs available to the FIC at the time of preparation and are intended to provide an assessment of trends, risks and developments affecting Namibia's financial system integrity.

While reasonable measures have been taken to ensure the accuracy and reliability of the information, the FIC does not warrant that all information is complete, current or free from error. The findings and views expressed should not be interpreted as allegations of wrongdoing against any individual or institution, nor as a substitute for legal, regulatory or professional advice.

The report may be updated or amended where new information becomes available or where material corrections are identified. The FIC accepts no liability for any loss or consequence arising from reliance on the report beyond its intended purpose.

Copy right @2026 FIC, Republic of Namibia.

All rights reserved. No part of this report may be reproduced or distributed without prior written authorization, except as permitted by the FIC.

TABLE OF CONTENTS

LIST OF TABLES	5
LIST OF FIGURES	5
ABBREVIATIONS	6
DEFINITIONS	7
FOREWORD BY THE ACTING DIRECTOR	8
REMARKS BY THE AML/CFT/CPF COUNCIL CHAIR	10
EXECUTIVE SUMMARY	11
CHAPTER 1: INTRODUCTION	12
1.1 Background	12
1.2 Objectives of the report	12
1.3 Scope of the report	12
1.4 Data analysis methodology	13
1.5 Limitations	13
CHAPTER 2: INTERNATIONAL AML/CFT/CPF TRENDS AND DEVELOPMENTS	14
2.1 Global financial crime landscape	14
2.2 Emerging global money laundering trends	14
2.2.1 Implications of money laundering on financial stability	17
2.3 Terrorist financing trends	17
2.3.1 Implications of terrorist financing on financial stability	18
2.4 Proliferation financing trends	19
2.4.1 Implications of proliferation financing on financial stability	20
CHAPTER 3: NAMIBIA'S ECONOMIC AND FINANCIAL CRIME LANDSCAPE	22
3.1 Economic overview	22
3.2 Geographic and demographic factors	22
3.3 Crime landscape	22
CHAPTER 4: DOMESTIC AML/CFT/CPF DEVELOPMENTS	24
4.1 Legislative developments	24
4.2 Institutional developments	25
4.3 Technological developments	26
4.4 Namibia's removal from the FATF grey list	26
CHAPTER 5: FINANCIAL INTELLIGENCE DATA OVERVIEW	28
5.1 Data overview from the FIC	28
5.2 Summary of key observations	33
CHAPTER 6: ANALYTICAL FINDINGS	36
6.1 Overview	36
6.2 Potential tax-related offence trends	36
6.2.1 Various reasons for reporting transactions as suspicious	38

TABLE OF CONTENTS

6.3 Potential fraud-related offence trends	40
6.3.1 Various reasons for reporting transactions as suspicious	42
6.4 Potential corruption-related offence trends	43
6.4.1 Various reasons for reporting transactions as suspicious	45
6.5 Geographic distribution and frequency of reported typologies	46
CHAPTER 7: CASE STUDIES	48
7.1 Overview	48
CHAPTER 8: ANALYSIS OF KEY FINANCIAL RISKS IN NAMIBIA	56
8.1 Overview	56
8.2 Fraud-related offence risk analysis	56
8.2.1 Fraud risk cycle	56
8.2.2 Fraud risk matrix	56
8.3 Tax-related offence risk analysis	57
8.3.1 Tax-related offence flow	57
8.3.2 Tax-related risk matrix	58
8.4 Corruption-related offence risk analysis	58
8.4.1 Corruption-related risk cycle	58
8.4.2 Corruption-related risk matrix	59
8.5 Stakeholder questionnaire: Summary of key findings	60
8.5.1. Overall AML/CFT/CPF maturity assessment	61
8.5.2. Most significant financial crime risks	61
8.5.3. Key operational challenges	61
8.5.4. Effectiveness of anti-money laundering controls	61
8.5.5. Heat map of risk areas	62
8.5.6. Stakeholder priorities	62
8.5.7. Executive control panel	63
8.6 Overall observations	63
CHAPTER 9: RECOMMENDATIONS	64
9.1 Policy and regulatory recommendations	64
9.2 Strategic priorities	65
CHAPTER 10: CONCLUSION	66
Bibliography	67

LIST OF TABLES

Table 1: Summary of emerging global ML trends and financial stability implications	15
Table 2: Financial stability implications of emerging ML trends	17
Table 3: Emerging TF trends and financial stability implications.....	18
Table 4: Implications of emerging TF trends on financial stability	19
Table 5: Implications of PF for financial stability.....	20
Table 6: Summary of key outcomes for institutional developments.....	25
Table 7: Technological developments adopted and implemented by institutions	26
Table 8: Categorisation of STRs by analysis outcome	29
Table 9: Categorisation of SARs by analysis outcome	30
Table 10: Cross-border movement of cash reports received from sectors	31
Table 11: Summary of key observations as per FIC statistics.....	34
Table 12: Potential tax-related offence typologies and indicators by reporting entities.....	38
Table 13: Cross-border movement of cash reports received from sector.....	41
Table 14: Potential fraud-related offence typologies and indicators.....	42
Table 15: Value of potential corruption-related spontaneous disclosures to the ACC.....	45
Table 16: Potential corruption-related offence typologies and indicators.....	46
Table 17: Rating of fraud risk assessment matrix	57
Table 18: Rating of tax risk assessment.....	58
Table 19: Corruption-related risk cycle	59
Table 20: Corruption-related risk assessment matrix.....	59
Table 21: Consolidated key findings	60

LIST OF FIGURES

Figure 1: Evolution of emerging ML trends and AML/CFT/CPF responses.....	16
Figure 2: Namibia's major predicate offences and their impact on financial stability	23
Figure 3: AML/CFT/CPF compliance: Namibia's legislative and regulatory framework.....	24
Figure 4: STRs received from reporting sectors per annum	28
Figure 5: SARs received from reporting sectors per annum	30
Figure 6: Incoming requests domestic received per annum	32
Figure 7: Incoming requests international received per annum	33
Figure 8: STRs related to potential tax offences received from sectors	36
Figure 9: Tax-related offences: spontaneous disclosures to NamRA per annum	37
Figure 10: Potential tax offence values per annum	38
Figure 11: STRs related to potential fraud offences filed by sectors.....	40
Figure 12: Potential fraud spontaneous disclosures per annum	41
Figure 13: STRs related to potential corruption offences filed by sectors.....	43
Figure 14: Potential corruption spontaneous disclosures per annum to the ACC	44
Figure 15: Demonstration of fraud risk cycle.....	56
Figure 16: Demonstration of tax-related flow stage	57

ABBREVIATIONS

ADLAs	Authorised dealers with limited authority
AML/CFT/CPF	Anti-money laundering, countering the financing of terrorism, and countering proliferation financing
AML	Anti-money laundering
AI	Artificial intelligence
BO	Beneficial ownership
CDD	Customer due diligence
CFT	Countering the financing of terrorism
CMA	Common Monetary Area
CPF	Countering proliferation financing
CTR	Cash threshold report
DeFi	Decentralised finance
DNFBPs	Designated non-financial businesses and professions
EDD	Enhanced due diligence
ESAAMLG	Eastern and Southern Africa Anti-money Laundering Group
FATF	Financial Action Task Force
FIC	Financial Intelligence Centre
FIUs	Financial intelligence units
FIs	Financial institutions
FIA	Financial Intelligence Act, 2012 (No. 13 of 2012), as amended
IFIs	Illicit financial flows
IT	Information technology
IRDs	Incoming requests domestic
IRIs	Incoming requests international
KYC	Know your customer
LEAs	Law enforcement agencies
ML	Money laundering
ML/TF/PF	Money laundering, terrorist financing, and proliferation financing
NamPol	Namibian Police Force
NamRA	Namibia Revenue Agency
NPOs	Non-profit organisations
NRA	National Risk Assessment
PEPs	Politically exposed persons
PF	Proliferation financing
PIPs	Prominent influential persons
POCA	Prevention of Organised Crime Act, 2004 (No. 29 of 2004)
REs	Reporting entities
SADC	Southern African Development Community
SAR	Suspicious activity report
SOEs	State-owned enterprises
STR	Suspicious transaction report
TBML	Trade-based money laundering
TF	Terrorist financing
UN	United Nations
UNCAC	United Nations Convention Against Corruption
UNODC	United Nations Office on Drugs and Crime
UNSCR	United Nations Security Council Resolution
VASPs	Virtual asset service providers
WMD	Weapons of mass destruction

DEFINITIONS

Accountable Institution	An accountable institution refers to a person or entity listed in schedules 1 and 3 of the Financial Intelligence Act, 2012 (No. 13 of 2012), as amended. In this document, the term 'accountable and reporting institutions' refers to all authorised dealers and authorised dealers with limited authority.
Act	Financial Intelligence Act, 2012 (No. 13 of 2012), as amended
Anti-Money Laundering, Countering the Financing of Terrorism and Countering Proliferation Financing Framework (AML/CFT/CPF)	An AML/CFT/CPF framework is the national (or international) framework that combats and prevents money laundering, the financing of terrorism, and proliferation financing activities.
Customer Due Diligence	Customer due diligence is the process that involves establishing the identity of a client and monitoring all transactions of the client against the client's profile.
Proliferation Financing (PF)	"The act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations."
Money Laundering (ML)	ML refers, generally, to the act of disguising the true source of proceeds generated from unlawful activities and presenting such in the financial system as sourced from legitimate activities. However, in terms of the Prevention of Organised Crime Act, 2004 (No. 29 of 2004), the definition of ML is broad enough to include the engagement, acquisition, and concealment of the proceeds of crime, whether directly or indirectly.
Suspicious Activity Report (SAR)	Suspicious activity reports are submitted to the FIC in terms of sections 33(1) and (2) of the Financial Intelligence Act, 2012 (No. 13 of 2012), as amended.
Suspicious Transaction Report (STR)	Suspicious transaction reports are submitted to the FIC in terms of sections 33(1) and (2) of the Financial Intelligence Act, 2012 (No. 13 of 2012), as amended.
Terrorist Financing (TF)	"Acts which are aimed at directly or indirectly providing or collecting funds with the intention that such funds should be used, or with the knowledge that such funds are to be used, in full or in part, to carry out any act of terrorism as defined in the Organization for African Unity (OAU) Convention on the Prevention and Combating of Terrorism of 1999, irrespective of whether or not the funds are actually used for such purpose or to carry out such acts."
Terrorism	While no acceptable international definition for terrorism exists, it is generally described as the execution of acts of violence against persons or property, or a threat to use such violence, with the intent to intimidate or coerce a government, the public, or any section of the public to achieve or promote any tribal, ethnic, racial, political, religious, or ideological objectives.
Vulnerabilities	When used in a risk assessment, the term 'vulnerabilities' comprises those weaknesses that can be exploited by the threat or that may support or facilitate its activities
Threat	A 'threat' is an activity, person, group of people, or object with the potential to cause harm. A threat is contingent on actors who possess both the capability and the intent to do harm.
Supervisory Technology (SupTech)	Supervisory technology is used by regulators to enhance supervision and compliance monitoring.

FOREWORD BY THE ACTING DIRECTOR



This inaugural Financial Intelligence Centre AML/CFT/CPF Financial System Integrity Report marks a significant milestone in the advancement of Namibia's anti-money laundering, countering the financing of terrorism, and countering proliferation financing (AML/CFT/CPF) regime. As a flagship publication, the report provides a strategic and comprehensive assessment of the money laundering, terrorist financing, proliferation financing, and related financial crime risks that have the potential to impact the integrity, resilience, and stability of Namibia's financial system. The report seeks to strengthen risk understanding, support evidence-based decision-making, and enhance the effectiveness of Namibia's AML/CFT/CPF framework.

The integrity of the financial system in Namibia is fundamental to economic growth, investment, financial inclusion, and national development. However, increasingly sophisticated financial crime threats continue to exploit technological advancements, globalisation, and cross-border financial flows. As these risks evolve, effective cooperation among government institutions, reporting entities, supervisory authorities, law enforcement agencies, and the private sector and international partners remains essential to safeguarding Namibia's financial system.

A significant achievement during the period under review was Namibia's successful completion of the Financial Action Task Force (FATF) Action Plan within

a shorter timeframe than originally anticipated. Through strong political commitment and coordinated national efforts, Namibia addressed all identified strategic deficiencies, reinforcing the country's commitment to protecting the integrity of its financial system, reducing illicit financial flows, and maintaining confidence in the international financial architecture. These accomplishments demonstrate the resilience of Namibia's AML/CFT/CPF framework and the effectiveness of collaboration across the public and private sectors. While this achievement marks an important milestone, it also signals the beginning of the next phase of continuous improvement. Namibia has commenced preparations for the next National Risk Assessment and the country's forthcoming Mutual Evaluation in 2030. These processes will provide an opportunity to deepen our understanding of emerging risks, strengthen mitigation measures, and further enhance the effectiveness of the national AML/CFT/CPF regime. The findings contained in this report are intended to support these efforts by providing a comprehensive assessment of key trends, vulnerabilities, risks, and developments affecting financial system integrity.

The report highlights encouraging progress in reporting, financial intelligence generation, inter-agency cooperation, and stakeholder awareness. At the same time, it identifies areas that require continued vigilance as criminal actors increasingly exploit new technologies, cross-border channels, and complex financial structures to move and conceal illicit funds. Addressing these challenges will require sustained commitment, innovation, and the effective use of financial intelligence to detect, deter, and disrupt financial crime.

The findings of this report give us confidence that Namibia's financial system remains resilient to the threats of money laundering and is becoming increasingly capable of identifying and mitigating financial crime risks. The strengthening of financial intelligence to the threats of money laundering, supervision, investigations, prosecutions, and stakeholder cooperation has improved our national ability to prevent, detect, and respond to money laundering (ML), terrorist financing (TF), and proliferation financing (PF) threats. Looking ahead, our focus must remain on addressing emerging risks, embracing technological innovation, strengthening beneficial ownership transparency, building institutional capacity, and deepening intelligence-led cooperation at both domestic and international levels.

The Financial Intelligence Centre (FIC) remains committed to supporting national efforts through strategic analysis, stakeholder engagement, and the production of actionable financial intelligence. It is our hope that this report will serve as a valuable resource for policymakers, reporting institutions, supervisors, law enforcement agencies, development partners, and the wider public in strengthening Namibia's collective response to financial crime.

As Namibia looks towards the future, let us remain steadfast in our commitment to protecting the integrity of our financial system, combating illicit financial flows, and strengthening the effectiveness of our AML/CFT/CPF framework. Together, through continued partnership, innovation, and vigilance, we can safeguard our financial system, support sustainable economic development, and position Namibia as a trusted and resilient participant in the global financial community.

With the report now published, we look forward to the AML/CFT/CPF Conference in October 2026, led by the FIC. Convened under the theme 'From Prevention to Recovery: Strengthening Namibia's AML/CFT/CPF Framework for Sustainable Effectiveness', the Conference will provide an important platform for advancing dialogue, strengthening partnerships, and promoting an integrated approach that connects preventive measures with effective investigation, prosecution, asset recovery, and the sustainable implementation of Namibia's AML/CFT/CPF framework.

In closing, the conclusions of this report reaffirm that protecting financial system integrity is a continuous national responsibility. The progress recorded provides a strong foundation, and the risks and priorities identified call for sustained vigilance, coordinated action, and measurable implementation. I therefore encourage all stakeholders to use the report's conclusions and recommendations to guide policy and strengthen institutional responses.

I wish to express my sincere appreciation to all stakeholders who contributed to the development of this report and to the broader strengthening of Namibia's AML/CFT/CPF framework. Through continued cooperation, vigilance, and a shared commitment to reducing illicit financial flows, we can further safeguard the integrity of our financial system, support sustainable economic development, and position Namibia for continued success in the years ahead.



Ms Zenobia Barry

Acting Director: Financial Intelligence Centre

Windhoek, Namibia
2026

At the same time, it identifies areas that require continued vigilance as criminal actors increasingly exploit new technologies, cross-border channels, and complex financial structures to move and conceal illicit funds. Addressing these challenges will require sustained commitment, innovation, and the effective use of financial intelligence to detect, deter, and disrupt financial crime.

REMARKS BY THE AML/CFT/CPF COUNCIL CHAIR



As the first publication of its kind, this report demonstrates our collective commitment to evidence-based policymaking, transparency, and continuous improvement of the national AML/CFT/CPF framework.

The findings of this report confirm that Namibia's financial system remains resilient and increasingly capable of identifying and mitigating financial crime risks. The improvements observed in reporting quality, financial intelligence generation, supervision, stakeholder awareness, and inter-agency cooperation are encouraging indicators of a maturing national framework. At the same time, this report reminds us that financial crime continues to evolve. As these risks evolve, our response must evolve with equal determination and agility.

One of the most important messages emerging from this report is that effectiveness matters. Success cannot be measured solely by compliance with laws and regulations. Sustainable effectiveness requires that financial intelligence leads to investigations, investigations lead to prosecutions, and prosecutions ultimately contribute to the recovery of criminal proceeds and the disruption of criminal networks. This is how we protect our financial system, our economy, and our citizens from the harmful effects of financial crime.

Through the work of the FIC and its partners, financial intelligence continues to support domestic investigations, international cooperation, asset

Sustainable effectiveness requires that financial intelligence leads to investigations, investigations lead to prosecutions, and prosecutions ultimately contribute to the recovery of criminal proceeds and the disruption of criminal networks. This is how we protect our financial system, our economy, and our citizens from the harmful effects of financial crime.

recovery efforts, and informed decision-making across the government and private sector. This strengthens our ability to detect, deter, and disrupt illicit financial activity while supporting transparency and accountability.

The publication of this report comes at a particularly important time for Namibia. Having successfully completed the FATF Action Plan, we are now entering a new phase focused on sustaining effectiveness, and addressing emerging risks. It is therefore fitting that this year's AML/CFT/CPF Conference will be convened under the theme 'From Prevention to Recovery: Strengthening Namibia's AML/CFT/CPF Framework for Sustainable Effectiveness'.

As Chairperson of the AML/CFT/CPF Council, I wish to thank the FIC and all stakeholders who contributed to the strengthening of Namibia's AML/CFT/CPF framework. The progress reflected in this report demonstrates what can be achieved through partnership, commitment, and a shared determination to protect our financial system. Together, we can continue to strengthen financial system integrity, reduce illicit financial flows, enhance public confidence, and ensure that Namibia remains a trusted, transparent, and resilient participant in the global financial system.

Mr Ebsen Uunguta

Chairperson, AML/CFT/CPF Council

Governor of the Bank of Namibia

Windhoek, Namibia
2026

EXECUTIVE SUMMARY

This report provides a strategic assessment of the key developments, trends, and emerging risks that affect the integrity, resilience, and stability of Namibia's financial system. The report evaluates the effectiveness of Namibia's AML/CFT/CPF framework by analysing financial intelligence, stakeholder feedback, regulatory developments, and international best practices. The report also examines the impact of global and domestic financial crime trends, economic developments, technological innovation, and cross-border financial activities on the country's exposure to ML/TF/PF risks.

The findings indicate that Namibia has continued to strengthen its AML/CFT/CPF framework through legislative and regulatory reforms, enhanced supervisory oversight, improved financial intelligence capabilities, and increased collaboration among the FIC, supervisory authorities, law enforcement agencies, and reporting institutions. While these efforts have enhanced governance, compliance, and reporting quality, the report identifies corruption, fraud, cyber-enabled financial crime, trade-based money laundering, virtual asset-related risks, and cross-border illicit financial flows as the most significant threats to Namibia's financial system integrity.

Stakeholder feedback further highlights the need to strengthen beneficial ownership transparency, improve the quality of suspicious transaction reporting, enhance intelligence sharing, build institutional capacity, improve investigations and prosecutions, and expand the use of technology to address increasingly sophisticated financial crime. Overall, the report concludes that Namibia's financial system regarding the prevention and combatting of ML, TF, and PF remains resilient, supported by an established AML/CFT/CPF framework and continued commitment to adhere to international standards. To sustain this progress, continued implementation of risk-based supervision, stronger inter-agency and international cooperation, improved financial intelligence sharing, technological innovation, and enhanced public-private partnerships will be essential. These measures will strengthen the country's ability to detect, prevent, and disrupt financial crime, safeguard the integrity and reputation of the financial sector, and support sustainable economic growth and financial stability.



1.1 Background

ML, TF, and PF pose significant threats to financial integrity, economic stability, national security, and good governance. These illicit activities enable criminals and terrorist networks to conceal the proceeds of crime, finance unlawful activities, and exploit weaknesses within financial systems. As financial transactions become increasingly globalised and technology-driven, criminals continue to develop more sophisticated methods to move and disguise illicit funds, creating new challenges for governments, regulators, and financial institutions worldwide.

Namibia has established a comprehensive AML/CFT/CPF framework, which is aligned with international standards. The FIC, established in terms of the Financial Intelligence Act, 2012 (No. 13 of 2012), as amended, serves as Namibia's Financial Intelligence Unit and is mandated to receive, analyse, and disseminate financial intelligence relating to suspected ML/TF/ PF activities. The Act further empowers the FIC to undertake strategic analysis, monitor trends and patterns of financial crime, and provide guidance and information that support the effective implementation of Namibia's AML/CFT/CPF framework. These responsibilities are consistent with the standards set by the FATF, particularly FATF Recommendation 29, which requires financial intelligence units (FIUs) to serve as national centres for the collection and analysis of financial intelligence and the dissemination of information to competent authorities.

As financial crime threats continue to evolve, strategic analysis has become increasingly important in identifying emerging risks, vulnerabilities, and trends. Furthermore, FATF Recommendation 1 requires countries to identify, assess, and understand their ML/ TF/PF risks and to apply a risk-based approach to mitigating those risks. In support of these obligations, this report provides a strategic assessment of Namibia's AML/CFT/CPF environment by examining key developments, financial crime threats, sectoral vulnerabilities, and emerging typologies. The findings are intended to support evidence-based policymaking, strengthen stakeholder awareness, enhance inter-agency cooperation, and contribute to the effectiveness of Namibia's efforts to combat ML, TF, and PF.

1.2 Objectives of the report

The objectives of this report are to provide stakeholders with a comprehensive understanding of Namibia's AML/CFT/CPF environment by highlighting key developments, emerging risks, legislative and regulatory changes, and financial crime trends; to assess the impact of ML, TF, and PF on the financial system; to enhance awareness of Namibia's risk profile and compliance with international standards; and to strengthen stakeholder capacity through strategic insights and best practices.

Specifically, this report aims to:

- highlight key developments in the prevention and detection of ML/TF/PF risks at national, regional, and international levels;
- assess the impact of ML, TF, and PF on Namibia's economy, financial system, and financial integrity;
- identify key risks, threats, vulnerabilities, and mitigation measures within Namibia's AML/CFT/CPF framework;
- provide an overview of legislative and regulatory developments and enforcement actions related to AML/ CFT/CPF;
- inform stakeholders of emerging ML/TF/PF typologies, trends, and patterns that affect the financial system;
- enhance awareness of Namibia's ML/TF/PF risk profile and alignment with international AML/CFT/CPF standards;
- demonstrate the FIC's analytical value through strategic insights on financial crime risks and trends;
- strengthen stakeholder capacity by providing information on emerging AML/CFT/CPF issues and best practices;
- promote the effectiveness of Namibia's AML/CFT/CPF framework through risk-based and coordinated responses; and
- strengthen national AML/CFT/CPF efforts through enhanced cooperation among stakeholders.

1.3 Scope of the report

The scope of the report includes:

- ML: An assessment of money laundering threats, vulnerabilities, typologies, and trends that affect Namibia's financial system and economy.
- TF: An overview of terrorism financing risks, methods, preventive measures, and developments relevant to the national AML/CFT/CPF framework.
- PF: An examination of risks associated with the financing of the proliferation of weapons of mass destruction and measures implemented to mitigate such risks.
- Domestic and international developments: A review of significant AML/CFT/CPF developments, initiatives, and emerging issues at national, regional, and international levels.

- Sectoral risk trends: An analysis of ML/TF/PF risks and vulnerabilities across various sectors, including financial institutions, designated non-financial businesses and professions (DNFBPs), and other reporting entities.
- Financial intelligence trends: An assessment of trends in financial intelligence, including suspicious transaction reporting, intelligence analysis, and information sharing to support the detection and disruption of financial crime.
- Regulatory developments: A summary of key legislative, regulatory, supervisory, and enforcement developments aimed at strengthening Namibia's AML/CFT/CPF framework and compliance with international standards.

1.4 Data analysis methodology

The analysis in this report is based on multiple data sources to provide a comprehensive assessment of Namibia's AML/CFT/CPF environment. It primarily draws on FIC data, including suspicious transaction reports (STRs), suspicious activity reports (SARs), and other regulatory reports, complemented by information from law enforcement agencies (LEAs), supervisory authorities, and other competent authorities.

The report also incorporates open-source intelligence and publications from international bodies such as the FATF, the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), and the Egmont Group of Financial Intelligence Units, as well as relevant academic and industry research. Both quantitative and qualitative analytical approaches were used to assess reporting trends, sectoral risks, typologies, regulatory developments, enforcement actions, and emerging threats. Such approaches enable

the identification of key risks and opportunities to strengthen Namibia's AML/CFT/CPF framework and financial system integrity.

1.5 Limitations

- Not all suspicious or illicit financial activities are detected or reported, which results in possible under-reporting.
- Findings are based on information available during the reporting period and may not capture emerging risks after the reporting cut-off date.
- Certain operational and intelligence information cannot be disclosed due to confidentiality and legal restrictions.
- Historical data may be revised as additional information becomes available or analytical methodologies are updated.

The analysis presented in this report underscores the importance of a strong and adaptive AML/CFT/CPF framework in protecting Namibia's financial system from abuse. An informed understanding of ML/TF/PF risks is fundamental to safeguarding financial system integrity, strengthening transparency, and ensuring that financial institutions and other stakeholders remain resilient in the face of evolving threats. By supporting risk-based decision-making and evidence-based policy development, the report contributes to enhancing public confidence, international credibility, and the overall effectiveness of Namibia's efforts to combat financial crime.

2.1 Global financial crime landscape

Financial crime continues to pose a significant threat to global economic stability, financial integrity, national security, and sustainable development. The increasing interconnection of financial systems, growth in cross-border transactions, digitalisation of financial services, and rapid technological advancements have created new opportunities for criminals to move, conceal, and utilise illicit proceeds across jurisdictions. Criminal networks are becoming more sophisticated in exploiting vulnerabilities in financial systems, regulatory gaps, emerging technologies, and international trade channels to facilitate ML, TF, and PF.

According to international assessments conducted by the FATF, the United Nations, and other international organisations, financial crime is increasingly transnational in nature, involving multiple jurisdictions, complex ownership structures, virtual assets, shell companies, and professional facilitators. The proceeds generated from predicate offences are often integrated into the legitimate economy through various laundering methods, undermining financial stability, distorting markets, weakening governance, and facilitating further criminal activity.

Globally, several predicate offences continue to generate substantial illicit proceeds and remain key drivers of ML activities. These predicate offences include:

- **Corruption:** The abuse of entrusted power for private gain, including bribery, embezzlement, and procurement fraud, that generates significant illicit proceeds and undermines public institutions.
- **Drug trafficking:** The production, distribution, and sale of illicit drugs that generates substantial criminal profits, which are often laundered through formal and informal financial channels.
- **Human trafficking:** The exploitation of individuals for forced labour, sexual exploitation, or other forms of abuse that creates significant proceeds for organised criminal groups.

- **Cybercrime:** Technology-enabled crimes, such as ransomware attacks, phishing, identity theft, and online fraud, that continue to grow alongside digital financial services.
- **Tax crimes:** Activities aimed at evading tax obligations, including tax evasion and customs fraud, that result in significant revenue losses for governments.
- **Environmental crimes:** Illegal activities, such as wildlife trafficking, illegal mining, logging, and fishing, that generate substantial illicit profits while damaging natural resources.
- **Fraud and scams:** Financial deception schemes, including investment fraud, business email compromise, and online scams, that target individuals, businesses, and public institutions.¹

Understanding these global threats is critical for identifying emerging ML/TF/PF risks, strengthening preventive measures, and enhancing the effectiveness of Namibia's AML/CFT/CPF framework in protecting the integrity of the financial system.

2.2 Emerging global money laundering trends

ML methods continue to evolve in response to technological innovation, increased globalisation, and strengthened anti-money laundering (AML) frameworks. Criminals are continuously adapting their techniques to evade detection by exploiting weaknesses in financial systems, regulatory gaps, and emerging technologies. Recent international typology reports published by the FATF, the Egmont Group, and regional AML bodies indicate several emerging trends that present significant challenges to financial institutions, regulators, and law enforcement agencies worldwide.

¹Financial Action Task Force (FATF). (2022). International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation (The FATF Recommendations). Paris: FATF. (<https://www.fatf-gafi.org>).

Table 1: Summary of emerging global ML trends and financial stability implications

Emerging ML trend	Description	Common techniques	Key financial stability risks
 Trade-based money laundering	The exploitation of legitimate international trade transactions to disguise and transfer illicit funds across borders while concealing their criminal origin.	• Over- or under-invoicing of goods and services • Multiple invoicing • Falsified shipping documents • Misrepresentation of goods • Phantom shipments	• Weakens trade integrity • Facilitates cross-border illicit financial flows • Distorts international trade statistics • Challenges customs and financial supervision
 Shell companies	The use of legal entities with little or no genuine business activity to hide beneficial ownership and move illicit funds through the financial system.	• Hidden beneficial ownership • Offshore corporate structures • Layering through multiple jurisdictions • Nominee directors and shareholders	• Reduces corporate transparency • Facilitates corruption and tax evasion • Weakens customer due diligence • Increases financial system opacity
 Professional money laundering networks	Organised criminal networks that provide laundering services to multiple criminal organisations using sophisticated international financial structures.	• Front companies • Money mules • Cash-intensive businesses • Underground banking • International transfers • Virtual assets	• Supports organised crime • Enables large-scale laundering operations • Complicates criminal investigations • Requires international cooperation
 Abuse of virtual assets	The misuse of cryptocurrencies and virtual asset service providers (VASPs) to conceal, transfer, and launder criminal proceeds.	• Cryptocurrency wallets • Privacy coins • Blockchain transfers • Multiple digital wallets • Decentralised finance (DeFi) platforms • Cross-chain bridges	• Increased transaction anonymity • Rapid cross-border movement of funds • Regulatory challenges • Emerging cybercrime risks
 Complex layering schemes	Multiple financial transactions are designed to obscure the origin of illicit funds and conceal audit trails.	• Multiple electronic fund transfers • Cross-border banking transactions • Securities investments • High-value asset purchases • Trusts and corporate entities	• Reduces transaction transparency • Complicates financial investigations • Increases supervisory challenges • Weakens detection capabilities
 Use of FinTech platforms	The exploitation of digital financial services to rapidly move illicit funds across jurisdictions using innovative payment technologies.	• Digital payment applications • E-wallets • Peer-to-peer payments • Online lending • Digital remittances • Instant payment systems	• Faster movement of illicit funds • Remote onboarding risks • High transaction volumes • Increased AML/CFT/CPF compliance challenges

Figure 1: Evolution of emerging ML trends and AML/CFT/CPF responses

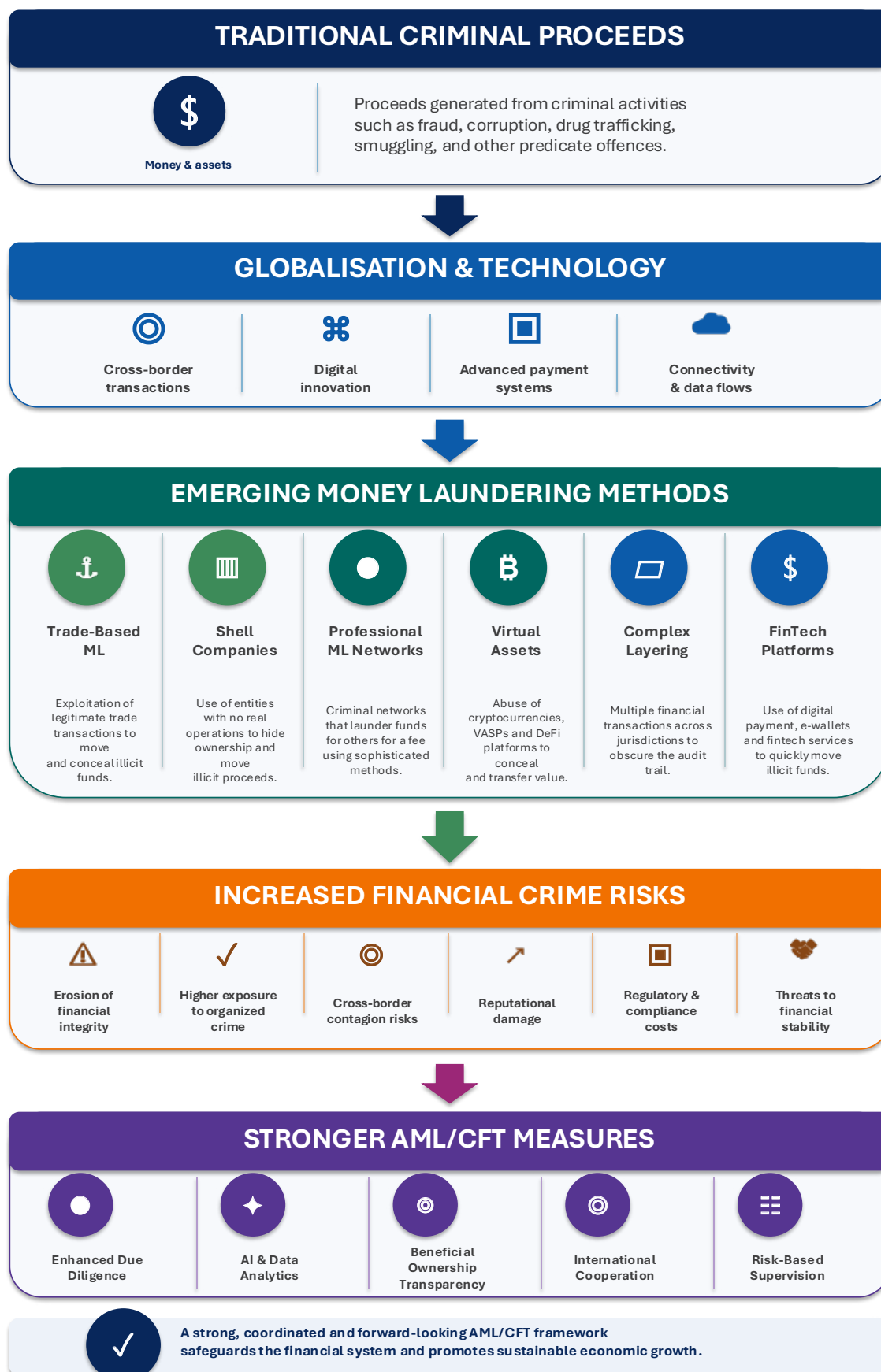


Figure 1 illustrates the evolution of ML from traditional predicate offences, such as fraud, corruption, and drug trafficking, to increasingly sophisticated methods facilitated by globalisation, digitalisation, and technological innovation. Criminals now exploit trade-based ML, shell companies, virtual assets, professional facilitators, and FinTech platforms to conceal illicit proceeds across jurisdictions, increasing risks to financial institutions and the integrity of the financial system.

These developments highlight the need for stronger AML/CFT/CPF measures, including enhanced customer due diligence, beneficial ownership transparency, advanced technology, international cooperation, and risk-based supervision to effectively detect and disrupt complex ML activities.²

2.2.1 Implications of money laundering on financial stability

These evolving ML typologies continue to increase risks to the integrity, transparency, and resilience of the global financial system. Financial institutions are expected to adopt risk-based AML/CFT/CPF measures, strengthen customer due diligence, enhance beneficial ownership transparency, improve transaction monitoring systems, and leverage advanced technologies, including artificial intelligence, to detect sophisticated laundering techniques.

Enhanced domestic and international cooperation among financial intelligence units, supervisory authorities, LEAs, and reporting entities remains critical in identifying emerging threats and safeguarding financial stability.

Table 2: Financial stability implications of emerging ML trends

Strategic area	Potential impact on financial stability
Financial system integrity	Criminal proceeds undermine confidence in financial institutions and reduce the integrity of the financial system. Further, it reduces stakeholder confidence which may directly impact foreign direct investments.
Transparency and beneficial ownership	Complex ownership structures and shell companies obscure the identity of beneficial owners, reducing market transparency, and abuse of corporate structures.
Cross-border financial flows	Illicit international transfers increase vulnerabilities within global payment systems and international trade.
Regulatory compliance	Financial institutions face increased compliance costs associated with customer due diligence, transaction monitoring, and sanctions screening.
Technological risks	Virtual assets, FinTech innovations, and digital payment platforms introduce new AML/CFT/CPF vulnerabilities that require enhanced supervisory approaches.
Operational risks	Sophisticated money laundering techniques increase the complexity of investigations and require advanced analytical tools, artificial intelligence, and skilled investigators.
International cooperation	Effective mitigation requires timely information sharing among FIUs, supervisory authorities, LEAs, and international partners.
Overall financial stability	Failure to effectively detect and prevent money laundering may weaken public confidence, expose institutions to reputational risks, increase systemic risks, and threaten the resilience of the financial sector.

2.3 Terrorist financing trends

Recent international assessments indicate that terrorist organisations are continuously adapting their financing methods to exploit technological advancements, globalisation, and weaknesses within financial systems.

Rather than relying solely on traditional funding sources, terrorist groups increasingly utilise a combination of formal and informal financial channels to raise, move, store, and distribute funds while avoiding detection. Table 3 outlines the trends that have emerged as significant TF risks to the integrity and stability of the global financial system.

² Egmont Group of Financial Intelligence Units. (2024). Egmont Group Annual Report 2023-2024. (<https://egmontgroup.org>).

Table 3: Emerging TF trends and financial stability implications

Emerging terrorist financing channel	How it is exploited	Key financial stability risks
 Informal value transfer systems	Terrorist organisations use informal remittance networks (e.g. hawala/informal money transfer system) to transfer funds across borders outside regulated financial institutions, often with limited documentation and oversight.	• Reduced transaction transparency • Difficult detection and tracing of funds • Increased cross-border financial vulnerabilities
 Crowdfunding platforms	Online fundraising campaigns may be disguised as humanitarian, charitable, or religious initiatives to solicit donations from supporters across multiple jurisdictions.	• Anonymous or small-value donations • Misuse of digital fundraising platforms • Challenges in monitoring illicit fundraising
 Virtual asset service providers	Cryptocurrencies, digital wallets, and DeFi platforms are used to receive, transfer, and store terrorist funds while attempting to conceal financial trails.	• Rapid cross-border transactions • Increased anonymity • Regulatory and supervisory challenges
 Non-profit organisations (NPOs)	Some NPOs may be abused through weak governance, poor financial controls, or operations in high-risk jurisdictions to divert charitable funds for terrorist purposes.	• Abuse of charitable donations • Reputational risks to the non-profit sector • Weak governance and oversight vulnerabilities
 Social media platforms	Social media is used to disseminate propaganda, recruit supporters, promote fundraising campaigns, and direct donations through digital payment channels and virtual asset wallets.	• Rapid global outreach • Online radicalisation and fundraising • Increased difficulty in identifying terrorist financing networks

2.3.1 Implications of terrorist financing on financial stability

The evolving TF landscape continues to present significant challenges to the stability and integrity of the financial system. Terrorist organisations increasingly exploit technological advancements, informal financial channels, virtual assets, and online platforms to raise, move, and conceal funds, making detection and prevention more complex.

These emerging methods expose financial institutions and other reporting entities to heightened risks and underscore the importance of adopting effective AML/CFT/CPF measures. Table 4 summarises the key implications of these emerging TF trends on financial stability and outlines the corresponding measures required to strengthen resilience and mitigate associated risks.³

³ Egmont Group of Financial Intelligence Units. (2024). *Egmont Group Annual Report 2023-2024*. (<https://egmontgroup.org>). Financial Action Task Force (FATF). (2023). *Crowdfunding for Terrorism Financing*. Paris: FATF. (<https://www.fatf-gafi.org>).

Table 4: Implications of emerging TF trends on financial stability

Area	Implications for financial stability	Recommended response
Financial system integrity	Emerging TF methods undermine the integrity, transparency, and resilience of the financial system.	Strengthen risk-based AML/CFT/CPF frameworks across all reporting entities.
Informal financial networks	Increased use of informal value transfer systems reduces transaction transparency and complicates detection.	Enhance monitoring of informal remittance channels and improve regulatory oversight
Digital fundraising and virtual assets	Online fundraising platforms and virtual assets facilitate rapid, anonymous, and cross-border movement of funds.	Implement enhanced due diligence, blockchain analytics, and monitoring of VASPs
Cross-Border financial risks	Cross-border transfers create greater exposure to terrorist financing and regulatory arbitrage.	Strengthen international cooperation and cross-border information sharing
Reporting entities	Financial institutions, VASPs, NPOs, and other reporting entities face elevated terrorist financing risks.	Apply robust customer due diligence, ongoing transaction monitoring, and timely suspicious transaction reporting
National and international cooperation	Limited information sharing reduces the ability to identify and disrupt emerging terrorist financing networks.	Enhance collaboration among FIUs, supervisory authorities, law enforcement agencies, and international partners
Overall financial stability	Failure to address evolving terrorist financing risks may weaken public confidence, increase systemic vulnerabilities, and threaten financial stability.	Maintain continuous risk assessments, intelligence-led supervision, and coordinated AML/CFT/CPF responses

2.4 Proliferation financing trends

Proliferation financing refers to the provision of funds or financial services used to support the proliferation of weapons of mass destruction, including nuclear, chemical, and biological weapons, and their means of delivery. As international sanctions and regulatory controls continue to tighten, proliferation networks are increasingly adopting sophisticated methods to procure restricted goods, disguise financial transactions, and evade detection. These evolving trends pose significant risks to the integrity of the financial system and require strengthened vigilance by financial institutions, supervisory authorities, and other reporting entities.

Key emerging PF trends include:

a) Complex trade networks

Risks:

- use of multiple intermediaries and transshipment routes;
- conceals the origin, destination, and end-user of goods; and
- renders suspicious financial flows difficult to detect.

Financial stability impacts:

- increases trade-based financial crime risks; and
- weakens transparency in cross-border trade.

b) Sanctions evasion

Risks:

- circumvention of international sanctions through shell companies, third-country intermediaries, and alternative payment methods; and
- conceals prohibited financial transactions.

Financial stability impacts:

- exposes financial institutions to regulatory, legal, and reputational risks; and
- undermines the effectiveness of sanctions regimes.

c) Front companies

Risks:

- Use of legitimate-looking businesses to disguise the true beneficiaries of transactions; and
- facilitates procurement and movement of restricted goods.

Financial stability impacts:

- reduces ownership transparency; and
- increases the risk of financial institutions unknowingly facilitating proliferation financing.

d) Dual-use goods procurement

Risks:

- acquisition of goods with both civilian and military applications; and
- procurement through complex supply chains to conceal the end-user.

Financial stability impacts:

- increases vulnerabilities within international trade finance; and
- complicates customer due diligence and transaction monitoring.

2.4.1 Implications of proliferation financing on financial stability

The evolving PF landscape poses significant risks to the integrity, transparency, and resilience of the financial system. The use of complex trade networks, front companies, sanctions evasion, and dual-use goods procurement increase financial, regulatory, and reputational risks while undermining international sanctions and trade integrity. Table 5 outlines the implications of PF on financial stability.⁴

Table 5: Implications of PF for financial stability

Area	Implications for financial stability	Recommended mitigation measures
Financial system integrity	Proliferation financing undermines the integrity, transparency, and resilience of the financial system.	Strengthen risk-based AML/CFT/CPF frameworks across all reporting entities
Complex trade networks	The misuse of complex trade routes and intermediaries obscures the origin, destination, and end-use of goods, increasing financial crime risks.	Enhance trade finance monitoring, verify trade documentation, and conduct risk-based trade assessments
Sanctions evasion	Evasion of international sanctions exposes financial institutions to legal, regulatory, operational, and reputational risks.	Implement robust sanctions screening, continuous monitoring, and enhanced customer due diligence
Front companies	Front companies conceal beneficial ownership and facilitate prohibited procurement and financial transactions.	Strengthen beneficial ownership verification and ongoing customer risk assessments
Dual-use goods procurement	The procurement of goods with both civilian and military applications increases vulnerabilities within trade finance and supply chains.	Apply enhanced due diligence to high-risk trade transactions and monitor procurement activities involving dual-use goods
International trade	Proliferation financing threatens the integrity of international trade and weakens the effectiveness of global sanctions regimes.	Improve cross-border cooperation, information sharing, and customs oversight
Reporting entities	Financial institutions, VASPs, DNFBPs, and other reporting entities face increased exposure to proliferation financing risks.	Adopt robust AML/CFT/CPF controls, strengthen transaction monitoring, and promptly report suspicious transactions
National and international cooperation	Weak coordination limits the ability to detect and disrupt proliferation financing networks.	Enhance collaboration among the FIC, supervisory authorities, customs agencies, LEAs, and international partners
Overall financial stability	Failure to effectively mitigate proliferation financing risks may reduce confidence in the financial system and increase systemic vulnerabilities.	Conduct continuous national risk assessments, strengthen supervisory oversight, and promote intelligence-led cooperation to safeguard financial stability

⁴ Financial Action Task Force (FATF). (2021). *Guidance on Proliferation Financing Risk Assessment and Mitigation*. Paris: FATF (<https://www.fatf-gafi.org>); FATF, 2021; FATF, 2024; United Nations Security Council, 2024.

The evolving global ML, TF, and PF landscape highlights the increasing complexity and interconnectedness of financial crime risks. These developments demonstrate that Namibia's financial system cannot be viewed in isolation from regional and international trends. Strengthening resilience against emerging threats such as virtual assets, trade-based money laundering,

sanctions evasion, and technologically enabled financial crime is essential to maintaining transparency, protecting financial institutions from abuse, and preserving confidence in Namibia's financial system. Continuous vigilance, international cooperation, and proactive risk management remain critical to sustaining credibility within the global financial architecture.



Financial system integrity implication: International AML/CFT/CPF trends and developments

Integrity implication: Global ML/TF/PF trends expose Namibia to cross-border risks, which could weaken transparency and financial confidence if not managed.

Effectiveness implication: Emerging risks require strong customer due diligence, beneficial ownership transparency, transaction monitoring, sanctions controls, and international cooperation.

Policy implication: Supervisors, policymakers, and reporting entities should strengthen preparedness for virtual assets, trade-based money laundering (TBML), sanctions evasion, and cross-border risks.



3.1 Economic overview

Namibia's economy plays a critical role in maintaining the stability and integrity of the country's financial system. The economy is driven by key sectors including mining, agriculture, fishing, manufacturing, tourism, financial services, and wholesale and retail trade, with increasing integration into regional and international markets. Continued economic activity, cross-border trade, foreign investment, and digital financial innovation have supported financial inclusion and economic growth. However, greater participation in the global financial system has also increased exposure to ML, TF, PF, fraud, corruption, cyber-enabled crime, and sanctions evasion risks. These threats have the potential to undermine confidence in the financial sector and affect Namibia's reputation within the international financial system.⁵

From a financial stability perspective, maintaining a resilient and transparent financial system requires a strong AML/CFT/CPF framework supported by effective supervision, risk-based compliance, and timely financial intelligence. Financial institutions, VASPs, DNFBPs, and other reporting entities play a critical role in detecting and reporting suspicious financial activities that may threaten financial stability.

The FIC, together with supervisory authorities, LEAs, and other competent authorities, continues to strengthen preventive measures, to enhance inter-agency cooperation, and to monitor emerging financial crime risks, safeguarding the integrity, resilience, and stability of Namibia's financial system while supporting sustainable economic development.

3.2 Geographic and demographic factors

Namibia's geographic location and demographic characteristics significantly influence its financial crime risk profile and the stability of its financial system. Strategically located in Southern Africa, Namibia shares borders with Angola, Botswana, South Africa, and Zambia, while its Atlantic coastline and the Port of Walvis Bay provide an important gateway for regional and international trade.

As a member of the Southern African Development Community (SADC) and the Common Monetary Area (CMA) payment ecosystem, Namibia facilitates substantial cross-border trade, investment, and financial flows. These economic linkages support regional integration, enhance market access, and contribute to national economic growth.⁶

The high volume of cross-border movement of goods, services, people, and capital also creates opportunities for ML, TF, PF, TBML, customs fraud, tax evasion, and sanctions evasion. Criminal networks may exploit trade corridors, cash movements, informal value transfer systems, shell companies, and complex supply chains to disguise the origin and destination of illicit funds. The increasing use of digital payment platforms and virtual assets further amplifies these risks by enabling rapid cross-border transactions with limited transparency if not adequately monitored.⁷

Namibia's relatively small population, combined with increasing financial inclusion and expanding access to digital financial services, has improved access to formal financial services while introducing new vulnerabilities to fraud, cyber-enabled financial crime, and the misuse of financial products. Reporting entities, including financial institutions, VASPs, and DNFBPs, must therefore apply risk-based customer due diligence, enhanced transaction monitoring, and effective sanctions screening, particularly for higher-risk cross-border customers and transactions.

From a financial stability perspective, effective management of geographic and demographic risks is essential to protecting the integrity and resilience of Namibia's financial system. The FIC, in collaboration with supervisory authorities, customs agencies, law enforcement, and regional and international counterparts, continues to strengthen information sharing, intelligence-led risk assessments, and cross-border cooperation to detect and disrupt illicit financial flows. These measures support the integrity of the financial sector, promote confidence in the financial system, and reinforce Namibia's compliance with international AML/CFT/CPF standards.⁸

3.3 Financial crime landscape

The FIC, through financial intelligence, STRs, stakeholder engagement, and national risk assessments, has identified several major predicate offences that generate illicit proceeds and pose significant risks to the integrity and stability of Namibia's financial system. These offences are commonly associated with ML and, in some cases, may facilitate TF or PF. Understanding these threats enables reporting entities and competent authorities to adopt targeted, risk-based AML/CFT/CPF measures.

⁵ Bank of Namibia. (2024). *Annual Report 2024*. Windhoek: Bank of Namibia; International Monetary Fund. (2024). 2024 Article IV Consultation – Namibia: Staff Report. Washington, DC: International Monetary Fund.

⁶ Southern African Development Community (SADC). (2024). *SADC Regional Indicative Strategic Development Plan (RISDP) 2020-2030*. Gaborone: SADC Secretariat.

⁷ Financial Action Task Force (FATF). (2020). *Trade-based Money Laundering: Trends and Developments*. Paris: FATF.

⁸ Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG). (2023). *ESAAMLG Annual Report 2022-2023*. Dar es Salaam: ESAAMLG.

Figure 2: Namibia's major predicate offences and their impact on financial stability

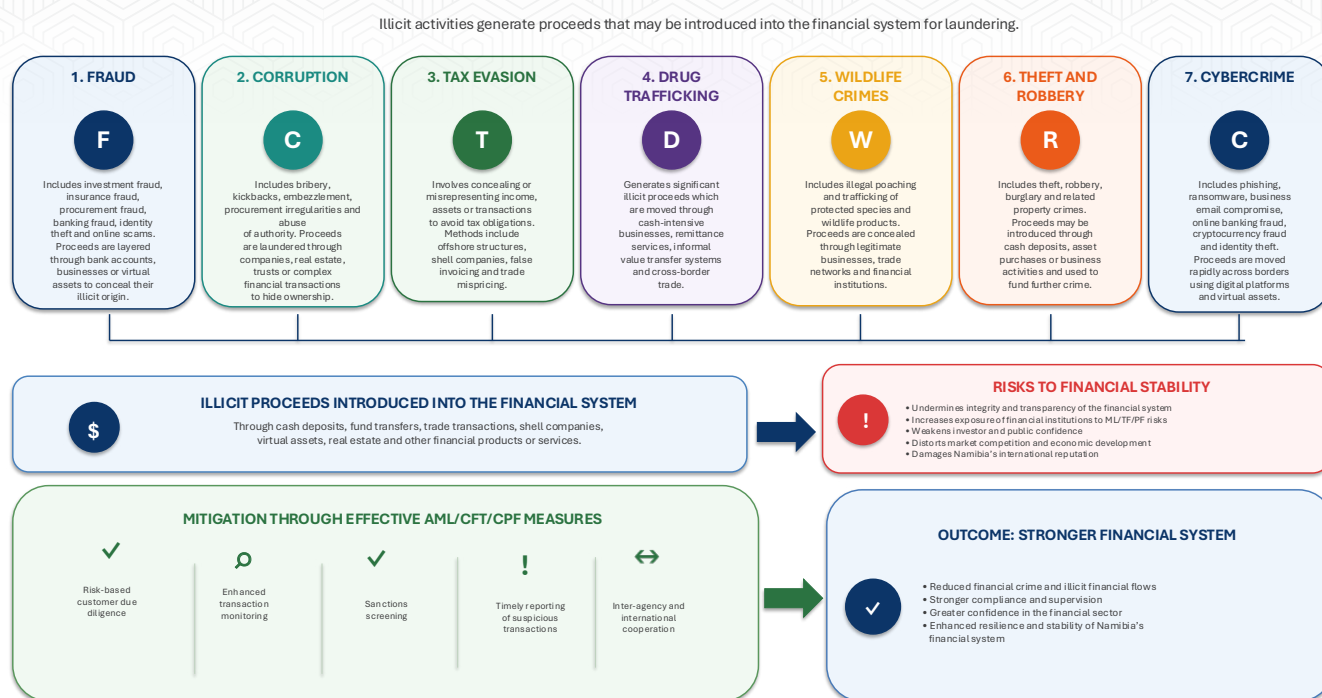


Figure 2 illustrates how major predicate offences including fraud, corruption, tax evasion, drug trafficking, wildlife crimes, theft and robbery, and cybercrime generate illicit proceeds that are introduced into the financial system through various channels, such as bank accounts, trade transactions, shell companies, real estate, and virtual assets. These activities increase exposure to ML/TF/PF risks, undermining the integrity, transparency, and resilience of Namibia's financial system. The figure further demonstrates that effective risk-based AML/CFT/CPF measures are essential to mitigating these threats. Enhanced customer due diligence, transaction monitoring, sanctions screening, timely suspicious transaction reporting, and strong cooperation among the FIC, supervisory authorities, LEAs, and international partners are critical to detecting illicit financial flows, protecting financial institutions, and safeguarding Namibia's financial stability.

Namibia's economic structure, strategic geographic position, growing connectivity to international markets, and emerging industries present both opportunities and vulnerabilities for financial crime exploitation. The presence of predicate offences such as fraud, corruption, tax crimes, wildlife crime, and cyber-enabled crime reinforces the need for robust preventative and detection measures. As Namibia prepares for increased economic activity, including developments in the oil and gas sector, protecting financial system integrity will require strengthened transparency, enhanced risk management, and effective mitigation of illicit financial flows. Failure to adequately address these risks could undermine investor confidence, economic growth, and the long-term credibility of the financial sector. Conversely, effective risk-based controls will strengthen resilience and reinforce Namibia's position as a trusted financial jurisdiction.



Financial system integrity implication: Namibia's economic and crime landscape

Integrity implication: Namibia's economy, geography, trade links, and crime landscape create vulnerabilities that may be exploited to move or conceal illicit proceeds.

Effectiveness implication: Predicate offences such as fraud, corruption, tax crimes, wildlife crimes, and cybercrime reinforce the need for stronger detection and enforcement.

Policy implication: Priorities should continue to include enhanced risk assessments, beneficial ownership transparency, inter-agency cooperation, and supervision of emerging sectors such as oil and gas.

CHAPTER

04

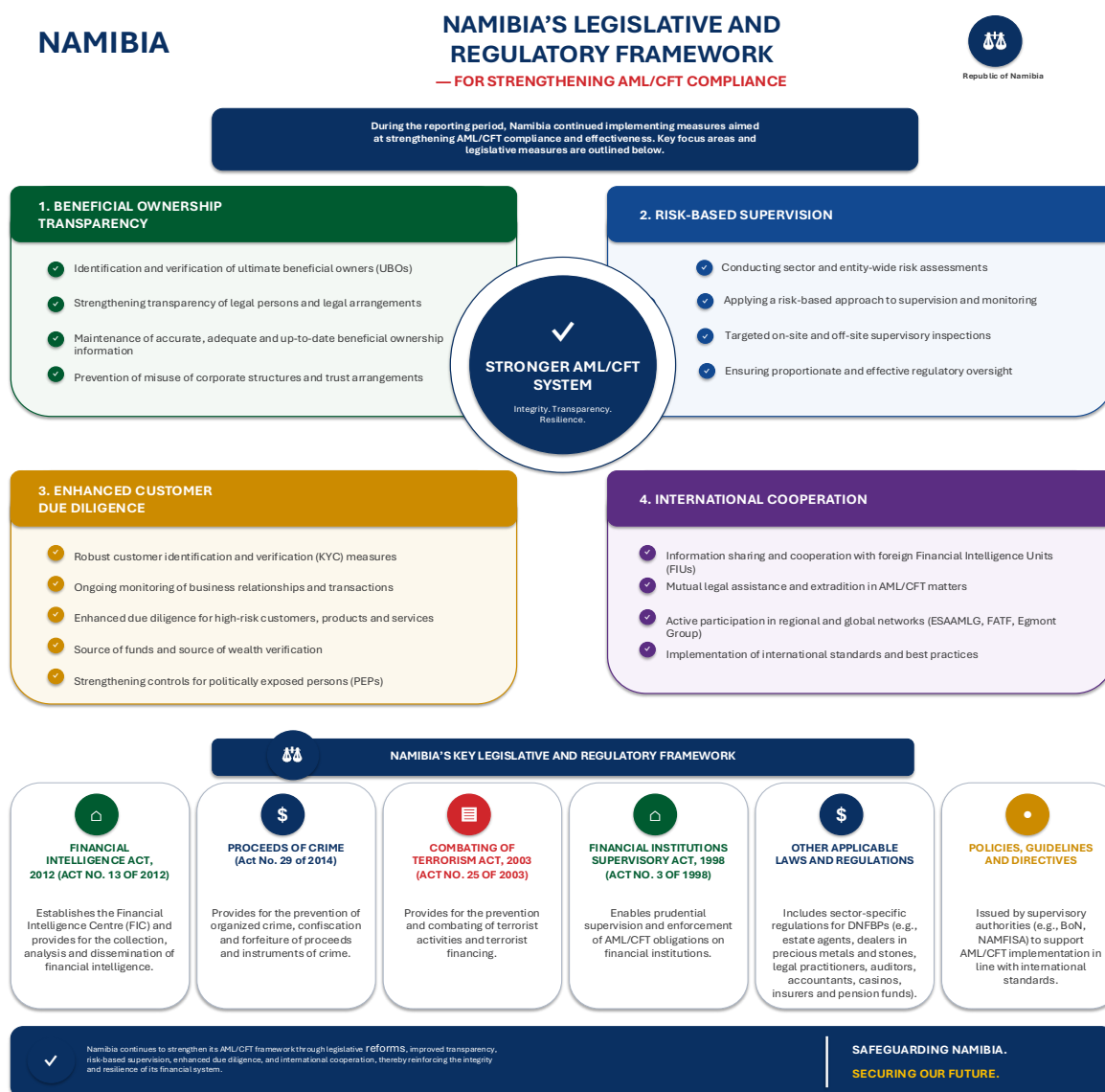
DOMESTIC AML/CFT/CPF DEVELOPMENTS

4.1 Legislative developments

During the reporting period, Namibia continued to strengthen its AML/CFT/CPF framework through legislative, regulatory, and institutional reforms. These developments are aimed at enhancing the effectiveness of the national AML/CFT/CPF regime, addressing risks identified through national risk assessments, and maintaining compliance

with the international standards set by the FATF and regional commitments. The reforms also support the integrity, resilience, and stability of Namibia's financial system by improving transparency, strengthening supervision, and enhancing cooperation among competent authorities. Namibia continued to implement measures aimed at strengthening AML/CFT/CPF compliance and effectiveness. Key focus areas and legislative measures are outlined in Figure 3.

Figure 3: AML/CFT/CPF compliance: Namibia's legislative and regulatory framework



4.2 Institutional developments

Namibia continued to strengthen its institutional AML/CFT/CPF framework through enhanced cooperation, effective information sharing, improved analytical capabilities, and higher-quality reporting. These developments have increased the

country's capacity to detect, investigate, and prevent financial crime while supporting compliance with international AML/CFT/CPF standards and reinforcing the integrity of the financial system. Table 6 provides a summary of the key outcomes for institutional developments that were observed.

Table 6: Summary of key outcomes for institutional developments

Institutional development		Key outcomes
	Improved inter-agency cooperation	Strengthened collaboration among the FIC, law enforcement, supervisory authorities, customs, tax authorities, and prosecutors has enhanced coordinated investigations and the national response to financial crime.
	Enhanced information sharing	The timely exchange of financial intelligence and regulatory information among domestic and international authorities has improved risk identification, investigations, and cross-border cooperation.
	Strengthened analytical capabilities	Investment in analytical tools, data systems, and staff capacity has improved the detection of complex money-laundering and terrorist financing activities and strengthened intelligence-led decision-making.
	Improved reporting quality	Better compliance programmes, customer due diligence, and reporting practices have resulted in more accurate, complete, and actionable STRs, enhancing financial intelligence analysis and enforcement outcomes.

4.3 Technological developments

Technological advancements continue to reshape Namibia's financial sector by improving the efficiency, accessibility, and security of financial services. The increasing adoption of digital banking, mobile payment platforms, electronic wallets, and automated transaction monitoring systems has enhanced financial inclusion and operational efficiency while supporting innovation across the financial sector.

At the same time, these technologies have expanded the digital risk landscape, requiring financial institutions to strengthen cybersecurity, AML/CFT/CPF controls, and transaction monitoring to effectively detect and mitigate emerging financial crime risks. Consequently, financial institutions and other reporting entities are expected to strengthen technology-driven AML/CFT/CPF controls to safeguard the integrity, resilience, and stability of Namibia's financial system. Table 7 outlines the technological developments adopted and implemented by various institutions.

Table 7: Technological developments adopted and implemented by institutions

Technological Development	Key Points
 Digital Banking	Expanded access to banking services through online platforms, enabling customers to perform transactions remotely while improving convenience and operational efficiency.
 Mobile Payments	Increased use of mobile payment platforms facilitated faster, secure, and more accessible financial transactions, contributing to greater financial inclusion
 Electronic Wallets (E-Wallets)	Growing adoption of electronic wallets provided convenient cashless payment solutions and supported digital financial transactions across various sectors.
 Automated Monitoring Systems	Financial institutions enhanced AML/CFT compliance through automated transaction monitoring systems capable of detecting unusual or suspicious transaction patterns in real time, improving risk management and reporting effectiveness.

4.4 Namibia's removal from the FATF grey list

Namibia was placed on the FATF List of Jurisdictions under 'Increased Monitoring (grey list)' in February 2024 after strategic deficiencies were identified in the effectiveness of its AML/CFT/CPF framework. Following its grey-listing, Namibia implemented a comprehensive action plan, which was developed in collaboration with the FATF and ESAAMLG. The action plan focused on strengthening risk-based supervision; improving beneficial ownership transparency; enhancing financial intelligence; increasing the effectiveness of ML, TF, and PF investigations and prosecutions; implementing targeted financial sanctions; and improving cooperation among competent authorities. As a result of sustained efforts by the Government of Namibia, the FIC, supervisory authorities, LEAs, prosecutors, and reporting institutions, Namibia successfully addressed the identified strategic deficiencies.

The FATF subsequently recognised the country's progress and removed Namibia from the grey list on 19 June 2026. This achievement reflects Namibia's commitment to implementing international AML/CFT/CPF standards and strengthening the effectiveness of its financial crime prevention framework. Namibia's removal from the grey list has reinforced confidence in the country's financial system, enhanced its international reputation, and reduced the risk of increased due diligence

by foreign financial institutions and correspondent banking partners. Nevertheless, maintaining this progress will require continued implementation of risk-based supervision, effective enforcement, high-quality financial intelligence, and ongoing cooperation between public and private sector stakeholders to ensure sustained compliance with FATF Standards and to safeguard the integrity and stability of Namibia's financial system.

The legislative, institutional, and technological developments highlighted in this chapter demonstrate Namibia's unwavering commitment to continuously strengthening its AML/CFT/CPF framework. Significant reforms, including the enactment and amendment of key AML/CFT/CPF legislation and the successful implementation of measures that enabled Namibia to address all FATF action items and exit the FATF grey list ahead of the anticipated timeframe, reflect the country's strong commitment to financial system integrity and international compliance standards. These achievements, together with enhanced cooperation among stakeholders, improved information sharing, stronger analytical capabilities, and ongoing regulatory reforms, have collectively contributed to a more transparent, resilient, and effective financial system.

From a financial system integrity perspective, these advancements have strengthened Namibia's ability to detect, deter, and disrupt financial crime; reduce vulnerabilities; enhance transparency; and curb illicit financial flows. They have also reinforced the credibility of Namibia's financial system, both domestically and internationally, helping to preserve investor confidence and strengthen the country's reputation as a trusted and responsible participant in the global financial system.

Ultimately, sustained investment in institutional effectiveness, innovation, and risk-based reforms remains essential to maintaining public trust and safeguarding the integrity, resilience, and long-term stability of Namibia's financial system as the country prepares for the next National Risk Assessment (NRA) and the 2030 Mutual Evaluation.



Financial system implication: AML/CFT/CPF developments

Integrity implication: Legal, institutional, and technological reforms, including progress that supported Namibia's exit from enhanced monitoring, strengthen confidence and credibility.

Effectiveness implication: These reforms improve Namibia's ability to detect, prevent, supervise, and respond to financial crime in line with international standards.

Policy implication: Stakeholders should sustain reforms, strengthen supervision, leverage technology, reduce illicit financial flows, and prepare for the next NRA and 2030 Mutual Evaluation.

CHAPTER

05

FINANCIAL INTELLIGENCE DATA OVERVIEW

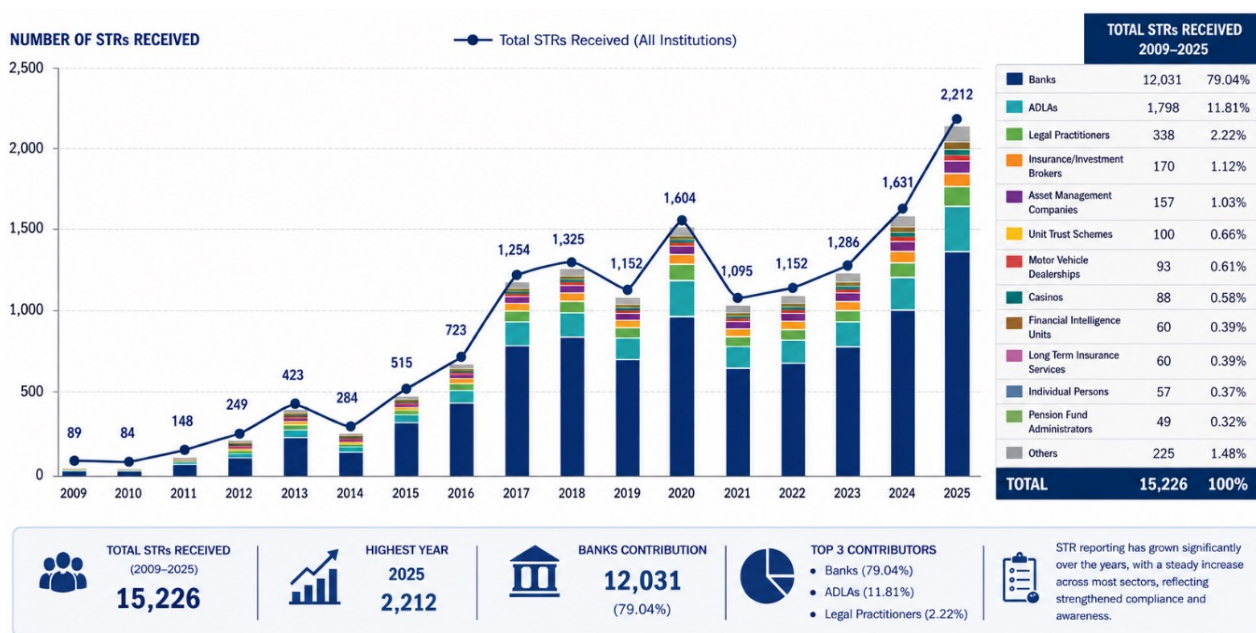
5.1 Data overview from the FIC

The FIC is mandated to receive, collect, analyse, and disseminate financial intelligence to combat ML, TF, PF, and related financial crimes. The FIC receives regulatory reports from accountable and reporting institutions through its reporting platforms, analyses these reports together with information from domestic and international partners, and disseminates actionable intelligence to

competent authorities. In addition to operational analysis, the FIC produces strategic analysis to identify emerging risks, trends, and typologies that inform national AML/CFT/CPF policy and risk mitigation measures.

This section presents the key statistics derived from the FIC's databases during the reporting period. The analysis provides an overview of reporting trends, financial intelligence products, and indicators of ML/TF/PF risks from inception to 31 December 2025.

Figure 4: STRs received from reporting sectors per annum



Note: ADLAs – Accountable and Designated Non-Financial Businesses and Professions

The FIC received a total of 15,226 STRs during the review period. Annual reporting increased significantly from 89 reports in 2009 to a record 2,212 reports in 2025. Although there were slight declines in 2019 and 2021, the overall trend in Figure 4 shows a sustained growth in reporting, reflecting strengthened AML/CFT/CPF compliance, enhanced awareness of reporting obligations, and improved suspicious transaction monitoring across reporting institutions.

The banking sector remained the primary source of STRs, submitting 12,031 reports (79.0%) of all the STRs received, followed by authorised dealers with limited authority (ADLAs) with 1,798 reports (11.8%).

Other reporting institutions, including legal practitioners, insurance and investment brokers, asset management companies, and unit trust schemes, also contributed to the reporting landscape, demonstrating increasing participation across both financial and designated non-financial sectors. Overall, the upward reporting trend indicates continued strengthening of Namibia's AML/CFT/CPF regime and an enhanced ability to detect and report suspicious financial activities.

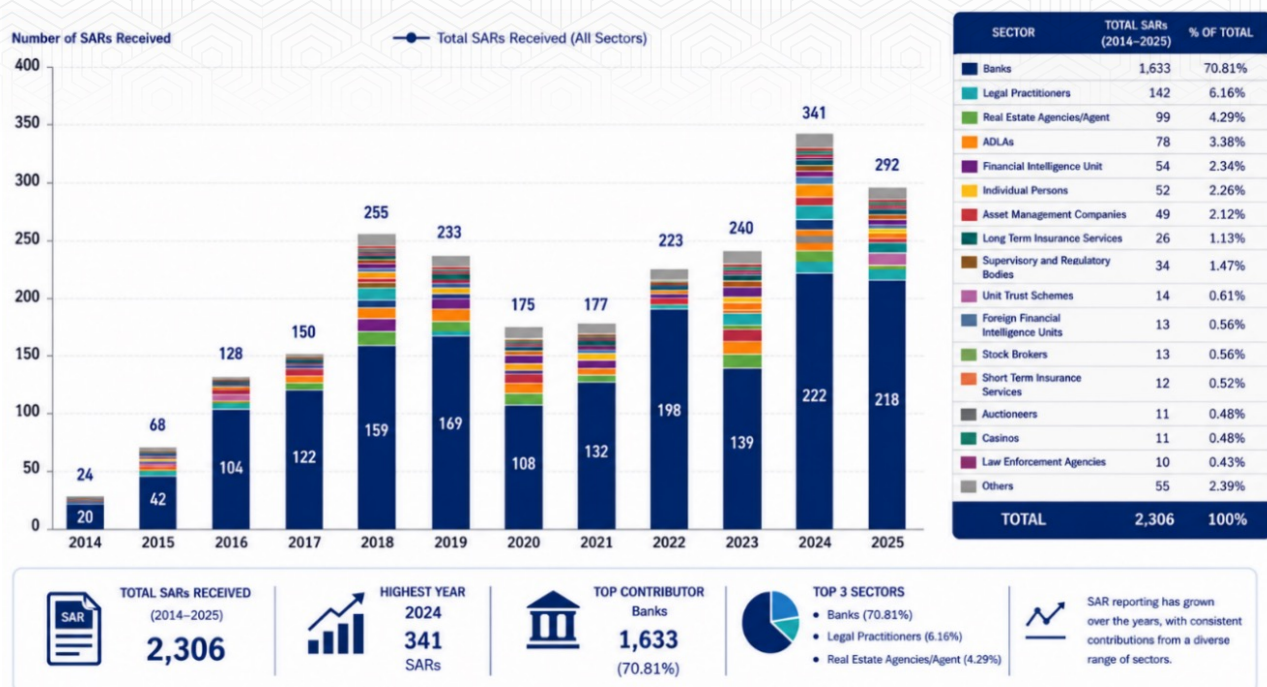
Table 8: Categorisation of STRs by analysis outcome

Year	Case files opened	Low priority	Medium priority	Set aside	Total STRs
2009	75	-	-	14	89
2010	79	-	-	5	84
2011	144	-	-	4	148
2012	234	11	-	4	249
2013	206	210	-	7	423
2014	128	152	-	4	284
2015	173	340	-	2	515
2016	220	490	-	13	723
2017	290	947	-	17	1,254
2018	262	1,056	-	7	1,325
2019	189	957	-	6	1,152
2020	320	1,270	-	14	1,604
2021	212	881	-	2	1,095
2022	261	888	54	3	1,152
2023	150	1,082	409	0	1,286
2024	94	1,127	407	1	1,631
2025	149	1,656	870	-	2,212
Total	3,186	11,067	870	103	15,226

Using a risk-based approach, the FIC assessed 15,226 STRs during the review period. Of these, 11,067 reports were classified as low priority, 3,186 (20.9%) were escalated into case files for further analysis, 870 were assessed as medium priority, and 103 were set aside during the reporting period. The introduction of the medium-priority category in 2022 demonstrates the continued evolution of the FIC's risk-based assessment methodology, enabling more effective prioritisation of reports according to their intelligence value and associated risks.

While the number of case files opened fluctuated over the years, the trend reflects the application of more targeted analytical processes rather than changes in criminal activity. Overall, the findings indicate that the FIC has strengthened its capacity to assess increasing volumes of STRs efficiently, ensuring that analytical resources are directed toward reports posing the greatest ML/TF/PF risks.

Figure 5: SARs received from reporting sectors per annum



From inception to 31 December 2025, the FIC received 2,306 SARs, and reporting generally increased over the period. Annual SARs rose from 24 in 2014 to a peak of 341 in 2024, before declining slightly to 292 in 2025, indicating a sustained improvement in SARs.

The banking sector remained the largest contributor, submitting 1,633 SARs (70.8%), followed by legal practitioners with 142 and real estate agencies/agents with 99. The increasing contributions from a wider range of reporting sectors demonstrate strengthened AML/CFT/CPF compliance, enhanced awareness of reporting obligations, and improved detection of suspicious activities across Namibia's financial and non-financial sectors.

Table 9: Categorisation of SARs by analysis outcome

Assessment outcome	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	Total	Percentage (%)
Case file opened	5	22	56	61	81	103	69	58	38	25	31	54	603	26.1
Low priority	19	45	70	89	172	127	105	119	185	215	310	238	1,694	73.4
Set aside	–	1	2	–	2	3	1	–	–	–	–	–	9	0.4
Total	24	68	128	150	255	233	175	177	223	240	341	292	2,306	100.0%

The FIC analysed a total of 2,306 SARs during the review period. Of these, 603 reports (26.1%) warranted the opening of case files for further financial intelligence analysis, and 1,694 reports (73.4%) were analysed as low priority, indicating that they did not present sufficient intelligence value or immediate indicators of ML, TF, PF, or related financial crimes. Only 9 SARs (0.4%) were set aside, reflecting instances where reports could

not proceed due to duplication, insufficient information, or other administrative reasons.

Overall, the assessment outcomes demonstrate a risk-based approach, whereby only reports with sufficient intelligence value are escalated for detailed analysis and the majority are screened out as lower risk.

Table 10: Cross-border movement of cash reports received from sectors

Reporting Sector	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	Total
Law enforcement agencies	7	66	12	11	3	36	68	70	10	1	284
Banks	–	1	–	2	–	–	–	–	–	–	3
Legal practitioners	–	–	–	1	–	2	–	–	–	–	3
Casinos	–	–	–	1	–	–	–	1	–	–	2
Short-term insurance services	–	–	1	–	–	–	–	–	–	–	1
Total reports	7	67	13	15	3	38	68	71	10	1	293

The FIC received a total of 293 cross-border movement of cash reports (CBMCRs) from reporting sectors during the review period. LEAs were by far the largest contributors, submitting 284 reports (96.9%), demonstrating their central role in identifying and reporting cross-border cash movements at Namibia's ports of entry and exit. The remaining 9 reports (3.1%) were submitted collectively by other reporting sectors, including banks (3 reports; 1.0%), legal practitioners (3 reports; 1.0%), casinos (2 reports; 0.7%), and short-term insurance services (1 report; 0.3%).

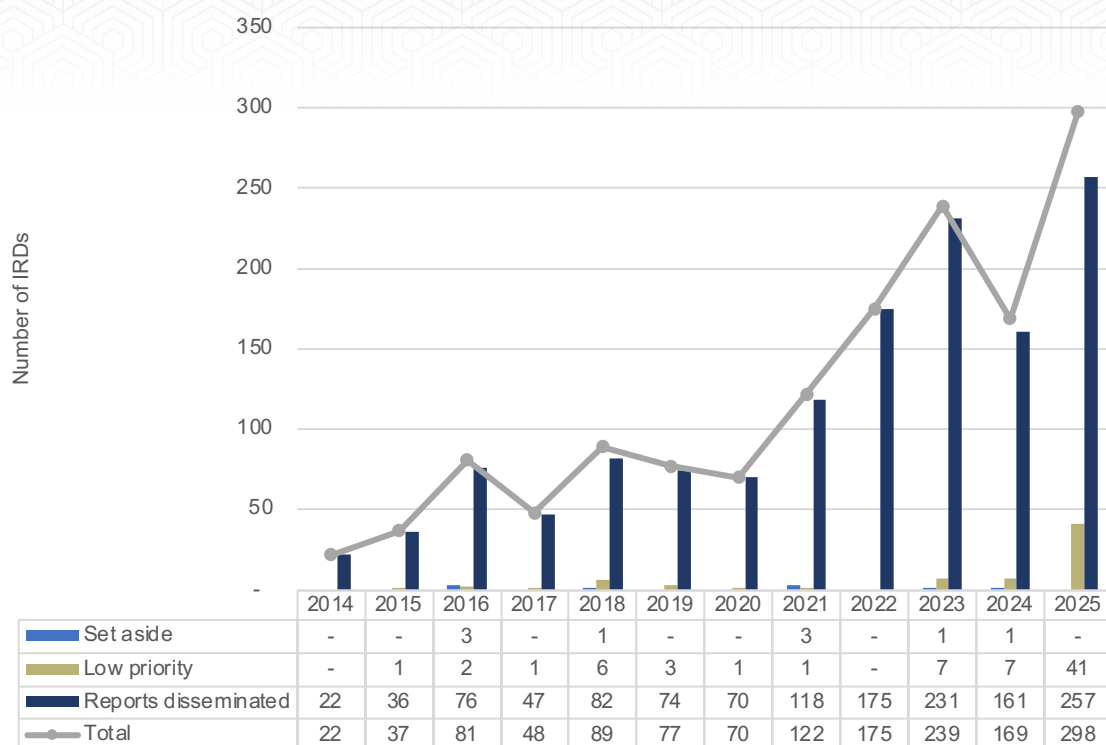
Annual reporting fluctuated over the reporting period, with notable peaks in 2023 (71 reports; 24.2% of all reports), 2022 (68 reports; 23.2%), and 2017 (67 reports; 22.9%). Together,

these three years accounted for 206 reports (70.3%) of all the CBMCRs received. Reporting declined significantly thereafter, with only 10 reports (3.4%) received in 2024 and 1 report (0.3%) in 2025.

The overwhelming contribution from LEAs highlights their critical role in enforcing cross-border cash declaration requirements. At the same time, the very limited reporting from other sectors suggests that the detection and reporting of cross-border cash movements remain highly dependent on law enforcement, underscoring the importance of continued inter-agency cooperation, intelligence sharing, and enhanced awareness among other reporting institutions where cross-border cash-related risks may be identified.



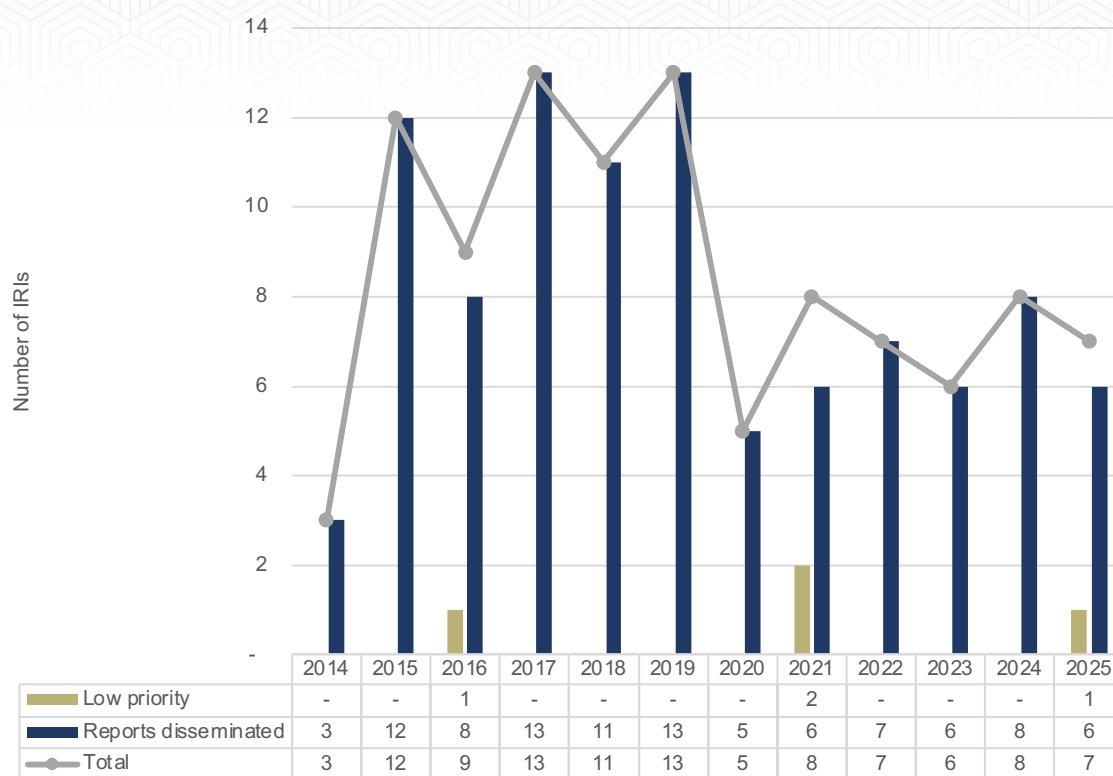
Figure 6: Incoming requests domestic received per annum



From 2014 to 2025, the FIC recorded 1,427 incoming requests domestic (IRDs), of which 1,349 (94.5%) were disseminated, only 70 (4.9%) were classified as low priority, and 9 (0.6%) were set aside. The number of IRDs increased significantly from 22 in 2014 to 298 in 2025, indicating a growing demand for financial intelligence and an expanded role of the FIC in supporting competent authorities.

The consistently high dissemination rate demonstrates that most requests were considered relevant and actionable, while the increase in low-priority cases in 2025 highlights the need for continued risk-based prioritisation and efficient allocation of analytical resources.

Figure 7: Incoming requests international received per annum



The FIC received 102 incoming requests international (IRIs) between 2014 and 2025. Of these, 98 (96.1%) resulted in reports being disseminated and only 4 (3.9%) were classified as low priority. IRI volumes fluctuated over the period, ranging from three requests in 2014 to a peak of 13 in both 2017 and 2019, before declining in subsequent years. The consistently high dissemination rate indicates that the majority of the IRIs were considered relevant and actionable, demonstrating the FIC's active role in international information exchange and cooperation with foreign FIUs in support of ML, TF, PF, and related financial crime investigations.

5.2 Summary of key observations

The FIC statistics provide valuable insights into reporting trends, the effectiveness of the AML/CFT/CPF Framework, and the evolving risk landscape in Namibia. The key observations presented in the following table highlight notable developments in reporting patterns, reporting quality, sectoral contributions, and transaction monitoring. These findings support the assessment of the country's financial system's integrity and demonstrate areas where compliance and financial intelligence capabilities have strengthened over the reporting period.

Table 11: Summary of key observations as per FIC statistics

Key Observation	FIC Statistics (Trend/Evidence)	Interpretation	Impact
 REPORTING VOLUMES INCREASED	- Steady increase in STRs/SARs over the years. - STRs received increased from 1,205 in 2015 to 3,049 in 2024. - Average annual growth rate of 10.7%.	Increased awareness, better compliance and enhanced reporting systems have contributed to a consistent rise in reporting by accountable institutions and DNFBPs.	Enhances the FIC's ability to detect, analyze and disseminate financial intelligence for effective risk mitigation.
 REPORTING QUALITY IMPROVED	- Higher proportion of actionable reports. - Increase in reports escalated to case files: from 391 in 2015 to 919 in 2024. - Improved completeness and relevance of information provided.	Improved compliance frameworks, training, and feedback engagements have enhanced the quality and usefulness of reports submitted to the FIC.	More actionable intelligence supports better- informed investigations and prosecutions.
 BANKING SECTOR REMAINED DOMINANT CONTRIBUTOR	- Banking sector consistently submitted the highest number of STRs. - In 2024, banks accounted for 93% (2,839) of total STRs.	Banks continue to have stronger systems, larger customer bases, and higher transaction volumes, leading to more detections and reporting.	Reflects strong compliance culture in the banking sector and its critical role in the AML/CFT regime.
 CROSS-BORDER TRANSACTION MONITORING INCREASED	- Cross-border cash reports increased from 29 in 2016 to 71 in 2023. 96.9% of cross-border cash reports received from Law Enforcement Agencies.	Enhanced monitoring at borders, stronger inter- agency collaboration and risk-based controls have led to increased detection and reporting of cross-border movements.	Improves Namibia's ability to identify cross- border risks and contributes to regional and international cooperation.

The reporting and intelligence trends presented in this chapter indicate significant progress in Namibia's ability to identify, report, analyse, and respond to suspicious financial activity. Growing reporting volumes, increased engagement by reporting institutions, and the continued use of financial intelligence in supporting domestic and international cooperation reflect the maturation of Namibia's AML/CFT/CPF framework. At the same time, the data underscores the importance of

continuously improving reporting quality, analytical capabilities, and stakeholder participation to ensure that emerging risks are effectively identified and addressed.

Overall, these trends enhance transparency, strengthen resilience against financial crime, support the reduction of illicit financial flows, and reinforce confidence in the integrity and credibility of Namibia's financial system.



Financial system integrity implication

Integrity implication: Growth in STRs, SARs, and financial intelligence use reflects stronger compliance culture, transparency, and vigilance across the financial system.

Effectiveness implication: The data shows improved detection, cooperation, and risk-based analysis, and highlights the need to improve reporting quality and sector participation.

Policy implication: Priorities should include feedback, better data quality, broader reporting participation, and greater use of financial intelligence for operational and strategic outcomes.



6.1 Overview

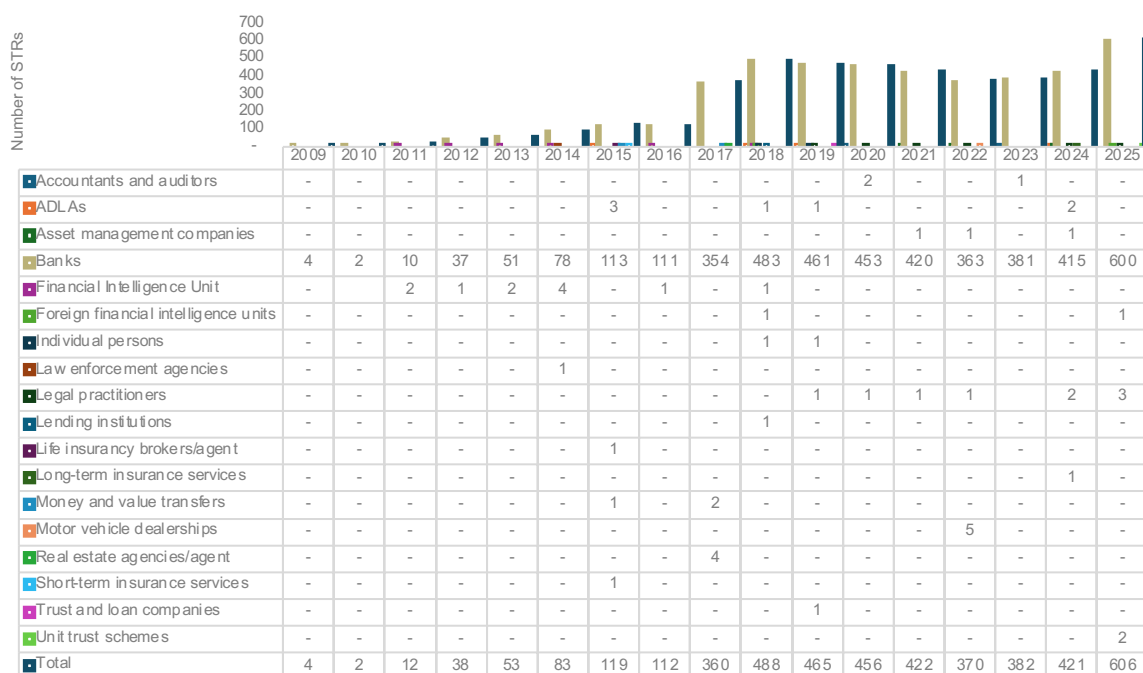
This section provides a comprehensive analysis of the financial intelligence collected by the FIC during the reporting period. Generally, this section examines key ML/TF/PF risks, identifies emerging trends and vulnerabilities, and evaluates how these threats affect the integrity and stability of Namibia's financial system. The analysis draws on the most potential predicate offences such as tax, fraud, and corruption reports filed to the FIC by various sectors to identify significant patterns, typologies, and areas that require enhanced AML/CFT/CPF controls.

6.2 Potential tax-related offence trends

Potential tax-related offences remain an important area of analysis within Namibia's AML/CFT/CPF framework, as tax evasion and associated financial crimes can generate illicit proceeds that are subsequently laundered through the financial system. Analysis of STRs and other financial intelligence enables the FIC to identify trends, emerging typologies, and sectors vulnerable to tax-related offences, thereby supporting competent authorities in detecting, investigating, and mitigating risks to the integrity and stability of the financial system.

This section provides statistical reports related to potential tax-related offences received from various sectors from inception to 31 December 2025.

Figure 8: STRs related to potential tax offences received from sectors

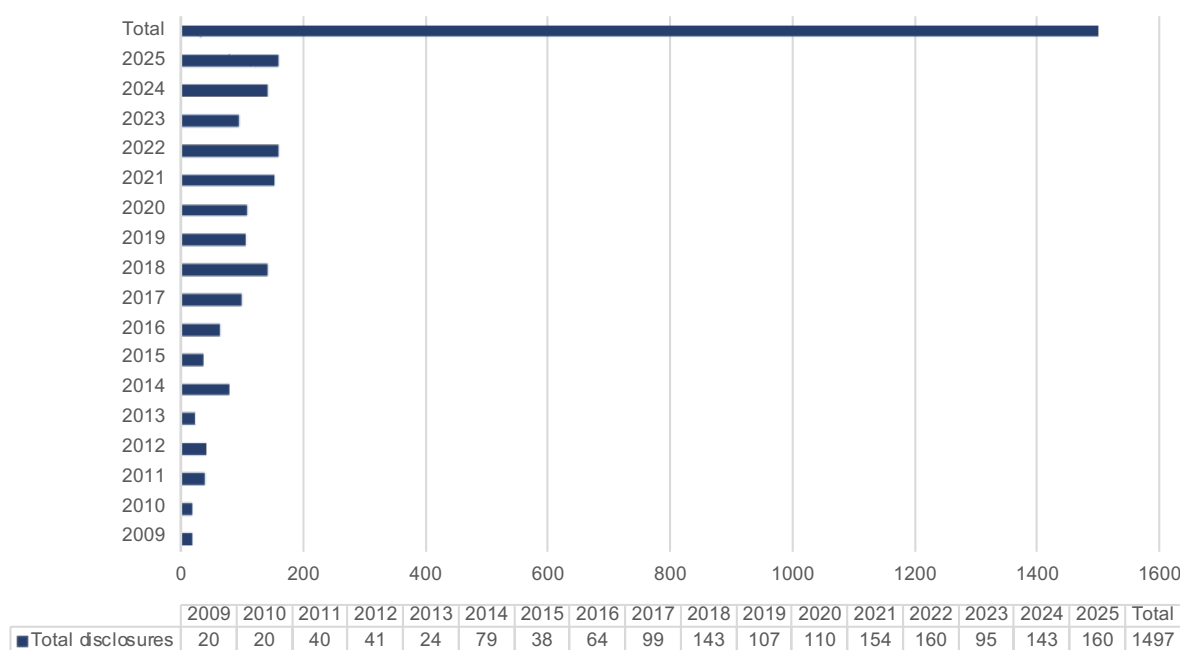


The FIC received 4,393 STRs relating to potential tax-related offences as at 31 December 2025. Banks submitted 4,336 STRs (98.7%), demonstrating that the banking sector is the primary source of intelligence on potential tax-related offences.

All other reporting sectors collectively accounted for 57 STRs (1.3%). The largest contributions came from the Financial

Intelligence Unit with 11 STRs, legal practitioners with 9 STRs, and ADLAs with 7 STRs. These findings indicate that banks remain the most effective sector for detecting suspicious financial activity linked to potential tax-related offences, reflecting their extensive customer base, transaction monitoring capabilities, and AML/CFT/CPF compliance obligations.

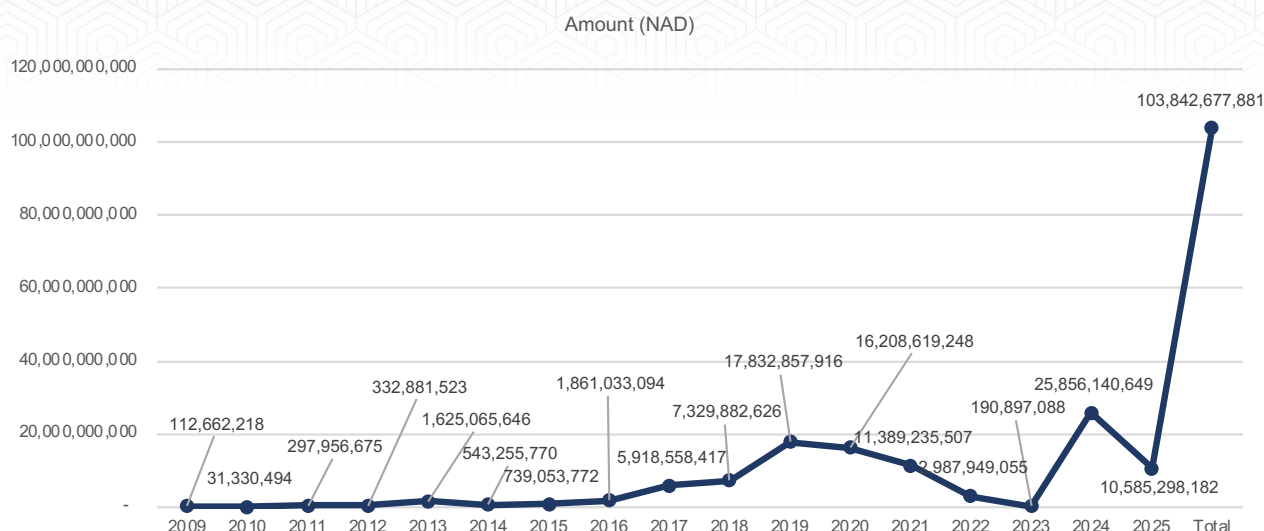
Figure 9: Tax-related offences: spontaneous disclosures to NamRA per annum



In total, the FIC has made 1,497 spontaneous disclosures to the Namibia Revenue Agency (NamRA) with regard to potential tax-related offences. The number of disclosures generally increased over the reporting period, rising from 20 disclosures in 2009 to 160 disclosures in both 2022 and 2025, reflecting enhanced financial intelligence analysis, stronger cooperation between the FIC and NamRA, and an increased focus on identifying suspected tax-related offences.

Although disclosure volumes have fluctuated in some years, the overall upward trend demonstrates the FIC's growing role in supporting tax compliance and detecting financial crimes linked to tax offences. The sustained increase in disclosures since 2017 indicates improved identification and dissemination of actionable financial intelligence, thereby strengthening NamRA's capacity to investigate potential tax offences and contributing to the integrity and resilience of Namibia's financial system.

Figure 10: Potential tax offence values per annum



The FIC identified transactions linked to potential tax-related offences with a cumulative value of approximately N\$103.84 billion. The annual value of these transactions generally increased over the reporting period, with notable peaks in 2024 (N\$25.86 billion), 2019 (N\$17.83 billion), and 2020 (N\$16.21 billion).

Although values fluctuated from year to year, the consistently high transaction amounts in recent years indicate continued exposure to significant tax-related financial crime risks and highlight the critical role of financial intelligence and inter-agency cooperation in detecting and addressing potential tax offences.

6.2.1 Various reasons for reporting transactions as suspicious

Reporting entities are required to provide grounds for suspicion when submitting STRs and SARs to the FIC, identifying the suspected offence and the indicators that gave rise to the suspicion. These grounds are based on observed red flags, transaction patterns, and other risk indicators that assist the FIC in analysing suspicious activities.

The following section highlights key observations from case studies and the predominant methods and indicators associated with potential tax-related offences identified during the reporting period.

Table 12: Potential tax-related offence typologies and indicators by reporting entities

Reporting entity	Predicate offence(s)	Key financial intelligence indicators
Asset management companies	Potential tax-related offence	- Rapid investment and disinvestment of funds - Significant cash deposits into personal accounts from business activities
	Potential tax-related offence / fraud	Refusal to provide evidence of business activities or proof of source of funds
	Unknown	Investments made shortly after the client has been de-risked by a commercial bank
Life insurance brokers/agents	Potential tax-related offence	Placement of funds into insurance policies followed by withdrawals within a short period
Long-term insurance services	Potential tax-related offence / unknown	Placement of significant funds into insurance policies without adequate explanation of the source of funds

Reporting entity	Predicate offence(s)	Key financial intelligence indicators
	Potential tax-related offence / theft	High-value insurance policy surrendered shortly after inception to obtain a refund of invested funds
Banking sector	Potential tax-related offence / capital flight	Large cash deposits followed by withdrawals in foreign jurisdictions
	Potential tax-related offence / under-declaration of income tax	- Personal accounts used for business transactions - Large unexplained cash deposits - Transactions inconsistent with customer profile - Multiple cash withdrawals at different branches or ATMs on the same day - Structuring of deposits below the N\$100,000 reporting threshold - Sudden activity on dormant accounts - Frequent closure of business or investment accounts
	Potential tax fraud	Submission of fraudulent or inflated VAT invoices to obtain tax refunds
	Potential tax-related offence / mobile payment risks	Cash deposited by multiple individuals before being transferred abroad using mobile payment services
Authorised dealers with limited authority	Potential tax-related offence	- Frequent remittances to the same beneficiary without a legitimate purpose - Self-remittances for repeated travel that never occurs - Large transfers repeatedly described as 'gifts'
Legal practitioners	Potential tax-related offence / fraud	High-value property purchases or deposits where the source of funds is unclear or unsupported
Motor vehicle dealerships	Potential tax-related offence	- Cash purchase of expensive vehicles by unemployed or low-income individuals - Vehicle purchases are inconsistent with the customer's financial profile
Short-term insurance services	Potential tax-related offence / unknown	Frequent addition of cash-purchased vehicles or assets to existing insurance policies
Stockbrokers	Potential tax-related offence	Rapid investment and withdrawal of funds where the source of wealth is unknown
Supervisory and regulatory bodies	Potential tax-related offence / unknown	Supervised entities receiving operational funding from unidentified or unexplained sources
Unit trust management companies	Potential tax-related offence / unknown	Transactions inconsistent with the customer's financial profile or historical activity
	Potential tax-related offence / fraud	- Refusal to provide evidence of business activities or proof of source of income - Rapid investment and disinvestment of funds
	Potential tax-related offence	Early withdrawal from long-term investment products without a reasonable explanation
	Potential tax-related offence / fraud	International fund transfers authorised using fraudulent or spoofed email instructions

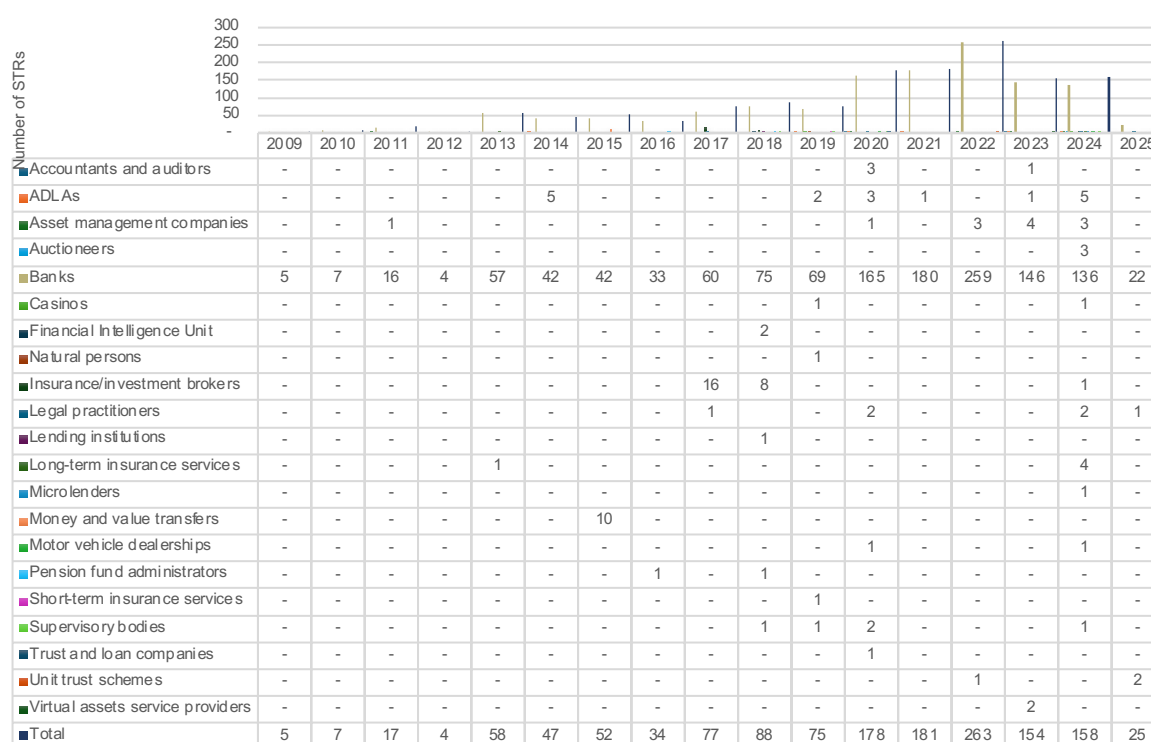
6.3 Potential fraud-related offence trends

Fraud remains one of the most significant predicate offences associated with ML and poses a threat to the integrity and stability of Namibia's financial system. It involves the intentional use of deception, misrepresentation, or concealment of material facts to obtain an unlawful financial or economic benefit or to cause another party to suffer a loss.

Analysis of financial intelligence enables the FIC to identify fraud-related trends, emerging typologies, and associated money laundering risks, thereby supporting the detection and disruption of illicit financial activities.

This section provides an overview of intelligence reports related to possible fraud filed by accountable institutions and reporting institutions from the commencement of reporting obligations in 2009 up to 31 December 2025.

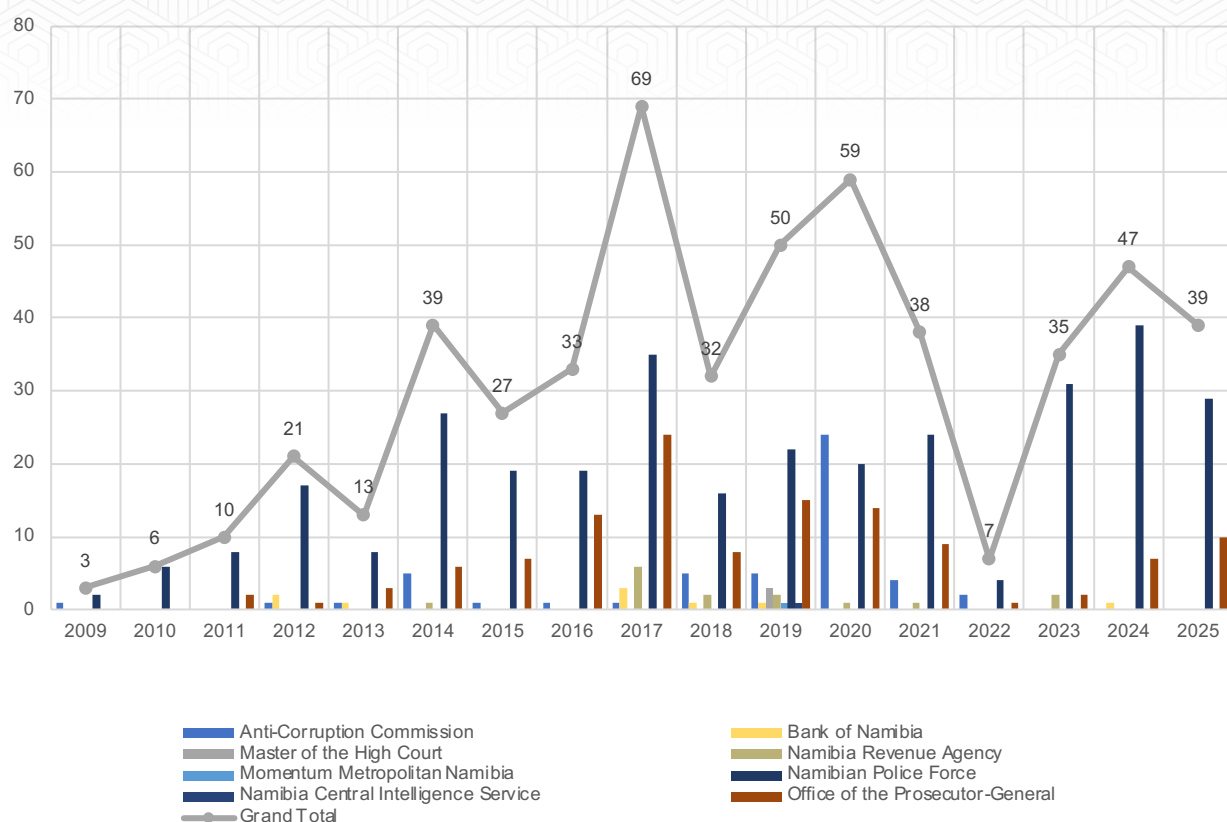
Figure 11: STRs related to potential fraud offences filed by sectors



Analysis of the FIC data indicates that 1,423 STRs relating to potential fraud were received, demonstrating that fraud remains one of the most prevalent predicate offences associated with ML. The banking sector accounted for 1,318 STRs (92.6%), making it by far the largest contributor, followed by insurance/investment brokers with 25 STRs, ADLAs with 17 STRs, and asset management companies with 12 STRs. The dominance of the banking sector reflects its extensive customer base, transaction monitoring capabilities, and central role in detecting suspicious financial activities.

Fraud-related reporting generally increased over the reporting period, rising from 5 STRs in 2009 to a peak of 263 STRs in 2022, before declining to 154 STRs in 2023, 158 STRs in 2024, and 25 STRs in 2025. The decline in 2025 may reflect the reporting period under review or changes in reporting patterns. Overall, the sustained reporting volumes highlight the continued exposure of Namibia's financial system to fraud-related risks and underscore the importance of robust transaction monitoring, customer due diligence, and inter-agency cooperation to detect, investigate, and disrupt fraud and associated ML activities.

Figure 12: Potential fraud spontaneous disclosures per annum



A total of 528 spontaneous disclosures relating to potential fraud were disseminated to LEAs and other competent authorities, demonstrating the FIC's continued role in supporting the investigation of fraud and related financial crimes. The Namibian Police Force (NamPol) received the largest share of disclosures, with 326 disclosures (61.7%), followed by the Office of the Prosecutor-General (122 disclosures; 23.1%), the Anti-Corruption Commission (51 disclosures; 9.7%), and NamRA (15 disclosures; 2.8%). The remaining disclosures were disseminated

to the Bank of Namibia (9), Master of the High Court (3), Momentum Metropolitan Namibia (1), and the Namibia Central Intelligence Service (1).

The concentration of disclosures to NamPol and the Office of the Prosecutor-General underscores the critical role of law enforcement and prosecutorial authorities in investigating and pursuing fraud-related offences identified through financial intelligence.

Table 13: Cross-border movement of cash reports received from sectors

Reporting Sector	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	Total
Law enforcement agencies	7	66	12	11	3	36	68	70	10	1	284
Banks	–	1	–	2	–	–	–	–	–	–	3
Legal practitioners	–	–	–	1	–	2	–	–	–	–	3
Casinos	–	–	–	1	–	–	–	1	–	–	2
Short-term insurance services	–	–	1	–	–	–	–	–	–	–	1
Total reports	7	67	13	15	3	38	68	71	10	1	293

Analysis of the FIC dissemination data indicates that the total value of potential fraud-related transactions disseminated to competent authorities amounted to approximately N\$8.86 billion between 2009 and 2025. The Office of the Prosecutor-General received the highest cumulative value of N\$3.12 billion (35.2%), followed by the Anti-Corruption Commission with N\$2.44 billion (27.6%), NamPol with N\$1.14 billion (12.8%), and NamRA with N\$917.76 million (10.4%). Smaller values were disseminated to the Bank of Namibia (N\$228.36 million) and Momentum Metropolitan Namibia (N\$16.61 million).

The extremely high values recorded between 2019 and 2020 were driven by large-scale fraud matters disseminated between the Office of the Prosecutor-General and the Anti-Corruption

Commission, reflecting the FIC's identification of significant and complex fraud schemes. Overall, the findings demonstrate the FIC's critical role in generating and disseminating high-value financial intelligence to competent authorities, thereby supporting investigations, prosecutions, and the disruption of fraud-related criminal activity while safeguarding the integrity and stability of Namibia's financial system.

6.3.1 Various reasons for reporting transactions as suspicious

The following section highlights key observations from case studies and the predominant methods and indicators associated with potential fraud-related offences identified during the reporting period.

Table 14: Potential fraud-related offence typologies and indicators

Sector	Fraud-related typology	Potential indicators / red flags
Banking	Account takeover fraud	- Sudden changes to customer contact details followed by large transfers - Unauthorised online banking transactions - Multiple failed login attempts followed by successful access
	Identity fraud	- Accounts opened using suspected forged or stolen identity documents - Customer information is inconsistent with official records - Multiple accounts linked to the same identification details
	Business email compromise	- Large payments made following email instructions that differ from normal business practices - Sudden changes in beneficiary banking details - Urgent payment requests with no supporting documentation
	Loan/application fraud	- False income or employment documentation submitted to obtain credit - Loan proceeds immediately transferred to unrelated third parties
	Card and electronic payment fraud	- Unusual ATM withdrawals - Multiple small transactions within a short period - Card-not-present transactions inconsistent with customer behaviour
Insurance	Claims fraud	- Repeated or exaggerated insurance claims - Claims supported by suspicious or altered documentation - Multiple claims involving the same individuals or assets
	Premium investment fraud	- Large premiums paid and policies cancelled shortly afterwards to obtain refunds - Source of funds is inconsistent with customer's financial profile
Asset management / unit trusts	Investment fraud	- Rapid investment and disinvestment without a clear commercial rationale - Refusal to provide sources of wealth or sources of funds documentation - Investment activity inconsistent with customer profile
Legal practitioners	Property and trust fraud	- Property transactions that involve unexplained cash payments - Use of nominees without legitimate commercial purpose - Frequent transfers of property ownership below market value
Real estate	Property fraud	- Cash purchases of high-value properties - Property values are inconsistent with buyer's known income - Multiple purchases and rapid resales without economic justification
Motor vehicle dealerships	Vehicle purchase fraud	- Purchase of luxury vehicles using unexplained cash - Buyers unable to demonstrate legitimate source of funds - Vehicles registered in third-party names
Money and value transfer services	Remittance fraud	- Multiple transfers structured below reporting thresholds - Numerous senders transferring funds to the same beneficiary - Frequent cross-border remittances without an apparent purpose
Casinos and gambling	Gambling fraud	- Purchase of chips with cash followed by minimal gambling and redemption - Frequent high-value cash transactions are inconsistent with customer profile
Public sector	Procurement and corruption fraud	- Unusual government contract payments - Multiple payments to newly established suppliers - Payments inconsistent with procurement records

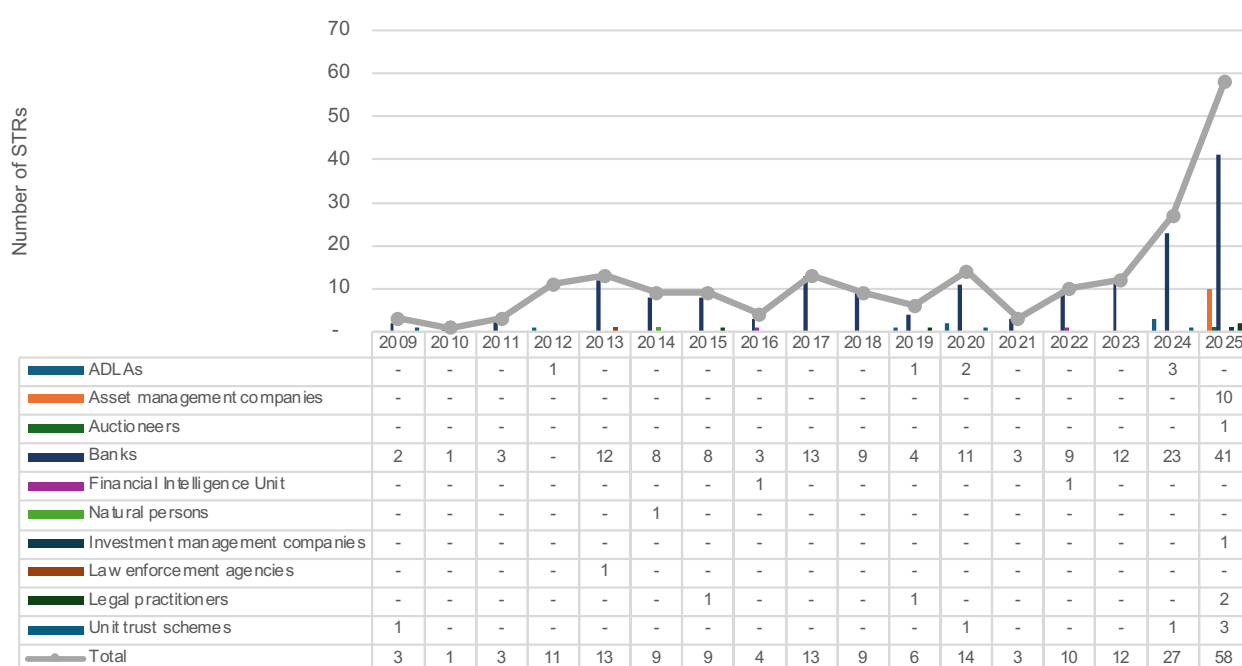
6.4 Potential corruption-related offence trends

Corruption remains a significant predicate offence for ML and poses a threat to the integrity, transparency, and stability of Namibia's financial system. It involves the abuse of entrusted power or public office for private gain, including offences such as bribery, embezzlement, abuse of office, and the misappropriation of public resources.

The analysis of STRs, financial intelligence, and spontaneous disclosures provides insight into emerging corruption-related trends, associated ML risks, and sectors most vulnerable to abuse. This analysis supports the detection and disruption of illicit financial flows while strengthening governance, accountability, and the resilience of Namibia's financial system.

This section provides an overview of intelligence reports related to possible corruption filed by accountable institutions and reporting institutions from the commencement of reporting obligations in 2009 to 31 December 2025.

Figure 13: STRs related to potential corruption offences filed by sectors

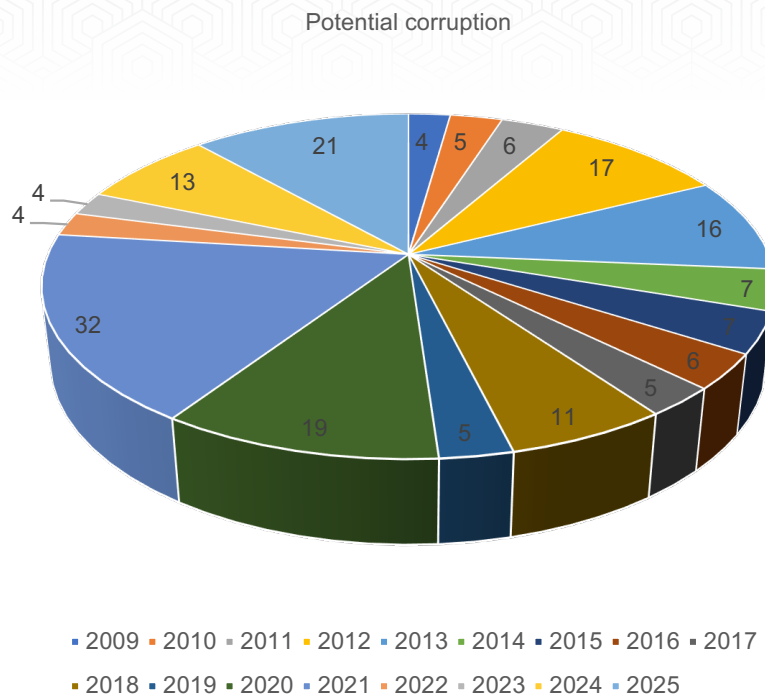


Analysis of the FIC data indicates that a total of 205 STRs relating to potential corruption offences were received. The banking sector accounted for 162 STRs (79.0%), making it the predominant reporting sector, followed by asset management companies (10 STRs), ADLAs (7 STRs), unit trust schemes (6 STRs), and legal practitioners (4 STRs).

Annual reporting volumes remained relatively low during the early years of the reporting period but increased gradually over time, with the highest number of reports recorded in 2025 (58 STRs), followed by 2024 (27 STRs).

This upward trend suggests enhanced detection and reporting of transactions potentially linked to corruption, particularly by the banking sector, which continues to play a central role in identifying suspicious financial activity. The increase in recent years may also reflect strengthened AML/CFT/CPF controls, improved transaction monitoring systems, and greater awareness of corruption-related risks among reporting institutions.

Figure 14: Potential corruption spontaneous disclosures per annum to the ACC



A total of 182 spontaneous disclosures relating to potential corruption offences were disseminated to the Anti-Corruption Commission (ACC) during the review period. Reporting volumes fluctuated throughout the reporting period, increasing from 4 disclosures (2.2%) in 2009 to 17 disclosures (9.3%) in 2012, before declining and remaining relatively stable between 2014 and 2019, where annual disclosures ranged between 5 (2.7%) and 11 (6.0%).

A significant increase was recorded in 2020, with 19 disclosures (10.4%) disseminated, followed by the highest annual volume of 32 disclosures (17.6%) in 2021. This peak was followed by a sharp decline to 4 disclosures (2.2%) in both 2022 and 2023, before increasing again to 13 disclosures (7.1%) in 2024 and 21 disclosures (11.5%) in 2025.

Overall, the upward trend observed in recent years indicates enhanced identification and dissemination of corruption-related financial intelligence by the FIC. The findings demonstrate the FIC's continued support to the ACC by providing actionable intelligence to facilitate the investigation and prosecution of corruption-related offences, thereby contributing to the protection of the integrity and stability of Namibia's financial system.

Table 15: Value of potential corruption-related spontaneous disclosures to the ACC

Year	Value (N\$)
2009	51,419,578.00
2010	55,375,101.00
2011	12,268,968.00
2012	21,869,338.00
2013	36,449,969.00
2014	37,094,223.00
2015	9,867,305.00
2016	17,393,276.00
2017	6,244,604.00
2018	45,889,645.00
2019	29,935,548.00
2020	314,682,159.00
2021	2,114,057,409.00
2022	5,101,922.00
2023	959,370,903
2024	21,335,120.00
2025	191,721,837.00
Total	3,930,076,905.00

The corruption-related financial disclosures show significant volatility over the 2009–2025 period, with a cumulative reported value of N\$3.93 billion. The highest value was recorded in 2021 at N\$2.11 billion, followed by 2023 at N\$959.37 million and 2020 at N\$314.68 million. These peaks indicate periods involving potentially substantial corruption-related financial exposure. The sharp fluctuations across years suggest that corruption risks are episodic and may involve high-value transactions, complex schemes, or concentrated cases requiring enhanced investigation and asset-recovery measures.

Overall, the findings indicate that while the number of corruption-related cases may fluctuate annually, the financial impact can be substantial, underscoring the importance of the FIC's financial intelligence in supporting corruption investigations and safeguarding the integrity of Namibia's financial system.

6.4.1 Various reasons for reporting transactions as suspicious

The following section highlights key observations from case studies and the predominant methods and indicators associated with potential fraud-related offences identified during the reporting period.

Table 16: Potential corruption-related offence typologies and indicators

Typology	Potential indicators / red flags
Bribery	• Unexplained payments to public officials or prominent influential persons (PIPs) • Payments disguised as consultancy or facilitation fees • Large cash deposits following the award of public contracts
Procurement fraud	• Inflated invoices for government contracts • Repeated awards to the same suppliers without competitive bidding • Payments to shell or newly established companies with no operational history
Abuse of public office	• Public officials accumulating wealth inconsistent with known income • Unexplained acquisition of high-value assets • Frequent transactions involving related parties or family members
Embezzlement and misappropriation of public funds	• Diversion of public funds to personal or third-party accounts • Multiple transfers to unrelated beneficiaries • Unauthorised withdrawals from government or institutional accounts
Conflict of interest	• Contracts awarded to companies linked to public officials or close associates • Undisclosed beneficial ownership of bidding entities • Payments to businesses with common directors or shareholders
Use of shell or front companies	• Companies with no visible business operations that receive substantial government payments • Frequent transfers between related entities without a commercial purpose • Lack of supporting documentation for transactions
Cross-border movement of illicit financial proceeds	• Transfers of corruption proceeds to foreign jurisdictions without a legitimate business rationale • Payments to offshore companies or high-risk jurisdictions • Rapid movement of funds through multiple accounts to conceal ownership
Asset concealment and ML	• Purchase of luxury properties, vehicles, or investments using unexplained wealth • Use of nominees or third parties to hold assets • Layering of funds through multiple bank accounts or financial products

6.5 Geographic distribution and frequency of reported typologies

The geographic distribution of reported money laundering and predicate offence typologies indicates that cases are concentrated in Namibia's major commercial and administrative centres, particularly Windhoek, Walvis Bay, Swakopmund, Oshakati, Ondangwa, and Rundu. These locations account for a significant proportion of financial activity, banking services, government procurement, and cross-border trade, making them more vulnerable to financial crime. Border towns and transport corridors also feature prominently in cases that involve cash smuggling, trade-based money laundering, tax-related

offences, and illicit cross-border fund movements due to their proximity to neighbouring countries and the high volume of commercial transactions.

Analysis of reporting trends further indicates that fraud, tax-related offences, corruption, and cash-intensive business typologies remain the most frequently reported predicate offences associated with money laundering. Banking institutions continue to account for the majority of STRs, reflecting their central role in detecting unusual financial activity. While the frequency of typologies varies from year to year, the recurring nature of these offences demonstrates persistent vulnerabilities within the financial system and highlights the need for continued

risk-based supervision, enhanced inter-agency cooperation, and targeted preventive measures in high-risk sectors and geographic locations.

The analytical findings presented in this chapter demonstrate that fraud, tax-related offences, and corruption continue to pose significant threats to Namibia's financial system. The increasing volume of suspicious transaction reports, financial intelligence products, and spontaneous disclosures highlights the growing effectiveness of reporting institutions and the FIC in identifying,

analysing, and disseminating intelligence related to financial crime. The chapter also illustrates the substantial financial values associated with these offences and highlights recurring typologies involving cash-intensive transactions, misuse of business accounts, cross-border transfers, complex ownership structures, and abuse of professional services. Collectively, the findings reinforce the importance of intelligence-led interventions, robust compliance controls, and inter-agency cooperation in detecting illicit financial flows and protecting the integrity and stability of Namibia's financial system



Financial system integrity implication

Integrity implication: The prevalence of fraud, tax-related offences, and corruption demonstrates continued attempts to misuse the financial system; however, increasing reporting and intelligence dissemination indicate stronger transparency and institutional vigilance.

Effectiveness implication: The growing use of financial intelligence and spontaneous disclosures reflects improved detection, analysis, and support to law enforcement and supervisory authorities.

Policy implication: Priority should be given to strengthening transaction monitoring, beneficial ownership transparency, cross-border intelligence cooperation, and sector-specific controls in areas vulnerable to financial crime.



7.1 Overview

The FIC develops case studies from financial intelligence gathered through STRs, SARs, supervisory information, law enforcement referrals and other intelligence sources. These case studies demonstrate how financial intelligence is used to identify, analyse, and disrupt ML, TF, PF, and related predicate offences. The case studies presented in this report highlight common ML methods, emerging trends, vulnerabilities exploited by criminals, and the effectiveness of inter-agency cooperation. They are intended to provide practical insights to

reporting institutions, competent authorities, and policymakers while strengthening the understanding of financial crime risks and supporting the implementation of effective AML/CFT/CPF measures. To protect ongoing investigations and comply with the Financial Intelligence Act, all case studies are sanitised and presented for illustrative purposes only. It is therefore crucial that accountable and reporting institutions constantly conduct risk assessments on their products, services, and customers in order to enable a proactive approach to combatting ML/TF/PF threats.

CASE STUDY 1: Virtual assets, fraud, human trafficking and ML (funds in foreign virtual asset wallets preserved)

This matter emanated from the proactive opening of a SAR by the FIC under IRDC-0394/22-AUG-23 (SAR-1586/22-AUG-23 and IRD-896/23-AUG-23) and the subsequent requesting of intelligence by the Police and foreign LEAs through the FIC. This case study is an example of how LEAs, local and international, can coordinate and cooperate to secure/confiscate the proceeds of crime associated with virtual assets.

Introduction

A registered entity (a close corporation) was used by its beneficial owners to conduct criminal activities. The entity reportedly employed about 90 young Namibians (the majority forcibly), who were hoarded at a house in an upmarket suburb in Windhoek. The entity operated secretly. The charges in this regard are, among others, human trafficking, fraud, money laundering (racketeering), and offences under the Virtual Assets Act of 2023.

During a clandestine night-time operation conducted in October 2023, the Police arrested 12 subjects at an office building around Ausspannplatz (see the newspaper articles under the links: <https://www.namibian.com.na/namibians-arrested-over-investment-scam-cooperating-with-the-police/> and <https://www.namibian.com.na/police-arrest-namibians-chinese-in-scam-targeting-americans/>). The involved subjects comprised supervisors of two nationalities and some local operators who were reportedly conducting illegal operations during which 'innocent victims/individuals' were tricked into investing in crypto platforms.

These illegal operations reportedly targeted wealthy foreigners (including Americans and Europeans) via email and WhatsApp. After being tricked into investing, the individuals were reportedly extorted with sexually explicit information/pictures that were shared with the operators during earlier 'innocent' conversations. The operations were reportedly stopped once the individuals became suspicious or raised concerns, and the funds accumulated in the crypto accounts were then emptied through withdrawals at a crypto kiosk or transfers to other wallets.

During February 2024, Police investigations identified and followed several crypto wallets and their addresses, leading them to a crypto currency exchange entity based in a foreign jurisdiction (virtual asset service provider), which reportedly held two crypto accounts. The Police reached out to the VASP and were advised that the wallets contained substantial amounts, approximately USD150,000.00. As these funds reportedly emanated from the 'innocent victims/individuals' scam (as referred to in the second paragraph), they are therefore the proceeds of crime.

The Police requested the FIC for assistance. The FIC reached out to its counterparts in the referred foreign jurisdiction where the wallets were being held, sharing intelligence on the crypto wallets. The FIC's counterparts used their powers under their AML/CFT Act to issue a directive for an administrative restriction/freeze on the wallet accounts for 10 working days.

Intelligence was shared with the Police and the Asset Forfeiture Unit within the Office of the Prosecutor-General, upon which a preservation of property application was brought to the High Court of Namibia with regard to the positive balances in the two crypto wallets. A Preservation of Property Order was granted on 19 July 2024 and a Forfeiture Order was subsequently granted in the High Court.

Evolution of the case

Initial detection: Details of the events that led to the initial detection of the crime

The FIC proactively opened a SAR, working towards sharing intelligence with LEAs. The Police subsequently requested that the FIC perform a financial analysis of the subjects. Additionally, the Police and Prosecution requested that the FIC follow the funds in the two crypto wallets identified in a foreign jurisdiction.

Role of the Financial Intelligence Unit and analysis: Methods used to gather information related to the case

The FIC mainly requested and obtained information from local LEAs (Police and Prosecution) and shared the same with the foreign FIU. Intelligence was also requested from the foreign FIU and shared with local LEAs. This intelligence sharing allowed the foreign FIU to use its domestic laws to restrict/freeze the crypto wallets, which in turn allowed the local Prosecution to bring a preservation application in the High Court of Namibia before the expiry of restriction/freezing. The application was granted.

How was the case developed and how did the FIU significantly contribute to the development of the case?

The FIC collected the intelligence pertaining to the two crypto wallets from the local LEAs (Police and Prosecution), which was followed and identified by the Police in the foreign jurisdiction during their investigation. The intelligence was shared with the foreign FIU, additional intelligence pertaining to their restriction/freezing capabilities was requested from the foreign FIU, and in turn this intelligence was shared with the local Prosecution.

How many FIUs were involved in the case and how did international cooperation contribute to effectively resolving the case?

The matter involved one foreign FIU. Upon request by our FIU, the foreign FIU provided valuable intelligence and restricted/froze the crypto wallets upon request, using their domestic laws. This allowed the local Prosecution to bring a preservation application in the High Court of Namibia before expiry of the restriction/freezing, which was granted.

Case status

During the ongoing investigations, several subjects were arrested. Further Police investigation identified additional subjects, which led to the preservation of approximately USD150,000.00 in the crypto wallets. A Forfeiture Order was subsequently granted in the High Court.

Summation of the case

Source of the case	Proactive opening of a SAR by the FIC and a subsequent request for intelligence by the Police
Subject/entity involved	Two crypto wallet holders
Fronting of the matter	N/A
Investigation began	October 2023
Key payment mechanisms	Transfer of funds to crypto wallets held by the VASP in a foreign jurisdiction
Perpetrators	Two crypto wallet holders
Crime type	Human trafficking, fraud, money laundering (racketeering), and offences under the Virtual Assets Act of 2023
Law contravened	Criminal Procedure Act (CPA); Prevention of Organised Crime Act, 2004; Money Laundering
Alleged service/product offered	Crypto currency
Seizures	Preservation of Property Order is awaiting representation and subsequent final forfeiture application in the High Court of Namibia
Proceeds identified	Approximately USD150,000.00 crypto currency held in two wallets
Agencies involved	FIC, foreign FIU, Police, Office of the Prosecutor-General • Several intelligences facilitated and shared between institutions • Virtual and face-to-face meetings with the Police and Office of the Prosecutor-General • Email correspondence

Jurisdictions	Namibia and Seychelles (foreign jurisdiction)
Bank product used	Account from which money was sent to crypto wallets
Banks used	Two local banks
Status of proceedings	• Matter is under Police investigation • Warrants of arrest (W/A) issued for the two crypto wallet holders
Period of criminal activity	Two years
Network financial analysis	• Victims tricked into making crypto investments in several wallets • Wallets followed by Police through investigative means • Funds followed and identified were held in crypto wallets of two subjects in a foreign jurisdiction • Crypto currency in wallets restricted/frozen for 10 working days by foreign FIU using powers under their AML/CFT Act • Preservation of Property Order granted in respect of positive balance in two crypto wallets

This case highlights the growing misuse of virtual assets to facilitate transnational financial crime and demonstrates the importance of financial intelligence and international cooperation in combating ML. Following a proactive SAR initiated by the FIC, investigations uncovered a criminal network operating from Namibia that allegedly used cryptocurrency investment scams to defraud foreign victims, generating illicit proceeds linked to human trafficking, fraud, racketeering, and ML. Through close collaboration between the FIC, the Namibian

Police, the Office of the Prosecutor-General, and a foreign FIU, approximately USD150,000 held in two cryptocurrency wallets was identified, frozen, and preserved through a High Court order pending forfeiture proceedings. The case demonstrates the effectiveness of investigations, cross-border information sharing, and asset recovery measures in disrupting sophisticated financial crime while underscoring the need for robust regulation and supervision of VASPs to protect the integrity of Namibia's financial system.

Case Study 2: Insurance fraud and money laundering

A suspicious transaction report (STR) filed by Bank-C revealed what appears to be a prevailing fraud syndicate targeting insurance companies through life and funeral policies by faking the deaths of unsuspecting individuals. In this matter, the subject, Mr N, took out several funeral covers on his alleged fiancée, Ms F, during October 2023. On 1 April 2024, Mr N submitted a claim, stating that Ms F had died in a motor vehicle accident on the same date. The claimant submitted all the required documentation. However, information within the FIC's domain suggests that these documents may have been forged and the identity card used to open the policies may have been stolen.

Modus operandi

- The perpetrators take out life/funeral policies that cover alleged relatives, where the perpetrator is listed as the beneficiary.
- A bank account is opened in the name of the beneficiary, from which monthly premiums are consistently paid throughout the grace period (normally six months).
- Shortly after the grace period, the covered relative is declared dead, often due to a motor vehicle accident.
- To initiate the insurance claim, the beneficiary then submits the required documents, which include:
 - » death certificate;
 - » certified copy of the deceased's ID;
 - » certified copy of the beneficiary's ID;
 - » medical certificate of cause of death;
 - » medico-legal postmortem examination report; and
 - » Namibia road accident report form.

Affected companies

The analysis indicates that the following insurance companies have fallen victim to the scheme:

- Company-A Namibia (Pty) Ltd.
- Company-B Namibia (Pty) Ltd.
- Company-C Namibia (Pty) Ltd.

The analysis suggests that multiple insurers could have been exposed to this fraud.

Suspected syndicate members

The scheme suggests collusion among multiple actors, including professionals whose roles provide access to critical documents and processes (e.g. medical, civil registration, financial, or insurance officials). These roles, if exploited, may enable fraudulent claims by:

- Police officers and doctors, who falsely declare deaths;
- Home Affairs officials, who issue fraudulent death certificates;
- insurance company staff involved in processing claims;
- the insured person themselves, in some cases; and
- bank officials, who may facilitate fraudulent account openings.

Outcome of analysis

- The analysis of the STR filed with the FIC shows strong indicators of fraud.
- Account 00000285 held at Bank-C in the name of Mr N (beneficiary) was restricted.
- Intelligence was shared with law enforcement agencies.
- After engagement with the FIC, Company-A Namibia (Pty) Ltd. reviewed both the new and old motor vehicle accident claims. This led to:
 - four suspicious reports filed; and
 - seven criminal investigations initiated with the Namibian Police.
- The Prosecutor-General successfully secured a Preservation Order amounting to N\$438,632.18.

Red flags observed

The following red-flag indicators were noted during the investigation:

- New bank accounts were opened almost at the same time as the policies.
- The accounts showed limited activity, with transactions mostly consisting of monthly premium payments.
- After the claims were paid, no funeral-related expenditures were observed.
- Withdrawals were made via ATMs only, raising suspicion that the accounts may have been opened with stolen identity cards.
- Inter-bank transfers contained vague or concealed descriptions to hide the source of funds.
- Each claim involved different accounts, individuals, and/or banks, making it challenging to directly link all the role players.

Analytical insight

- This case demonstrates how weaknesses in civil registration systems (identity documents, death certificates) and limited verification by insurers can be systematically exploited.
- The collusion of multiple actors, including police, health officials, and insurance staff, highlights the interconnected vulnerabilities across both public and private institutions.
- From an AML/CFT/CPF perspective, the absence of funeral-related expenditures and the use of ATMs for withdrawals are strong indicators of layering attempts.
- This typology suggests that fraudulent claims should not be viewed in isolation but as part of broader syndicate operations that can move significant sums through the financial system undetected.
- Strengthening cross-agency data validation and enhancing insurer due diligence on death claims would reduce exposure to both fraud and money laundering risks.

This case highlights a sophisticated fraud syndicate that exploited life and funeral insurance policies by using forged documents and stolen identities to submit fraudulent death claims. Analysis by the FIC, based on an STR, revealed a coordinated scheme involving multiple insurance companies and suspected collusion among individuals across both the public and private sectors. The investigation identified several ML indicators, including newly opened bank accounts, limited account activities, ATM cash withdrawals, and the absence of

funeral-related expenses following claim payments. Intelligence shared with law enforcement resulted in the restriction of bank accounts, multiple criminal investigations, and the preservation of N\$438,632.18 in suspected criminal proceeds. The case underscores the importance of enhanced customer due diligence, verification of death-related documentation, inter-agency cooperation, and proper investigations in detecting and disrupting insurance fraud and associated ML activities.

Case Study 3: Cocaine trafficking and cross-border organised crime (Angola-Namibia-South Africa cocaine transit)

Background	Two male Angolan nationals were arrested at a roadblock near Keetmanshoop while transporting 39.35 kg of cocaine (street value N\$20,125,000.00) from Angola through Namibia to South Africa. The drugs were hidden in a modified Toyota Land Cruiser.
Modus operandi	Cocaine was concealed in a false under-vehicle compartment and inside the spare tyre. Deodorants and silicon were used to mask the smell. The accused claimed they were hired to deliver the vehicle, and forged authorisation documents were provided.
Red flags	• Travel stories and documents were inconsistent, for example, forged papers that did not match the vehicle ownership or purpose. • The behaviour during inspection was nervous, which is often detected by trained officers as a sign of guilt or fear. • Concealment tools (e.g. pop rivet gun) were present, indicating that the vehicle was modified for smuggling. • A strong cocaine odour, which was not addressed by the accused despite attempts to mask it, revealed inadequate concealment. • The route from Angola to South Africa is high-risk and known for drug transit corridors. • The large quantity was inconsistent with personal use, suggesting commercial intent and potential ML proceeds. • The indication of financial transactions such as cash payments for vehicle modifications and/or unexplained funds for travel expenses are risk indicators.
LEA actions	• NamPol's Drug Law Enforcement Unit stopped and searched the vehicle. • Forensic analysis by the Namibia Forensic Science Institute confirmed the substance. • The FIC supported through general intelligence on drug-related STRs. • The Office of the Prosecutor-General prosecuted, with international cooperation via Angola links.
Status of the case	• Convicted of dealing in cocaine • Sentenced to 10 years (4 suspended) • Appeals dismissed by the Supreme Court
Sectors affected	• Road transportation (vehicles modified for smuggling) • Border security and customs (land checkpoints vulnerable to forged documents) • Financial sector (potential cash-based laundering in informal networks) • Automotive services (modifications for concealment)

This case highlights the link between transnational drug trafficking and ML, demonstrating how criminal networks exploit regional transport corridors to facilitate the movement of illicit drugs and generate criminal proceeds. Two male Angolan nationals were arrested near Keetmanshoop for transporting 39.35 kg of cocaine, valued at approximately N\$20.1 million. The cocaine was concealed in a modified vehicle that was travelling from Angola to South Africa. The investigation identified several risk indicators, including forged documentation, inconsistent travel explanations, sophisticated concealment methods, and

the use of a high-risk trafficking route. Through coordinated efforts by the Namibian Police, the Namibia Forensic Science Institute (NFSI), the FIC, and the Office of the Prosecutor-General, the offenders were successfully prosecuted and convicted. The case underscores the importance of border security intelligence, inter-agency cooperation, and financial investigations in disrupting organised crime, tracing criminal proceeds, and protecting the integrity of Namibia's financial system.

Case Study 4: Theft of diamonds, money laundering and unexplained wealth investigation

Background

This case arose after the FIC received intelligence indicating that several individuals, previously of modest means, were suddenly living lavish lifestyles following the theft of diamonds worth millions. The FIC conducted a proactive financial analysis and shared intelligence with NamPol and the Office of the Prosecutor-General, which led to the establishment of a multi-agency task team.

Summary of the case

The investigations linked the subjects to suspected illegal dealing in unpolished diamonds and money laundering. The financial analysis revealed significant unexplained wealth, including luxury vehicles, livestock, property renovations, expensive electronics, luxury holidays, firearms, and the use of cryptocurrency cards to conceal and spend the criminal proceeds. The intelligence further linked one suspect to a company from which diamonds had reportedly been stolen, and a luxury vehicle was traced to a convicted illegal diamond dealer in a neighbouring country.

Modus operandi

The suspects allegedly:

- sold or trafficked stolen diamonds;
- deposited large sums of cash into multiple bank accounts;
- rapidly transferred funds between personal and business accounts;
- used two cryptocurrency cards to purchase luxury goods and withdraw funds through cashback transactions;
- laundered the proceeds through the purchase of vehicles, livestock, household goods, electronics, and property improvements; and
- attempted to disguise the illicit proceeds through transactions involving multiple jurisdictions and cryptocurrency.

Role of the Financial Intelligence Centre

The FIC played a central role by:

- conducting financial profiling and analysing 22 bank accounts linked to 11 individuals and entities;
- identifying unexplained deposits, flow of funds, beneficial ownership information, and assets acquired;
- producing financial intelligence reports, account analyses, and link diagrams;
- restricting approximately N\$40,000 under section 42 of the Financial Intelligence Act;
- coordinating intelligence briefings with NamPol and the Office of the Prosecutor-General; and
- requesting intelligence from three foreign FIUs regarding cryptocurrency cards and cross-border transactions.

Law enforcement actions

Based on the FIC intelligence, NamPol:

- opened a criminal investigation and conducted a parallel financial investigation;
- executed search warrants on residences and farms;
- arrested three suspects;
- seized cryptocurrency cards, luxury vehicles, trailers, livestock, and other assets;
- created a government-controlled bank account to receive proceeds recovered from the cryptocurrency cards;
- successfully transferred over N\$2.3 million from the crypto cards into the government account; and
- gathered evidence to support an Unexplained Wealth Order application.

Prosecutorial actions

The Office of the Prosecutor-General:

- used the financial intelligence and Police evidence to obtain an Unexplained Wealth Order under section 50A of the Prevention of Organised Crime Act;
- secured preservation of identified assets; and
- continued to provide legal guidance throughout the ongoing investigation and asset recovery process.

Outcomes

The investigation resulted in:

- the arrest of three suspects, with two additional individuals remaining under investigation;
- a successful High Court Unexplained Wealth Order;
- the identification of unexplained wealth valued at approximately N\$5.7 million linked to suspected unlawful activities; and
- the preservation of:
 - approximately N\$2.3 million recovered from cryptocurrency cards;
 - approximately N\$40,000 frozen in a bank account;
 - three luxury vehicles;
 - two sedan vehicles;
 - one trailer; and
 - 92 head of livestock (79 goats and 13 sheep), with additional livestock later identified.

Key lessons learned

- Proactive financial intelligence can uncover organised criminal activity before assets are dissipated.
- Parallel financial investigations are essential to identify and preserve criminal proceeds alongside investigations into predicate offences.
- Cryptocurrency products, such as prepaid crypto cards, can be exploited to disguise and spend illicit proceeds.
- Multi-agency cooperation between the FIC, NamPol, the Office of the Prosecutor-General, and foreign FIUs significantly enhances the effectiveness of investigations and asset recovery.
- Early intelligence sharing and coordinated operational planning were instrumental in securing the assets and preventing further dissipation of the criminal proceeds.

The case studies presented in this chapter demonstrate the practical application and value of financial intelligence in detecting, investigating, and disrupting complex financial crime. The examples illustrate the growing risks posed by virtual assets, insurance fraud, organised drug trafficking, money laundering, unexplained wealth, and cross-border criminal networks. The cases highlight the importance of proactive

intelligence gathering, inter-agency cooperation, international information sharing, asset recovery measures, and parallel financial investigations. Collectively, the case studies show how financial intelligence contributes to preserving criminal assets, supporting investigations, and strengthening Namibia's ability to respond effectively to emerging financial crime threats.

Made for you, the professional designer who needs images that have one purpose - to make finding the perfect image easier, more rhythmic and user intuitive - then you'll love us. With fast customer service that's anywhere else. Picselements.com is raising the bar. Made for you, the professional designer who needs images that have one purpose - to make finding the perfect image easier, more rhythmic and user intuitive - then you'll love us. With fast customer service that's anywhere else. Picselements.com is raising the bar. Made for you, the professional designer who needs images that have one purpose - to make finding the perfect image easier, more rhythmic and user intuitive - then you'll love us. With fast customer service that's anywhere else. Picselements.com is raising the bar.

CHAPTER 08

ANALYSIS OF KEY FINANCIAL RISKS IN NAMIBIA

8.1 Overview

The FIC analysis identified fraud, corruption, and tax-related offences as the most significant predicate offences generating illicit proceeds within Namibia's financial system. These offences continue to account for a substantial proportion of the STRs, intelligence analyses, and spontaneous disclosures disseminated to competent authorities. Their prevalence demonstrates the persistent misuse of the financial system to conceal criminal proceeds, evade regulatory controls, and facilitate ML. Consequently, these offences remain key threats to the integrity, transparency, and stability of Namibia's financial system.

8.2 Fraud-related offence risk analysis

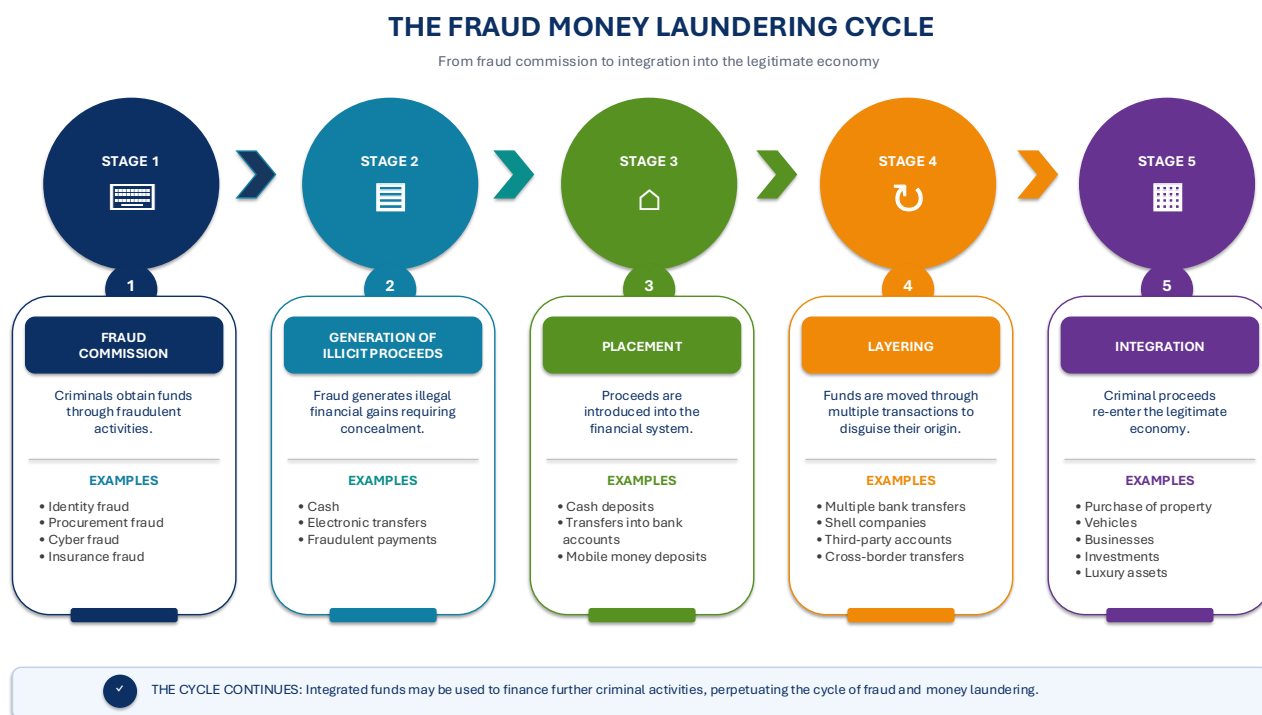
Fraud remains the most significant predicate offence identified by the FIC and continues to generate substantial proceeds that

are subsequently laundered through Namibia's financial system. This offence affects both the public and private sectors and increasingly exploits digital financial services, electronic banking platforms, insurance products, and commercial transactions. This section demonstrates fraud-related risk analysis.

8.2.2 Fraud risk cycle

The fraud cycle illustrates how illicit proceeds generated through fraud are introduced into the financial system, concealed through a series of transactions, and ultimately integrated into the legitimate economy. Understanding this process enables reporting institutions and competent authorities to identify suspicious activities, disrupt ML schemes, and prevent the misuse of the financial system.

Figure 15: Demonstration of fraud risk cycle



8.2.1 Fraud risk matrix

The risk assessment indicates that fraud remains one of the highest threats to Namibia's financial system, with an overall 'very high' risk rating. The banking sector continues to be the primary source of reporting due to its central role in the financial system and its ability to detect suspicious transactions. Fraud

poses a significant financial impact on government institutions, businesses, and individuals, with reporting trends indicating an increasing occurrence over time. These findings underscore the need for enhanced transaction monitoring, robust customer due diligence, and continued collaboration among reporting institutions and competent authorities to mitigate fraud-related ML risks.

Table 17: Rating of fraud risk assessment matrix

Fraud risk dashboard	Rating
Overall risk	Very high
Financial impact	Very high
Reporting trend	Increasing
Banking sector exposure	High
ML vulnerability	Very high
National financial stability impact	High

It is significant to indicate that the fraud risk ratings were derived from an assessment of FIC reporting data, including STRs and SARs, together with observed reporting trends, sectoral exposure, financial impact, and the potential for fraud-related proceeds to be laundered through the financial system. The assessment considered the volume and trend of fraud-related reporting, the concentration of reporting within the banking sector, the potential financial losses associated with fraud, and the extent to which fraud proceeds may enter or move through the financial system. Ratings were assigned using a qualitative risk-rating approach based on the assessed level of likelihood/exposure and potential impact, with the categories low, medium, high, and very high. The overall rating reflects the combined assessment of these risk dimensions and should therefore be interpreted as a strategic risk assessment rather than a statistical outlook.

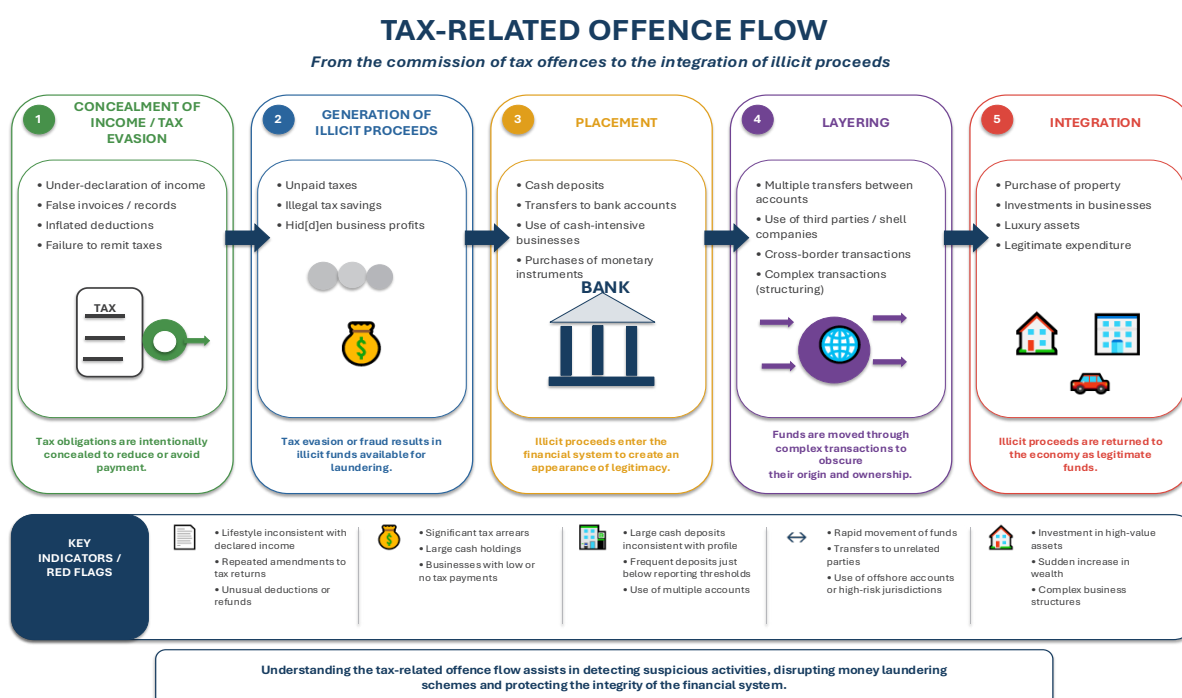
8.3 Tax-related offence risk analysis

Potential tax-related offences continue to represent a significant financial crime risk due to their impact on domestic revenue mobilisation and their close relationship with ML. Most reports originate from the banking sector and involve concealed business income, undeclared cash receipts, and suspicious international fund movements. This section demonstrates tax-related risk analysis.

8.3.1 Tax-related offence flow

The tax-related offence flow illustrates how illicit proceeds generated through tax evasion or tax fraud are concealed and laundered through the financial system. Understanding this process enables reporting institutions and competent authorities to identify suspicious transactions, detect potential tax-related offences, and disrupt the laundering of illicit proceeds.

Figure 16: Demonstration of tax-related flow stage



8.3.2 Tax-related risk matrix

The tax-related risk matrix illustrates the inherent ML risks associated with tax-related offences by assessing their likelihood and potential impact on Namibia's financial system. The matrix indicates that tax evasion, complex ownership structures, cross-border transactions, and the use of cash-intensive businesses present the highest risk due to their ability to generate and conceal substantial illicit proceeds. These activities often involve sophisticated methods to disguise the source and ownership of funds, making detection more challenging.

The matrix further demonstrates that weak compliance practices and inadequate internal controls increase the vulnerability of reporting institutions to tax-related offences, particularly when combined with other high-risk activities. Overall, the findings highlight the importance of strengthening risk-based supervision, customer due diligence, beneficial ownership transparency, and inter-agency cooperation to effectively detect, prevent, and disrupt tax-related ML and safeguard the integrity of Namibia's financial system.

Table 18: Rating of tax risk assessment

Tax-related ML risk driver	Likelihood (1 to 5)	Impact (1 to 5)	Risk score	Risk rating
Tax evasion	5	5	25	● Very high
Cross-border transactions	4	5	20	● Very high
Cash-intensive businesses	4	4	16	● Very high
Complex ownership structures	4	4	16	● Very high
Weak compliance and internal controls	3	4	12	● High
Overall tax-related ML risk	—	—	17.8	● Very high

The table indicates that tax-related ML presents a 'very high' inherent risk to Namibia's financial system, with tax evasion assessed as the most significant risk driver due to its high likelihood and potential financial impact. Cross-border transactions, cash-intensive businesses, and complex ownership structures also demonstrate a 'very high' risk, reflecting their potential to facilitate the movement, concealment, and integration of illicit proceeds. Weak compliance and internal controls are assessed as a 'high' risk factor that may further increase exposure. Overall, the average risk score of 17.8 places tax-related ML risk within the 'very high' category, highlighting the need for strengthened risk-based supervision, effective customer due diligence, beneficial ownership transparency, transaction monitoring, and inter-agency cooperation.

The tax-related ML risk assessment used a risk-based approach, which considered the likelihood and potential impact on Namibia's financial system. Five key risk drivers were assessed: tax evasion, cross-border transactions, cash-intensive businesses, complex ownership structures, and weaknesses in compliance and internal controls. The assessment was informed by FIC financial intelligence, STRs/SARs, identified cases, reporting trends, and information from competent authorities. Each risk driver was assigned a likelihood and impact score from 1 (very low) to 5 (very high).

The risk score was calculated by multiplying likelihood by impact. Scores of 1 to 4 are rated as low, 5 to 9 as moderate, 10 to 15 as high, and 16 to 25 as very high. The five assessed risk drivers produced an average score of 17.8 (overall score: average of the five risk-driver scores = $[25 + 20 + 16 + 16 + 12] \div 5 = 17.8$),

resulting in an overall 'very high' inherent ML risk rating. The rating reflects the level of risk before consideration of mitigating controls and should be reviewed periodically as new intelligence, cases, and reporting trends become available.

8.4 Corruption-related offence risk analysis

In Namibia, corruption risks are particularly associated with sectors involving public procurement, natural resources, infrastructure, and government-related transactions. Effective mitigation requires strong AML/CFT/CPF controls, including enhanced due diligence, beneficial ownership transparency, transaction monitoring, suspicious transaction reporting, and cooperation among competent authorities. Strengthening these measures supports the detection, prevention, and disruption of corruption-related ML risks while protecting the stability and reputation of Namibia's financial system. This section demonstrates corruption-related risk analysis.

8.4.1 Corruption-related risk cycle

The risk cycle illustrates how illicit benefits are generated, concealed, and integrated into the legitimate economy. It typically begins with the abuse of entrusted power through activities such as bribery, embezzlement, or procurement fraud, followed by the movement and concealment of illicit proceeds through financial systems, businesses, or complex ownership structures. The final stage involves the integration of laundered funds into the economy through investments, assets, or legitimate-looking transactions, allowing criminals to enjoy the proceeds of corruption.

Table 19: Corruption-related risk cycle

Stage of risk cycle	Description	Examples / risk indicators
1. Corruption opportunity	Abuse of entrusted power or position for personal or third-party benefit.	Bribery, kickbacks, conflict of interest, abuse of authority, favouritism
2. Generation of Illicit proceeds	Corrupt activities to generate illegal financial gains or assets.	Misappropriation of public funds, procurement fraud, illicit payments, inflated contracts
3. Concealment and layering	Criminals attempt to disguise the origin and ownership of corruption proceeds.	Use of shell companies, third parties, trusts, complex transactions, offshore accounts, cash movements
4. Integration into the economy	Laundered funds are introduced into legitimate economic activities.	Real estate purchases, investments, businesses, luxury assets, unexplained wealth accumulation
5. Reinvestment and continuation of corruption	Illicit proceeds are used to maintain influence, expand networks, or finance further corrupt activities.	Political influence, repeat fraud schemes, continued procurement manipulation, funding of associates
6. Detection and response measures	Authorities and reporting entities identify, investigate, and disrupt corruption-related financial flows.	STRs, financial intelligence analyses, asset recovery, law enforcement actions

Effective AML/CFT/CPF controls, including customer due diligence, beneficial ownership transparency, transaction monitoring, and law enforcement cooperation, are essential to interrupt this cycle and prevent corruption-related proceeds from entering the financial system.

8.4.2 Corruption-related risk matrix

The corruption-related risk matrix assesses the likelihood and impact of corruption-related offences and their potential effect on the financial system. It considers key risk factors such as the opportunity for abuse, exposure to illicit financial flows, and the effectiveness of existing controls.

Table 20: Corruption-related risk assessment matrix

Risk category	Description	Risk level	Impact on financial system	Key mitigation measures
Public procurement fraud	Manipulation of tender processes, bid rigging, kickbacks, and inflated contracts	Very high	Very high	Procurement oversight, enhanced due diligence, independent audits, transparency in procurement
Money laundering of corruption proceeds	Concealment of illicit proceeds through shell companies, complex ownership structures, real estate, and cross-border transfers	Very high	Very high	Transaction monitoring, beneficial ownership verification, suspicious transaction reporting, financial intelligence analysis
Prominent influential persons (PIPs)	Abuse of public office, conflicts of interest, and unexplained wealth involving public officials	High	High	Source of wealth and source of funds verification, enhanced due diligence, ongoing monitoring
State-owned enterprises	Weak governance, procurement irregularities, and misuse of public resources	High	High	Strengthened corporate governance, compliance reviews, internal and external audits
Mining and natural resources	Bribery, illegal licensing, royalty evasion, and corruption in extractive industries	High	High	Regulatory oversight, licensing transparency, inter-agency cooperation, continuous supervision
Misappropriation of public funds	Diversions, embezzlement, or unauthorised use of government funds and assets	High	High	Strong financial controls, forensic audits, segregation of duties, regular monitoring
Private sector corruption	Commercial bribery, fraudulent accounting, and unethical business practices	Medium	Medium	Corporate governance, ethics programmes, internal compliance controls, staff training
Cross-border corruption and asset transfers	Movement of illicit funds through international financial systems, offshore accounts, and foreign investments	Very high	Very high	International cooperation, International co-operation, sanctions screening, cross-border transaction monitoring, information sharing

The matrix indicates that corruption-related risks present a 'high' to 'very high' threat due to the ability of corruption offences to generate significant illicit proceeds and facilitate ML. Public procurement, misuse of public funds, and laundering of corruption proceeds represent the highest risk areas because they involve substantial financial flows, complex ownership structures, and potential cross-border movement of funds.

Effective mitigation requires enhanced due diligence for high-risk customers, strengthened beneficial ownership transparency, improved monitoring of PIPs, increased suspicious transaction reporting, and enhanced cooperation between the FIC, LEAs, supervisory authorities, and the Anti-Corruption Commission.

8.5 Stakeholder questionnaire: Summary of key findings

To support the assessment of Namibia's financial system integrity, the FIC conducted a stakeholder questionnaire across reporting institutions and competent authorities. The questionnaire assessed governance, risk management, customer due diligence, transaction monitoring, suspicious transaction reporting, beneficial ownership, emerging risks, supervisory effectiveness, and inter-agency cooperation. Overall, the responses indicate that institutions have made significant progress in strengthening AML/CFT/CPF controls, although several operational and systemic challenges remain.

Table 21: Consolidated key findings

Theme	Key findings
Governance and risk management	Most institutions reported that AML/CFT/CPF governance is well established, with the Board and senior management providing regular oversight. The NRA is widely used to inform institutional risk assessments and control measures.
Policies and compliance	Respondents indicated that AML/CFT/CPF policies are generally effective and are reviewed periodically to remain aligned with legislative and regulatory requirements.
Customer due diligence	Institutions reported the effective implementation of customer due diligence measures; however, challenges remain in verifying beneficial ownership, foreign legal entities, PIPs, and obtaining reliable customer information.
Transaction Monitoring and suspicious transaction reporting	Most institutions have implemented automated or semi-automated transaction monitoring systems and indicated improvements in the quality and timeliness of suspicious transaction reporting. Resource constraints, data quality issues, and occasional system outages continue to affect reporting effectiveness.
TF and PF risk management	Larger institutions generally assess terrorist financing and proliferation financing risks separately from money laundering, although respondents noted the need for additional guidance, specialised training, and typology information.
Training and awareness	Regular AML/CFT/CPF training is conducted across most institutions, contributing to improved compliance awareness and reporting capabilities.
Emerging risks	The most frequently identified emerging risks include cyber-enabled fraud, virtual assets, trade-based money laundering, public sector corruption, cash-intensive businesses, cross-border financial crime, and the misuse of non-profit organisations.
Financial intelligence and information sharing	Financial intelligence provided by the FIC is generally regarded as useful; however, respondents highlighted opportunities to improve feedback mechanisms, information sharing, and coordination among competent authorities.
Supervisory and enforcement effectiveness	Institutions acknowledged improvements in supervisory engagement but identified the need for greater consistency in enforcement, additional sector-specific guidance, and enhanced investigative capacity.
Cross-border cooperation	Respondents noted that increasing international transactions have heightened ML/TF/PF exposure; however, delays in obtaining information from foreign counterparts remain a challenge for effective investigations.

8.5.1. Overall AML/CFT/CPF maturity assessment

Maturity level	Percentage of respondents
Advanced	 45%
Established	 35%
Developing	 15%
Limited	 5%

Most institutions have established AML/CFT/CPF programmes, although a smaller proportion still require significant capacity building.

8.5.2. Most significant financial crime risks

Cyber-enabled fraud	 92%
Corruption	 88%
Money laundering	 84%
Trade-based money laundering	 72%
Virtual assets	 65%
Terrorist financing	 55%
Proliferation financing	 42%

While cyber-enabled fraud (92%) and corruption (88%) were identified as the most significant threats to financial system integrity, money laundering (84%) remains a major risk that enables organised crime. Criminals launder proceeds derived from offences such as fraud, corruption, tax evasion, drug trafficking, wildlife crime, and diamond smuggling through cash transactions, shell companies, cross-border transfers, trade-based money laundering schemes, and virtual assets. This high risk rating highlights the continued vulnerability of the financial and designated non-financial sectors to the concealment and movement of illicit funds, underscoring the need for robust preventive and detection measures.

8.5.3. Key operational challenges

Challenge	Identifying the issue (%)
Beneficial ownership verification	81%
Cross-border information sharing	74%
Digital fraud investigations	69%
Skilled AML personnel	63%
Quality of customer information	58%
Legacy information technology (IT) systems	47%

8.5.4. Effectiveness of anti-money laundering controls

Control area	Rating
Customer due diligence	 High
Transaction monitoring	 High
Suspicious transaction reporting	 High
Sanctions screening	 Moderate
Beneficial ownership verification	 Moderate
Politically exposed persons monitoring	 Moderate
TF/PF controls	 Developing

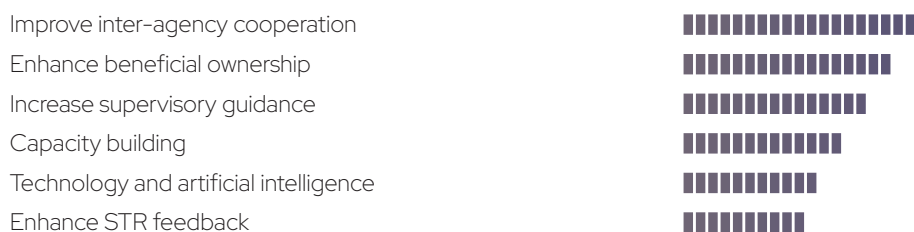
8.5.5. Heat map of risk areas

Risk area	Risk level
Corruption	Very high
Cybercrime	Very high
Fraud	Very high
Trade-based money laundering	High
Cross-border cash movement	High
Virtual assets	High
Terrorist financing	Medium
Proliferation financing	Medium

The risk assessment indicates that corruption, cybercrime, and fraud represent the highest threats to Namibia's financial system, reflecting their significant potential to generate illicit proceeds and facilitate ML. Trade-based money laundering, cross-border cash movement, and virtual assets are assessed as 'high' risk areas due to their increasing complexity, cross-border nature, and potential to exploit regulatory vulnerabilities.

In contrast, terrorist financing and proliferation financing are currently assessed as 'medium' risks. Although these threats are less prevalent, they remain important areas for ongoing monitoring because of evolving international risks and Namibia's obligations to comply with global AML/CFT/CPF standards. Overall, the findings highlight the need for continued risk-based supervision, enhanced transaction monitoring, stronger inter-agency cooperation, and effective implementation of preventive controls to safeguard the integrity and stability of the financial system.

8.5.6. Stakeholder priorities



The findings indicate that strengthening inter-agency cooperation is the highest priority for stakeholders, highlighting the importance of enhanced collaboration and information sharing among competent authorities to effectively combat financial crime. Stakeholders also identified the need to improve beneficial ownership transparency and enhance supervisory guidance as critical in order to strengthen compliance, transparency, and risk management across reporting entities.

In addition, respondents emphasised the need for capacity building and a greater adoption of technology and artificial intelligence (AI) to improve the detection of suspicious activities, as well as enhanced feedback on STRs to improve reporting quality and support more effective AML/CFT/CPF compliance. Collectively, these priorities reinforce efforts to strengthen the integrity, resilience, and effectiveness of Namibia's financial system.

8.5.7. Executive control panel

Indicator	Assessment
Overall AML/CFT/CPF maturity	Established
Governance	Strong
Reporting quality	Improving
Emerging risks	High
Technology readiness	Moderate
Cross-border risk	High
Compliance culture	Strong
Financial system integrity	Stable

This assessment indicates that Namibia has an established AML/CFT/CPF framework, supported by strong governance structures, a positive compliance culture, and a stable financial system. Reporting quality has continued to improve, reflecting increased awareness, strengthened compliance measures, and enhanced reporting by financial institutions and other reporting entities.

Despite these strengths, emerging financial crime risks and cross-border risks remain significant and require continued attention. While technology readiness is assessed as 'moderate', further investment in advanced technologies, data analytics, and digital monitoring capabilities would strengthen the detection and prevention of ML, TF, and PF. Overall, the findings suggest that continued enhancement of risk-based supervision, inter-agency cooperation, and technological capabilities will further reinforce the integrity and resilience of Namibia's financial system.

8.6 Overall observations

- » Governance and AML/CFT/CPF compliance frameworks continue to mature across reporting institutions.
- » The NRA is increasingly placed into institutional risk management and compliance programmes.
- » Customer due diligence and transaction monitoring have improved; however, beneficial ownership verification remains a common challenge.
- » Reporting quality has strengthened, supported by ongoing staff training and improved monitoring systems.
- » Digitalisation, virtual assets, cybercrime, corruption, trade-based money laundering, and cross-border financial crime were consistently identified as the most significant emerging threats.
- » Stakeholders emphasised the need for stronger inter-agency cooperation, enhanced supervisory guidance, improved beneficial ownership transparency, and increased operational capacity to sustain the effectiveness and integrity of Namibia's AML/CFT/CPF framework.

The analysis of key risks confirms that fraud, corruption, and tax-related offences remain the most significant threats to Namibia's financial system, as per the current NRA, due to their ability to generate substantial illicit proceeds and facilitate money laundering.¹ Stakeholder feedback indicates that institutions have generally strengthened governance, compliance, customer due diligence, transaction monitoring, and reporting practices. However, challenges remain in beneficial ownership verification, digital fraud investigations, cross-border information sharing, and managing emerging risks associated with cybercrime, virtual assets, trade-based money laundering, and corruption. Overall, the findings suggest that Namibia's AML/CFT/CPF framework is increasingly mature and effective, but continued efforts are required to enhance resilience against evolving financial crime risks.



Financial system integrity implication

Integrity implication: The assessment confirms that Namibia's financial system remains stable and supported by strong governance and compliance structures, despite exposure to significant domestic and international financial crime risks.

Effectiveness implication: Improved AML/CFT/CPF maturity, stronger reporting quality, and enhanced risk management demonstrate growing effectiveness across reporting institutions and competent authorities.

Policy implication: Strategic focus should remain on beneficial ownership transparency, emerging technology risks, inter-agency cooperation, advanced analytics, and strengthening controls relating to corruption, cybercrime, and cross-border financial crime.

The analysis presented in this report indicates that Namibia has continued to strengthen its AML/CFT/CPF framework. However, emerging financial crime threats, technological developments, and increasing cross-border financial activities require continuous enhancement of regulatory, supervisory, and operational capabilities. The following strategic recommendations are proposed to further strengthen the integrity, resilience, and stability of Namibia's financial system.

9.1 Policy and regulatory recommendations

Strategic priority area	Key recommendations	Expected outcomes
Legislative and regulatory framework	Continue to strengthen AML/CFT/CPF legislation, beneficial ownership transparency, and targeted financial sanctions to remain aligned with FATF Standards	Improved regulatory compliance and transparency
Risk-based supervision	Enhance supervisory activities using a risk-based approach, with greater focus on high-risk sectors such as banking, VASPs, DNFBPs, and cross-border transactions	More effective supervision and early identification of emerging risks
Financial intelligence	Improve the quality and timeliness of STRs, expand intelligence analysis, and strengthen strategic and operational intelligence products	Improved detection and disruption of illicit financial activities
Technology and innovation	Increase the use of artificial intelligence, data analytics, and automated transaction monitoring to identify complex financial crime patterns	Enhanced detection of ML, TF, PF, fraud, and cyber-enabled crime
Emerging risk management	Strengthen oversight of virtual assets, cybercrime, trade-based money laundering, corruption, and cross-border financial flows	Improved mitigation of emerging and evolving financial crime risks
Compliance and governance	Promote stronger customer due diligence, enhanced due diligence for high-risk customers, beneficial ownership verification, and sanctions screening	Stronger institutional compliance and reduced financial crime vulnerabilities
Capacity building	Deliver specialised AML/CFT/CPF training, sector-specific guidance, and awareness programmes for reporting institutions and competent authorities	Improved technical capacity and reporting quality
Inter-agency cooperation	Expand information sharing, joint investigations, and operational collaboration between the FIC, supervisory authorities, LEAs, customs, tax authorities, and prosecutors	Improved coordination and more effective enforcement outcomes
International cooperation	Strengthen collaboration with foreign FIUs, international organisations, and regional partners to combat cross-border financial crime	Enhanced management of transnational ML/TF/PF risks
Public-Private Partnership	Promote regular engagement with reporting entities through typology reports, outreach programmes, and strategic feed-back on suspicious transaction reporting	Stronger AML/CFT/CPF compliance culture and improved reporting effectiveness

9.2 Strategic priorities

Based on the findings of this report, the strategic priorities that should guide future AML/CFT/CPF efforts include:

- » **strengthen beneficial ownership transparency** to reduce the misuse of legal entities;
- » **enhance supervision of emerging technologies**, including virtual assets and digital financial services;
- » **improve the quality and effectiveness of suspicious transaction reporting** across all reporting sectors;
- » **strengthen intelligence-led supervision and enforcement** through enhanced analytical capabilities and the use of technology;
- » **increase investment in digital monitoring tools**, artificial intelligence, and advanced data analytics;
- » **enhance inter-agency and international cooperation** to address cross-border financial crime and illicit financial flows;
- » **build institutional capacity** through specialised training, sector-specific guidance, and continuous awareness programmes; and
- » **promote a risk-based and collaborative AML/CFT/CPF framework** that supports financial inclusion while safeguarding the integrity, resilience, and stability of Namibia's financial system.





The findings of this Financial System Integrity Report indicate that Namibia has continued to strengthen its AML/CFT/CPF framework through legislative reforms, enhanced supervision, improved financial intelligence capabilities, and greater collaboration among competent authorities. The analysis demonstrates that the country's financial system remains stable and resilient, supported by strong governance, an established AML/CFT/CPF framework, and improving reporting quality. However, increasing digitalisation, cross-border financial activities, and technological innovation continue to expose the financial sector to evolving risks, particularly corruption, fraud, cyber-enabled crime, trade-based money laundering, virtual asset-related risks, and illicit financial flows. These developments underscore the importance of maintaining a proactive, intelligence-led, and risk-based approach to safeguarding the integrity of the financial system.

Overall, the report concludes that while Namibia has made significant progress in strengthening its financial system integrity, continued efforts are required to address emerging risks and enhance the effectiveness of the national AML/CFT/CPF regime. Priority should be given to strengthening beneficial ownership transparency, improving the quality of financial intelligence, enhancing inter-agency and international cooperation, expanding the use of advanced technologies, and building institutional capacity across reporting entities and competent authorities. Sustained implementation of these measures will reinforce public confidence, support compliance with international standards, and ensure that Namibia's financial system remains transparent, resilient, and capable of preventing and detecting financial crime while supporting sustainable economic growth.

BIBLIOGRAPHY

Bank of Namibia. (2024). Annual Report 2024. Windhoek, Namibia.

Bank of Namibia. (2024). Financial Stability Report 2024. Windhoek, Namibia.

Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG). (2023). Annual Report 2022-2023. Dar es Salaam, Tanzania.

Egmont Group of Financial Intelligence Units. (2024). Annual Report 2023-2024. Ottawa, Canada.

Financial Action Task Force (FATF). (2020). Trade-Based Money Laundering: Trends and Developments. Paris, France.

Financial Action Task Force (FATF). (2021). Guidance on Proliferation Financing Risk Assessment and Mitigation. Paris, France.

Financial Action Task Force (FATF). (2023). Illicit Financial Flows from Corruption. Paris, France.

Financial Action Task Force (FATF). (2023). Crowdfunding for Terrorist Financing. Paris, France.

Financial Intelligence Centre. (2024). Annual Report 2023/24. Windhoek, Namibia.

Financial Intelligence Centre. (2025). National Risk Assessment on Money Laundering, Terrorist Financing and Proliferation Financing. Windhoek, Namibia.

Government of the Republic of Namibia. (2012). Financial Intelligence Act, 2012 (No. 13 of 2012), as amended. Windhoek, Namibia.

Government of the Republic of Namibia. (2023). AML/CFT/CPF Regulations. Windhoek, Namibia.

Namibia Statistics Agency. (2024). Annual National Accounts 2024. Windhoek, Namibia.

Southern African Development Community (SADC). (2024). Annual Report 2023/24. Gaborone, Botswana.

United Nations Office on Drugs and Crime (UNODC). (2023). World Drug Report 2023. Vienna, Austria.

United Nations. (2004). United Nations Convention against Corruption (UNCAC). New York, NY.

United Nations Security Council. (2024). Reports on Terrorist Financing and Proliferation Financing Sanctions. New York, NY.

World Bank. (2023). Global Findex Database 2023. Washington, DC.



www.fic.na | enquiries@fic.na

44 Nickle Street, Prosperita
PO Box 2882, Windhoek, Namibia

Phone: +264 61 283 528 / 5179 / 5100

Email: helpdesk@fic.na