The Eswatini Financial Intelligence Centre

Money Laundering and Terrorism Financing

Typologies Report

2022-2024

+268 2405 9000

www.efic.org.sz

Contents

Acronyms

DNFBP's	- Designated non-financial businesses and professions
EFIC	- Eswatini Financial Intelligence Centre
ESAAMLG	- Eastern and Southern Africa Anti-money Laundering Group
FATF	- Financial Action Task Force
KYC	- Know your customer
LEAS	- Law Enforcement Agencies
MLFTP Act amended	- Money Laundering and Financing of Terrorism Prevention Act 2011 as
NRA	- National Risk assessment
Person	- Natural or legal person
STR	- Suspicious Transaction Report
UBO	- Ultimate Beneficial Owner

MESSAGE FROM THE DIRECTOR GENERAL

It is my pleasure to present this typology report prepared by the Eswatini Financial Intelligence Centre (EFIC). The report reflects the Centre's ongoing commitment to combating money laundering and terrorist financing (ML/TF) and to safeguarding the integrity of Eswatini's financial system. It draws on ML/TF risks identified through national AML/CFT risk assessments and financial intelligence held by the EFIC, with a focus on key trends, emerging risks and the most prevalent money laundering typologies affecting the country.

The purpose of this report is to provide accountable institutions, LEA's, competent authorities, and policymakers with practical and actionable insights to strengthen the identification, assessment, and mitigation of ML/TF risks. It also serves as a reference tool to promote a shared understanding of ML/TF risks among domestic and international stakeholders. With the continued support of Government and in close collaboration with AML/CFT stakeholders, the EFIC remains committed to fulfilling its mandate. Stakeholders are encouraged to utilize the findings of this report to inform their risk assessments, supervisory frameworks, and investigative strategies.

EXECUTIVE SUMMARY

The Eswatini Financial Intelligence Centre (EFIC) has prepared this typology report in accordance with its statutory mandate under Section 31(d) of the Money Laundering and Financing of Terrorism Prevention Act, 2011 (as amended), which requires the Centre to analyze and assess reports and information through both operational and strategic analysis. The report is further aligned with Section 31 (l) and Recommendation 29 of the Financial Action Task Force (FATF) Standards, which "*requires Financial Intelligence Units conduct strategic analysis, to identify money laundering and terrorist financing trends and patterns using available and obtainable information, including information from other competent authorities.*

This report focuses on the most prevalent money laundering and terrorist financing typologies to which the Eswatini financial system is exposed. It is based on analysis conducted by the EFIC, supplemented by information obtained from competent authorities, LEA's, and foreign Financial Intelligence Units. The report examines methods used by criminals to commit predicate offences and highlights relevant typologies, indicators, and red flags associated with these activities.

The findings are intended to support accountable institutions in identifying and mitigating emerging risks, assist supervisory authorities in strengthening oversight, and enhance the investigative capacity of LEAs. By providing typologies, trends and risk indicators, the report promotes early detection of financial crime, disruption of illicit financial flows, and more effective allocation of resources through a risk-based approach. In addition, typology reports serve as an important investigative tool by identifying criminal patterns, emerging threats, and linkages between seemingly unrelated cases.

OBJECTIVES

This study aims to enhance understanding of how criminals generate, move, conceal and launder the proceeds of crime, as well as finance terrorism. Specifically, it seeks to:

- Identify emerging and persistent typologies of money laundering (ML) and terrorist financing (TF) observed in Eswatini between 2022 and 2024.
- Highlight emerging trends, vulnerabilities, and methods exploited within accountable institutions.
- Examine techniques used to exploit regulatory and operational gaps.
- Strengthen detection and investigative capabilities, supporting the development of AML/CFT policies.
- Provide practical, implementable recommendations to inform policy and operational responses by relevant authorities and stakeholders.
- Enhance the understanding of patterns, methods, and red flags associated with ML/TF among accountable institutions and LEA's.
- Support sectoral risk assessments and reinforce compliance frameworks, particularly in high-risk sectors.
- Promote proactive collaboration between reporting institutions and LEA's in detecting and reporting suspicious activities.
- Raise public awareness regarding the methods used by criminals to launder proceeds of crime or finance terrorism.

INTRODUCTION

The Eswatini Financial Intelligence Centre (EFIC) is established under Section 19 of the Money Laundering and Financing of Terrorism Prevention Act, 2011 (as amended), as the national centre responsible for the receipt, analysis and dissemination of financial intelligence to LEA's and other competent authorities. In this role, the EFIC supports the detection,

prevention and combating of money laundering, terrorist financing and related financial crimes.

The EFIC became fully operational in February 2017, serving as the centre for the receipt and analysis of suspicious transaction reports (STRs) and disseminating financial intelligence to LEAs and competent authorities, such as the Eswatini Revenue Service (ERS), Royal Eswatini Police Service (REPS) and the Anti-Corruption Commission (ACC). The EFIC also collaborates regionally with other FIUs, through its membership in the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) to align Eswatini's AML/CFT framework with the best international practices.

In terms of the MLFTP Act, the EFIC is mandated to receive the following reports:

- **Suspicious Transaction Reports (STRs)** (Section 12(1)(a), read with Section 31(a)): Submitted by accountable institutions when there is suspicion of money laundering, terrorist financing or proliferation financing.
- **Attempted Suspicious Transaction Reports** (Section 12(1)(a), read with Section 31(a)): Reports relating to suspicious transactions that were attempted but not completed.
- **Cash Threshold Reports (CTRs)** (Legal Notice No. 88 of 2024, issued under Section 12 bis): Threshold reports for cash transactions exceeding E25,000 or its equivalent in foreign currency.
- **Cross-Border Currency Declarations** (Section 41): Reports on persons entering or exiting Eswatini with currency or monetary instruments exceeding the prescribed threshold of E25,000.

The EFIC conducts typology studies based on the analysis of STRs, and other financial intelligence received from accountable institutions and competent authorities. As aforementioned this report is intended to assist accountable institutions, LEA's and other stakeholders in identifying, understanding and responding to money laundering and terrorist financing threats and vulnerabilities within Eswatini.

OVERVIEW OF STRs REPORTED TO THE EFIC

This section summarizes STRs submitted by accountable institutions between 2022 and 2024. It outlines how the EFIC assesses, analyses and disseminates these reports to LEA's, while providing feedback to help improve reporting quality and strengthen AML/CFT compliance programmes.

General Observations

During the period 2022- 2024, the EFIC observed the following recurring patterns in STRs submitted by reporting institutions:

- Large cash deposits into personal accounts without clear or declared sources of income.
- Immediate transfers following large cash deposits, often to foreign destinations.
- Use of third parties or nominees, including minors and relatives, to receive or transfer funds.
- Account activity which is inconsistent with KYC profiles or declared occupations.
- The use of social engineering techniques to defraud persons.

IDENTIFIED LOOPHOLES IN THE FINANCIAL SYSTEM

Eswatini's Cash-Based Economy

Despite efforts to digitalize payments, Eswatini remains largely cash dependent. Many sectors, such as retail, transport, and construction, operate heavily in cash, creating opportunities for placement of illicit funds into the financial system.

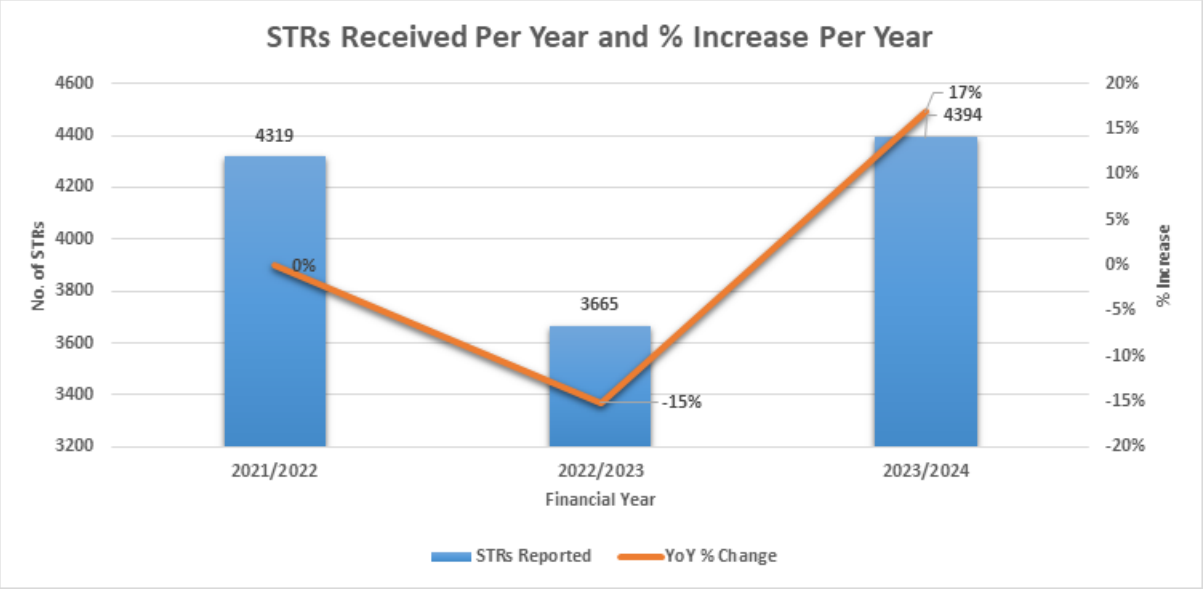
Cash Deposits and Withdrawals

The anonymity provided by cash transactions enables concealment of illicit sources. Weak controls in deposit and withdrawal monitoring increase the risk of undetected ML/TF, cash threshold reports are yet to be received.

Low reporting of other sectors

Some sectors have not been reporting STR's due to the infancy of their AML/CFT compliance frameworks resulting in unreported suspicious activity and enabling launderers to exploit compliance gaps as shown below:

Chart 1: STRs Received from Accountable Institutions



MONEY LAUNDERING TYPOLOGIES

This section outlines the observed predicate offences that are contributing to money laundering and the different sectors that have been exploited.

Tax crimes/evasion.

Eswatini's tax framework comprises various forms of taxation, including income tax, value-added tax (VAT), corporate tax and excise duties, all of which are essential to domestic revenue mobilisation. Tax evasion constitutes a criminal offence and arises where a person wilfully fails to comply with lawful tax obligations as they fall due. In Eswatini, tax evasion is criminalised under the Income Tax Order, 1975 and the Money Laundering and Financing of Terrorism Prevention (MLFTP) Act, 2011, as amended.

The 2023 NRA identified tax evasion as one of the principal predicate offences generating proceeds that are frequently laundered domestically. Analysis further indicates that a significant proportion of Suspicious Transaction Reports (STRs) submitted to the Eswatini Financial Intelligence Centre (EFIC) are associated with suspected tax evasion activities.

A prevalent typology involves the deliberate use of personal bank accounts to conduct business transactions in order to conceal taxable income, evade tax obligations or reduce declared tax liabilities. Individuals commonly implicated in such practices include sole traders, shareholders, employees and other related parties.

Additional methods observed include the channelling of business proceeds through accounts held in the names of minors, as well as the use of multiple bank accounts linked to front companies where beneficial ownership is deliberately obscured. Sectors frequently associated with these practices include retail, electronics and wholesale trade, travel agencies, grey import motor vehicle dealerships, illegal money-lending activities and illicit cigarette smuggling operations.

The predominance of sole proprietorships in Eswatini presents heightened tax compliance risks, particularly where business funds are co-mingled with the personal finances of the owner. While accountable institutions routinely encourage sole traders to open and utilise dedicated business accounts, it has been observed that some customers continue to use personal accounts for both business and personal purposes. In certain cases, business accounts are opened in compliance with institutional requirements, but remain dormant, with transactional activity continuing through personal accounts. The case study below illustrates this typology.

The case studies below are typical examples.

Case study 1- the use of personal accounts

The subject, a non-Swazi national, was found to be using his personal bank account for business activities. The individual is not registered for tax purposes. Analysis of the account revealed large cash deposits of a business nature, structured to avoid detection and reporting thresholds. Further investigation identified links between the subject and several non-Swazi individuals, who were also operating business activities through personal accounts. Transaction patterns between the subject and associates were similar, with funds transferred to the same beneficiary and references in transactions showing notable overlaps. All were associated with the same residential address.

During the reporting period, the subject received approximately E11,209,896.00, predominantly in cash, structured to circumvent reporting requirements. A significant portion of these funds was subsequently transferred to foreign jurisdictions, primarily through South Africa, using fintech platforms. These transfers lacked supporting

documentation, suggesting potential involvement in capital flight, tax evasion and money laundering.

Indicators and Red flags

- *Non-declaration of VAT returns.*
- *Frequent cash deposits just below reporting thresholds.*
- *Regular, large transfers to foreign jurisdictions via fintech platforms.*

A trend which was also observed during the period, is the use of minor's accounts for purposes of evading tax. This concealment strategy usually involves a parent or guardian transferring or depositing income or business proceeds into the account of the minor to obscure ownership and reduce the taxable income.

Case study 2- the use of a minor's account

Analysis identified a case involving a subject who was a minor whose parents opened a personal bank account on his behalf. The account was subsequently used to receive multiple cash deposits and business-related transactions. Transaction descriptions associated with outgoing payments clearly reflected commercial activity.

Over a period of approximately fifty (50) months, total credits received into the minor's account exceeded **E 6 million**. The volume, frequency and value of transactions were inconsistent with the minor's age and declared source of funds, which was reported as an allowance. The activity strongly indicated the use of the minor's account to conceal the true ownership and source of business income, likely for the purpose of tax evasion.

Indicators and Red Flags

- *Account activity in a minor's personal account inconsistent with the age, profile, and declared source of funds.*
- *Use of a minor's account to receive business-related proceeds.*
- *High transaction volumes and values inconsistent with legitimate allowance-based income.*

- *Transaction references indicating commercial or business activity in a personal account.*

Recommendations

- Accountable institutions should extend transaction monitoring beyond registered business accounts to include the personal accounts of shareholders, proprietors, close family members and key employees, in order to identify linked transactions and potential misuse.
- LEA's should adopt a risk-based approach that includes scrutiny of personal accounts held by shareholders, promoters, proprietors, key staff and their close associates during tax assessments and other financial investigations.
- Given that tax evasion is a high proceeds-generating predicate offence, LEA's should prioritise its investigation. Where tax evasion is identified during parallel investigations, authorities should also consider the associated money laundering offences to ensure that illicit proceeds and assets are effectively identified, restrained and confiscated.

Fraud

Fraud is the "misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment".[1] It refers to the deliberate misrepresentation or concealment of a material fact with the intent to induce another party to act to their detriment, thereby obtaining an unlawful benefit. It constitutes a criminal offence involving deception for financial or other gain. Increasingly, fraudsters exploit human behaviour, often the weakest element within security frameworks, through social engineering techniques designed to manipulate individuals into disclosing sensitive information or authorising financial transactions.

The 2023 Eswatini National Risk Assessment (NRA) identified fraud as a significant predicate offence generating substantial illicit proceeds. Fraud is observed across multiple sectors and analysis of Suspicious Transaction Reports (STRs) submitted to the Eswatini Financial Intelligence Centre (EFIC) during the 2022–2024 period indicates a notable increase in fraud-related activity. Based on this analysis, intelligence products were developed and disseminated to relevant LEA's to support investigative actions.

[1] Black's Law Dictionary

Fraud- mobile money fraud known as the Facata scam in Eswatini.

These scams typically involve impersonation, social engineering and the fraudulent use of SIM cards to unlawfully access and steal funds from victims' mobile money wallets. Perpetrators commonly pose as government officials, including police officers or representatives of the Office of the Deputy Prime Minister, in order to gain victims' trust. The perpetrators are predominantly youth aged between 24 and 29 years and primarily target vulnerable groups, including the elderly, young people and the unemployed.

Analysis of Suspicious Transaction Reports (STRs) indicates that multiple mobile phone numbers are used to receive illicit proceeds, with certain numbers being shared among different individuals. This pattern suggests coordination and the involvement of organised criminal networks. One of the most prevalent fraud typologies identified during the reporting period is the Facata scam. A significant proportion of STRs analysed were linked to fraud-related activity, with multiple indicators substantiating the suspicions. Based on these findings, intelligence products were developed and disseminated to relevant LEA's to support investigative and enforcement actions, and several arrests were made on the perpetrators.

Case study 3- social engineering

In this typology, the perpetrator contacts victims through phone calls or text messages, falsely claiming that funds have been mistakenly transferred into the victim's mobile money account. The perpetrator then requests the victim to "return" the funds and provides step-by-step instructions on how to reverse the purported transaction.

Victims typically do not verify their mobile money account balances or transaction histories prior to initiating the reversal. As a result, they are deceived into transferring their existing balances to mobile phone numbers controlled by the perpetrator. The fraud is only discovered after the victim realises that no erroneous credit had occurred and that their funds have been unlawfully transferred

Indicators and Red Flags

- *Requests to reverse or return funds relating to a transaction that never occurred.*
- *Urgent or persistent instructions to act immediately, discouraging verification.*
- *Caller claims to represent a company, government institution or service provider but uses a personal mobile number.*

- *Guidance provided on transaction steps rather than directing the victim to official customer service channels.*
- *Sudden withdrawals or transfers following suspicious or unverified communications.*
- *Claims that the victim qualifies for a special government programme or benefit as a pretext for engagement.*

Case study 4- impersonation fraud

The Eswatini Financial Intelligence Centre (EFIC) received multiple Suspicious Transaction Reports (STRs relating to mobile money fraud cases in which victims were induced into disclosing sensitive personal and financial information. A common tactic involved impersonation fraud, whereby perpetrators posed as technical support or cybersecurity personnel in order to obtain victims' mobile money (MoMo) access credentials.

In one reported case, the perpetrator claimed to be an officer from the Royal Eswatini Police Service (REPS), allegedly attached to the cybersecurity unit. The perpetrator informed the subject (victim) that their mobile phone and MoMo account had been compromised by hacking malware and claimed to have the technical capability to remove the threat. By creating a sense of urgency and authority, the perpetrator convinced the subject that immediate action was required to prevent further losses.

The subject was persuaded to disclose their MoMo login credentials under the pretext of receiving assistance. Upon obtaining the credentials, the perpetrator accessed the victim's MoMo account without authorisation and transferred and further withdrew funds amounting to E 12,000, resulting in financial loss to the subject.

Indicators and Red Flags

- *Unsolicited contact offering digital security or cybersecurity assistance.*
- *Relies on establishing institutional authority to encourage compliance e.g. claims to be with LEA's, telecommunications providers or cybersecurity units without verifiable credentials.*
- *Creation of urgency by asserting that the victim's device or account is "hacked," "infected" or "compromised."*
- *Representation that only the suspect can resolve the alleged problem.*
- *Informal provision of technical services in public or non-professional settings.*

- *Sudden or unexplained mobile money withdrawals or transfers following interaction with the suspect.*

Observations in the Facata Fraud

Analysis of STRs indicates that mobile money fraud, particularly Facata-type scams, exhibits several distinctive risk characteristics:

Victim Profile:

Mobile money services are designed as financial inclusion products and are accessible to both banked and unbanked populations. A significant proportion of users have low levels of financial and digital literacy, which fraudsters exploit through social engineering and deception techniques.

Accessibility:

Mobile money platforms are widely accessible and operate on a 24/7 basis, significantly expanding the potential victim pool. Of the 2,359 STRs received by the EFIC relating to mobile money fraud, 1,457 involved successful fraudulent transactions, while 902 reflected attempted but unsuccessful fraud.

Geographical Separation:

Facata scam fraud is predominantly conducted remotely, with no physical interaction between perpetrators and victims. This enables fraudsters to operate across different geographic locations while minimising the risk of physical identification.

Recommendations

- Enhance public awareness in Eswatini through targeted education initiatives, awareness campaigns and media outreach to promote vigilance and fraud prevention.
- Encourage the public to safeguard personal and financial information and refrain from sharing account credentials with any third parties.
- Urge mobile money operators, remittance service providers and relevant authorities to conduct regular fraud risk assessments and implement proportionate mitigation measures, including clear customer guidance on recognising and reporting scams.
- Introduce fintech regulatory sandboxes to pilot, test and implement innovative fraud detection and prevention technologies and services.

Case study 5-Use of fake invoices

The Eswatini Financial Intelligence Centre (EFIC) received several Suspicious Transaction Reports (STRs relating to employee-driven invoice fraud. Invoice fraud typically involves a perpetrator submitting false or manipulated invoices purporting to originate from legitimate suppliers, often accompanied by notifications that payment details have changed, thereby redirecting payments to accounts controlled by the fraudster.

In this case, the subject, employed as a financial accountant, received funds into her personal account from what appeared to be her employer, with transaction references reflecting the employer's initials ("XXX"). Individual transactions ranged between E 40,000 and E 100,000 and occurred frequently, in some instances more than twice per month.

Financial analysis conducted by the EFIC revealed that the proceeds were utilised for cash withdrawals, lifestyle-related expenditure and transfers to a motor vehicle dealership. Additional beneficiary accounts were identified during the analysis. The transactions displayed a recurring pattern of duplicated payments with varying amounts, a common typology in cases involving false invoicing by employees.

Further investigation established that the subject had misappropriated in excess of **E 7 million** from her employer.

Indicators and Red Flags

- *Frequent receipt of funds with transaction references indicating the employer's name.*
- *Subject occupying a position of trust within the company, particularly in finance or accounting.*
- *Immediate or rapid withdrawals following large credits.*
- *Repetitive or duplicated transactions with similar characteristics.*

Recommendations

- Ensure segregation of duties between invoice approval, payment authorization and the reconciliation function.
- Conduct risk-based audits of procurement and accounts payable processes.
- Implement confidential whistle-blowing measures

- Ensure parallel financial investigation are conducted with every procurement corruption investigation, expedite investigations and the prosecution of procurement related matters.
- Ensure the collection and development of UBO information registries.

Fraud- Ponzi scheme

A Ponzi scheme is a form of investment fraud that is presented as a legitimate investment opportunity. The scheme relies on misrepresentation, whereby the operator promises high or guaranteed returns that are not generated from legitimate business activity. Instead, returns paid to earlier investors are sourced from funds contributed by new investors, creating a false impression of profitability and sustainability, which eventually crashes, with "investors" incurring losses as a result.

Case study 6- Ponzi scheme

Four individuals acting as promoters of ABC Investment Limited, to operate a fraudulent investment scheme that targeted members of the public. ABC Investment Limited was promoted as a high-return investment opportunity through seminars, presentations and social media referrals. The entity was neither licensed nor regulated in Eswatini and was not authorised to offer or advertise capital market products or services. The promoters failed to disclose the high-risk nature of the investment and did not inform investors that they stood to benefit personally from the scheme.

Investors were enticed with promises of exorbitant returns of up to 400 per cent. Funds were deposited directly into the personal bank accounts of the four promoters. Upon receipt, the promoters shared a portion of the funds among themselves, while the remaining amounts were transferred to cryptocurrency accounts and to various entities located in South Africa.

Indicators and Red Flags

- *Investment entities operating without regulatory approval or licensing.*
- *Promotion of investment opportunities through social media and informal channels.*
- *Promises of exceptionally high returns within short timeframes.*
- *Representations that investments carry little or no risk.*
- *Difficulty or delays in withdrawing invested funds.*
- *Claims of proprietary or undisclosed trading software.*

- *Failure to disclose promoters' personal financial interests in the investment.*

Recommendations to mitigate the risks of Ponzi scheme fraudulent activities.

- Integrate Ponzi scheme risk indicators into supervisory risk assessments and prioritise oversight of sectors frequently exploited by such schemes.
- Strengthen the investigative and prosecutorial capacity of LEA's responsible for financial crimes.
- Increased social media monitoring to spot new Ponzi schemes being marketed early.

CONCLUSION

This typology report examines the primary money laundering (ML) and terrorist financing (TF) risks facing Eswatini, drawing on Suspicious Transaction Reports (STRs) and other financial intelligence received by the Eswatini Financial Intelligence Centre (EFIC) between 2022 and 2024. The analysis highlights how proceeds from key predicate offences, including tax evasion, fraud, Ponzi schemes and illicit drug trafficking are generated, laundered and integrated into the financial system.

Criminals continue to exploit vulnerabilities across multiple sectors, including banking, money transfer services, mobile money platforms and personal bank accounts. Key risk factors include the misuse of personal and minors' accounts, high reliance on cash, involvement of nominees, and third parties and the rising prevalence of technology-enabled fraud schemes. Notably, mobile money related fraud has contributed to increased STR reporting, reflecting both greater financial inclusion and heightened ML/TF exposure.

The report identifies recurring typologies, case studies and red-flag indicators that underscore the importance of:

- **Strengthening preventive measures:** including robust customer due diligence, ongoing transaction monitoring and transparency of beneficial ownership (Immediate Outcome 4).
- **Further enhancing financial intelligence:** improving the collection, analysis and dissemination of financial data to support investigations (Immediate Outcome 6).
- **Coordinating law enforcement and prosecution:** prioritising investigative and prosecutorial actions against ML/TF and predicate offences (Immediate Outcome 7).
- **Timely asset tracing and confiscation:** recovering illicit proceeds and disrupting criminal networks (Immediate Outcome 8).

The findings reinforce the need for a coordinated, risk-based approach among accountable institutions, supervisory authorities, LEA's and the EFIC to strengthen AML/CFT effectiveness. Stakeholders are encouraged to conduct sectoral risk assessments, improve customer due diligence and ensure effective monitoring and reporting of suspicious transactions. The EFIC remains committed to providing strategic and operational financial intelligence to support national AML/CFT objectives and safeguard the integrity of Eswatini's financial system in line with international standards.