SOUTH AFRICAN RESERVE BANK

Prudential Authority

Money Laundering, Terrorist Financing and Proliferation Financing Sector Risk Assessment for the South African Banking Sector

December 2025

Contents

Executive Summary

The South African banking sector includes local and foreign banks, mutual banks and cooperative banks, and is a central feature of and vital contributor to the national economy, offering essential financial products and services. The banking sector is dominated by six large banks, which together hold 92.8% of the total banking sector assets.

This Sector Risk Assessment (SRA), conducted by the Prudential Authority (PA), and provides a comprehensive evaluation of the money laundering, terrorism financing and proliferation financing (ML/TF/PF) risks in South Africa's banking sector, covering a three-year (36 month) period from January 2022 to December 2024.

The SRA draws on a wide range of data sources, including risk returns, intelligence reports, 2022 National Risk Assessment, 2024 Terrorism Financing National Risk Assessment and the 2024 Banking Association of South Africa (BASA) Proliferation Financing Threat Assessment, and seeks to strengthen the ML/TF/PF risk awareness across the banking sector, to inform a risk-based compliance and supervisory approach, and to contribute to South Africa's broader efforts to combat financial crime and ensure a more resilient financial system.

Inherent Risks

The inherent money laundering risks in the banking sector have been assessed as high for all large, medium and small domestic banks, medium-high for foreign banks, medium for mutual banks and medium-low for co-operative banks.

The inherent terrorist financing risks is high for large banks, medium for small-to-medium banks and foreign banks and low for mutual and co-operative banks.

The inherent proliferation financing risks is high for large banks, medium for small-to-medium banks and foreign banks and low for mutual and co-operative banks

This differentiation reflects the concentration of activity and the varying operating models across bank types, particularly retail scale, product breadth, cross-border connectivity and complexity of client structures.

Large domestic banks play a pivotal role within South Africa's financial system by acting as primary channels for high-volume retail payments, significant cash placements, and cross-border fund movements. Due to their extensive reach, broad product offerings, and extensive and complex client bases, large banks are inherently exposed to elevated risks. Their position as central gateways for both domestic and international financial flows means that large volumes of transactions, both in cash and through digital channels, pass through these banks, increasing the likelihood that illicit funds can be placed, layered, or integrated within the financial system.

Furthermore, the high degree of cross-border connectivity, combined with the complexity of client structures found in large banks, heightens their risk exposure, reinforcing the assessment that large banks face inherently higher levels of ML/TF/PF risks.

Small-to-medium domestic banks, despite holding a smaller share of sector assets compared to their larger counterparts, play a significant role in the South African banking landscape by serving nearly half of all banking customers. This extensive customer reach results in high volumes of both cash and digital transactions processed through these institutions. As a consequence, small-to-medium domestic banks are materially exposed to the risk of proceeds from domestic predicate-offences being introduced into the financial system. The combination of substantial transaction volumes and broad customer access makes these banks particularly vulnerable to ML risks.

Foreign banks generally have limited retail exposure but increased cross-border exposure through intra-group flows and complex corporate/offshore structures and, in some cases, private banking services, which elevate layering risk and supports a higher inherent ML rating.

Mutual and cooperative banks are comparatively small and largely domestically focused, with simpler business models and lower cross-border connectivity, which reduces inherent TF and PF exposure, however, cash-intensive segments and more manual processes can still sustain ML exposure.

Inherent Risks	Domestic banks		Foreign banks	Mutual banks	Co-operative banks
	Large banks	Small- to-medium banks			
Money Laundering	High	High	Medium-high	Medium	Medium-low
Terrorist Financing	High	Medium	Medium	Low	Low
Proliferation Financing	High	Medium	Medium	Low	Low

Mitigating Controls

Mitigating controls introduced by banks, as well as supervisory measures implemented by the PA, including strong market-entry controls, risk-based inspections, effective remediation processes and the imposition of dissuasive administrative sanctions, together with the PA's ongoing outreach and awareness initiatives to enhance the sector's resilience to financial crime, have contributed to reducing the inherent MT/TF/PF risks.

While controls across most subsectors are assessed as broadly adequate, the SRA observed control weaknesses, notably for PF, more frequently among smaller banks, although these institutions also have lower inherent exposure to PF channels.

The control areas requiring enhancement, are governance, the enhancement of business risk assessments, the implementation of customer due diligence, verification of beneficial ownership information, transaction monitoring, training programmes and reporting.

Mitigating Controls	Domestic banks		Foreign banks	Mutual banks	Co-operative banks
	Large banks	Small-to-medium banks			
Money Laundering	Adequate	Adequate	Adequate	Adequate	Non-existent
Terrorist Financing	Adequate	Adequate	Adequate	Adequate	Non-existent
Proliferation Financing	Adequate	Weak	Weak	Weak	Non-existent

Residual Risks

The overall residual risk ratings for ML/TF/PF risks in the South African banking sector are therefore as follows:

Residual Risks	Domestic banks		Foreign banks	Mutual banks	Co-operative banks
	Large banks	Small-to-medium banks			
Money Laundering	Medium-high	Medium-high	Medium	Medium-low	Medium-low
Terrorist Financing	Medium-high	Medium-low	Medium-low	Low	Low
Proliferation Financing	Medium-high	Medium	Medium	Low	Low

Overall, the banking sector's residual ML/TF/PF risk remains elevated, reflecting that material risk persists even after mitigating controls are applied.

1. Introduction

This third SRA, conducted by the PA, provides a comprehensive assessment of the inherent ML/TF/PF risks within the South African banking sector for the period of January 2022 to December 2024 (referred to as the 'review period'), that seeks to identify, assess and enhance awareness, deepen understanding of these risks and contribute to South Africa's broader efforts to combat financial crime and ensure a resilient financial system.

The findings of this SRA are intended to inform banks of the specific ML/TF/PF risks associated with this sector, which should be considered when implementing targeted measures and controls to mitigate such risk, to ultimately contribute to the overall reduction of ML/TF/PF activity.

This report should also serve as a guide to regulators, supervisors and policymakers, notably the South African Reserve Bank (SARB), Financial Intelligence Centre (FIC), Financial Sector Conduct Authority (FSCA) and National Treasury of South Africa, by providing insights into the identified ML/TF/PF risks facing the sector, which may inform future policymaking decisions.

Specifically, the SRA should assist in the application of risk-based supervisory measures based on a thorough understanding of threats, vulnerabilities and consequences at sectoral level, as well as an analysis of the effectiveness of existing mitigating controls.

Identifying, understanding and prioritising these financial crime risks should raise awareness within the sector and ensure that banks allocate adequate resources and implement tailored controls to effectively manage their risk exposure.

2. The mandate of the Prudential Authority

In terms of schedule 2 of the Financial Intelligence Centre Act 38 of 2001 (FIC Act), the PA is the designated supervisory body for banks, mutual banks and cooperative banks, which are classified as accountable institutions (AIs) in terms of schedule 1 of the FIC Act.

The PA's primary mandate as a FIC Act supervisor is to ensure that banks, mutual banks and cooperative banks comply with the legal obligations aimed at preventing and combating ML/TF/PF as imposed by the FIC Act on the banking sector.

The PA is thus responsible for supervising the banking sector, to assess their level of compliance with their FIC Act obligations and improve their compliance behaviour, which ultimately should minimise the occurrence of ML, TF and PF activity within the sector.

Fundamental to the improvement of compliance behaviour is the promotion of the understanding of ML, TF and PF risks, while ensuring alignment by the sector with both national legislation and international standards established by the Financial Action Task Force (FATF) and the Basel Committee on Banking Supervision (BCBS).

The PA is also a regulator in terms of Financial Sector Regulation Act 9 of 2017, the Banks Act 94 of 1990, the Mutual Banks Act 124 of 1993 and the Co-Operative Banks Act 40 of 2007, which collectively regulate the South African banking industry, ensuring its financial soundness, adherence to good governance practices and effective risk management, including those related to financial crime risks.

Through its regulatory and supervisory activities, the PA aims to safeguard the integrity of the South African financial system, protect consumers and ensure that the banking sector operates in a manner that is consistent with South Africa's commitment to international standards that seek to combat ML, TF and PF.

3. Definitions

This SRA references the following key terms and definitions:

- *Money Laundering (ML):* any person who knows or ought reasonably to have known that property is or forms part of the proceeds of unlawful activities and:

  (a) enters into any agreement or engages in any arrangement or transaction with anyone in connection with that property, whether such an agreement, arrangement or transaction is legally enforceable or not; or

  (b) performs any other act in connection with such a property, whether it is performed independently or in concert with any other person, which has or is likely to have the effect of:

    (i) concealing or disguising the nature, source, location, disposition or movement of said property, its ownership or any interest which anyone may have in respect thereof; or

    (ii) enabling or assisting any person who has committed or commits an offence, whether in South Africa or elsewhere:

  (c) to avoid prosecution; or

  (d) to remove or diminish any property acquired directly or indirectly as a result of the commission of an offence, shall be guilty of an offence;[1]

- *Terrorist Financing (TF):* the act of collecting or providing property, a financial or other service, or economic support, directly or indirectly, with the intention that the property or services be used, or knowing that they may be used, in whole or in part, to carry out a terrorism act;[2]

[1] See section 4 of the Prevention of Organised Crime Act 121 of 1998.

[2] See section 4 of the Protection of Constitutional Democracy Against Terrorist and Related Activities Act 33 of 2004.

- *Proliferation Financing (PF):* an activity which has or is likely to have the effect of providing property, a financial or other service, or economic support, to a non-state actor, which may be used to finance the manufacture, acquisition, possessing, development, transport, transfer or use of nuclear, chemical or biological weapons and their means of delivery, and which includes any activity that constitutes an offence in terms of section 49A of the FIC Act;[3]

- *Risk:* a risk is a function of three factors – namely threat, vulnerability and consequence – and occurs when a threat successfully takes advantage of a vulnerability to produce a consequence;[4]

- *Threat:* activities, individuals or entities that have the potential to cause harm through ML/TF/PF, including criminal actors, terrorist groups, proliferators and their facilitators;

- *Vulnerability:* features within a sector that can be exploited by a threat or that may support or facilitate its activities (e.g. criminal actors), including any weaknesses or gaps in controls, sector-specific product vulnerabilities or systemic weaknesses within the sector;

- *Consequence:* the impact or harm that ML/TF/PF may cause to an institution, sector or country, including reputational damage, financial losses, societal harm and the undermining of national or international financial systems;

- *Mitigating Controls:* strategies, measures or actions put in place to reduce the likelihood or impact of risks associated with a particular threat or vulnerability, including laws, policies, procedures, technologies, guidelines, training programmes as well as regulatory or supervisory frameworks aimed at preventing, detecting or responding to risks effectively; the strength and effectiveness of mitigating factors and controls is determined by their ability to successfully address and mitigate the identified risks, where strength refers to the robustness, reliability and resilience of

[3] See section 1 of the FIC Act.

[4] See FATF 2024 National Risk Assessment Guidance.

these measures while effectiveness pertains to their actual impact in reducing the likelihood or severity of risks;

- *Inherent Risk:* the level of ML/TF/PF risk present in the sector before applying any controls; while existing controls may mitigate some risk, inherent risk represents the vulnerabilities intrinsic to the sector's operations; and

- *Residual Risk:* the ML/TF/PF risk that remains after AML/CFT/CPF mitigating controls have been applied to address inherent risk.

4. Methodology

4.1 Assessment approach

The methodology used in this SRA is based on FATF guidance, which considers risk as a function of three factors, namely threats, vulnerabilities and consequences.

This assessment is calibrated to South Africa's most recent national risk outputs, namely the 2022 National Risk Assessment (NRA) and subsequent TF/PF work, as well as to FATF Recommendation 1 updated to require jurisdictions and institutions to identify, assess, understand and mitigate ML/TF/PF risks.

The SRA provides a structured approach for identifying, assessing and managing ML/TF/PF risks within the banking sector and discusses the types of threats, vulnerabilities and mitigating controls applicable to the sector, to determine residual risk.

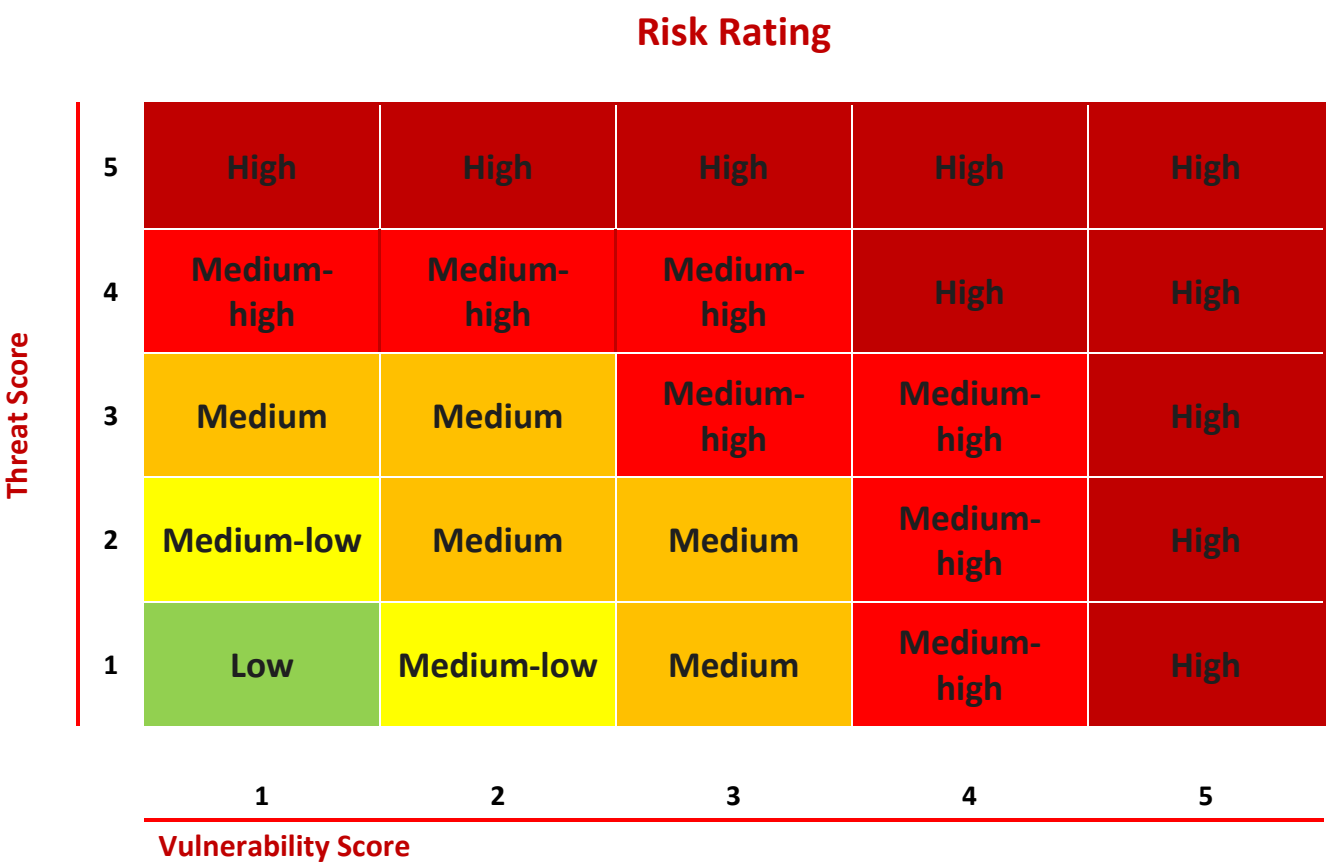
FATF Recommendation 6 and 7, guidance issued by the FATF, open searches for publicly available information as well as the FIC's Public Compliance Communication (PCC) 44A operational guidance. was considered for the purpose of considering TF and PF risk, including TFS risk.

Additionally, given the concentration within the banking sector, the approach for the analysis in this SRA was to differentiate risk between large, medium and small domestic banks, foreign banks, mutual banks and co-operative banks.

The assessment of risk in the banking sector is both qualitative and data-driven, and involves gathering extensive data from various sources, analysing the data and identifying the key threats, vulnerabilities and potential consequences associated with ML/TF/PF. The qualitative analysis allows for a nuanced understanding of these risks, considering factors such as the complexity of banking products and customer behaviour.

The risk-rating categories, illustrated in Figure 1 have been considered to evaluate risk as a function of threats and vulnerabilities, as presented in the heat map below:

Figure 1: Heat map



Based on the figure above, when the threat score (y-axis) and the vulnerability score (x-axis) converge in the heat map, the risk rating increases by one rating (e.g. a medium-high threat score and a medium-high vulnerability score = high risk score). This exemplifies the interaction between threats and vulnerabilities insofar as they maximise each other's impact in the overall inherent risk.

Risk ratings

Risk ratings have been categorised as follows:

Risk Ratings:	High	Medium-high	Medium	Medium-low	Low

Mitigating control ratings

Mitigating control ratings have been categorised as follows:

Mitigating Controls:	Non-existent	Weak	Adequate	Effective

4.2 Assessment scope

This assessment aims to evaluate the ML/TF/PF risks within the South African banking sector during the review period and includes both domestic and foreign banks, mutual banks and co-operative banks, each presenting distinct operational models and vulnerabilities.

To allow for more granular analysis, domestic banks are further segmented into small to medium and large domestic banks and recognising that these subgroups have varying risk profiles.

For purposes of this SRA large domestic banks refers to the six banks with the highest total asset size over the review period. All remaining domestic banks, based on total asset size, are classified as small-to-medium domestic banks.

Foreign banks are branches of foreign banks and/or foreign-controlled banks licensed to operate within the South African banking sector.

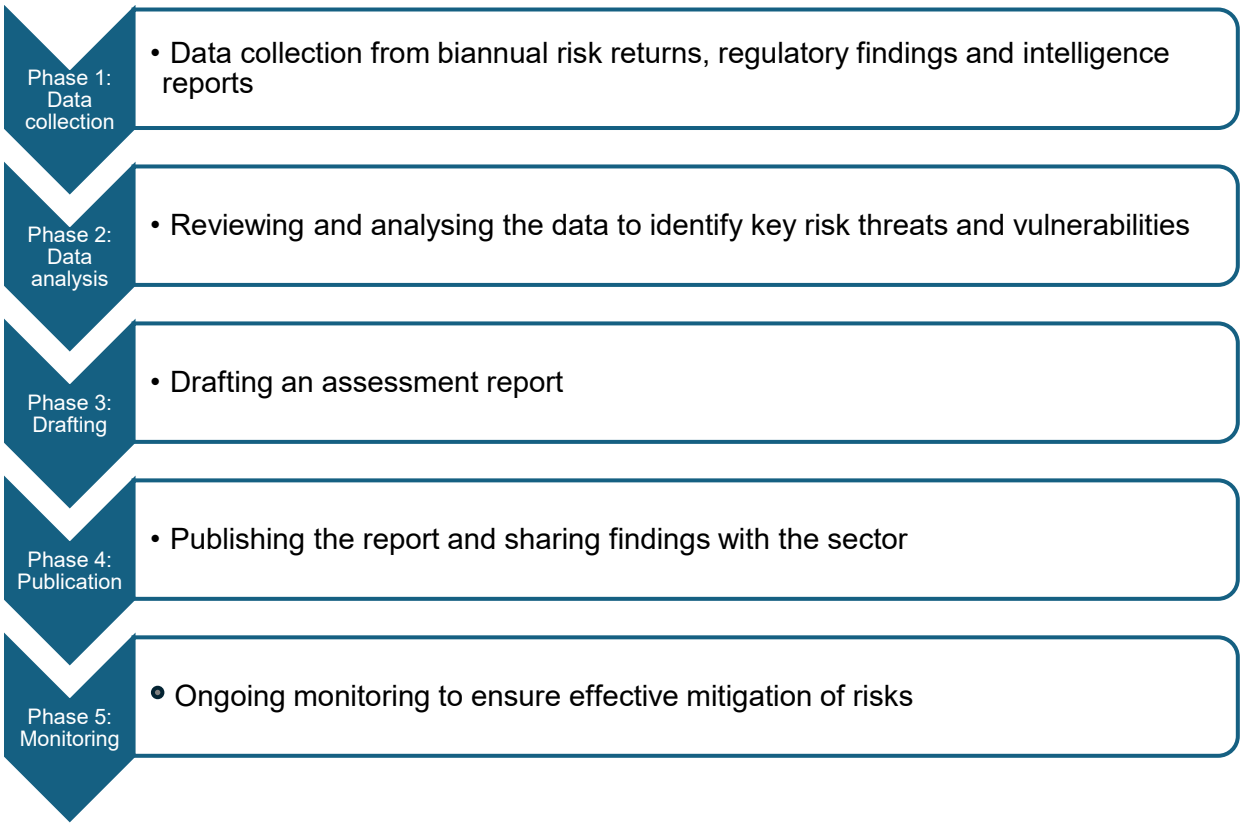
Mutual banks are banks licensed as deposit-taking financial institutions operating within the South African banking sector in terms of the Mutual Banks Act 124 of 1993 (Mutual Banks Act), and are owned by its depositors who qualify as members by virtue of their shareholding in the bank, and are entitled to participate in the exercise of control in a general meeting of that mutual bank and receive dividends.

Co-operative banks are banks licensed as deposit-taking financial institutions operating within the South African banking sector in terms of the Co-operative Banks Act 40 of 2007 (Co-operative Banks Act), characterised by an accepted common bond of association and wholly owned and controlled by its members, to which it provides financial products and services.

4.3 Assessment phases

This SRA was carried out through the following phases:

Figure 2: Assessment phases



4.4 Data sources

The assessment draws on intelligence and data from a variety of sources over the review period to ensure a comprehensive and comparative analysis, and includes data from:

- the AML/CFT/CPF risk returns submitted to the PA;

- regulatory findings, including data from an analysis of compliance assessment outcomes, inspection reports and investigations conducted by the PA and other relevant supervisory authorities;

- financial crime intelligence, including data from the FIC and other law enforcement agencies, on financial crime typologies, trends and case studies specific to the banking sector;

- the national and sector risk assessments, including the 2022 NRA, the 2024 TF NRA and the 2023 Co-operative Banks Sector Risk Assessment;

- business risk assessments submitted by banks to the PA to evaluate the inherent ML, TF and PF risks at institutional level;

- inspection reports issued by the PA, which highlight compliance deficiencies and gaps in the implementation and effectiveness of AML/CFT/CPF frameworks;

- thematic reviews conducted by the PA across the banking sector;

- formal requests for information, including data submitted by the FIC and law enforcement bodies to the PA;

- international financial crime reports, including reports from the FATF, BCBS and the Egmont Group, focusing on global insights on ML/TF/PF risks and emerging threats;

- publicly available information, statistics and articles from international organisations and authors; and

- policy and legislative reviews, including examinations of South African legislation, particularly the FIC Act as well as the directives, guidance notes and public compliance communications issued in terms thereof, to understand their implications for AML/CFT/CPF obligations within the banking sector.

4.5 Assessment participants

The SRA was led by the PA, with data received from the banking sector, the SARB Financial Surveillance Department (FinSurv), the State Security Agency and the FIC. Additional information was also requested from law-enforcement agencies and other central banks.

4.6 Limitations

While the SRA provides valuable insights into ML/TF/PF risks, some limitations may affect the completeness of the findings. Notably, the assessment relied on information submitted by the banking sector via risk returns, inspection reports, publicly available reports and open-source information. Additionally, data quality may vary due to data completeness and the accuracy of self-reported information.

Furthermore, not all suspicious activities are identified or reported by the banking sector, and criminals may employ other sophisticated methods to evade detection, resulting in undetected risks that are not reflected in this analysis.

Finally, South Africa is currently conducting an update to its ML/TF/PF NRA, and the findings from these assessments have not been published and thus could not be reflected in this SRA.

5. Overview of the banking sector

The banking sector in South Africa plays an essential role within the country's financial system, supporting the economy and offering a wide range of banking services and products to natural and legal persons.

As of December 2024, the South African banking sector included 55 licensed banks as indicated in Table 1 below.

Table 1: Licensed banks in South Africa

Banks per sector		No. of banks
Banks	Local Banks	16
	Foreign Banks	11
Mutual Banks		3
Co-operative	Cooperative Banks	5
	Cooperative Financial Institutions	20
Total		**55**

Asset size and customer base

As of December 2024, the banking sector served approximately 80.2 million clients.

The sector is dominated by six large banks, which together hold 92.78% of the total banking sector assets, as detailed Table 2 below.

Table 2: Assets and customer distribution as of December 2024

	Asset size	% of total assets	No. of customers	% of total customers
Large banks	R7 607 billion	92.78%	64 470 593	80.37%
Small-to-medium banks	R109 billion	1.33%	15 524 907	19.35%
Foreign banks	R479 billion	5.84%	61 648	0.08%
Mutual banks	R4.1 billion	0.05%	154 034	0.19%
Co-operative banks	R583 million	0.01%	5 778	0.01%
Total	**R8 199 billion**	**100%**	**80 216 960**	**100%**

Large domestic banks offer a comprehensive and broader range of products and services compared to the remaining banks within this sector, and act as financial hubs, providing access both within the continent and internationally, maintaining extensive regional networks in sub-Saharan Africa and global financial centres, and holding most correspondent banking relationships.

6. Threats

6.1 Money laundering threats

South Africa's large and diversified economy, well-developed financial system and strategic geographic location make it a potential target for illicit financial flows, posing a substantial threat to the integrity of the financial system, with the banking sector being primarily vulnerable to threat actors wishing to exploit possible vulnerabilities in the sector.

South Africa faces a relatively high volume and intensity of crime and as a result, significant ML threats primarily stemming from predicate offences such as fraud, corruption, bribery, tax evasion, drug trafficking, theft, robbery and smuggling. High levels of organised crime further exacerbate these threats, with criminals exploiting vulnerabilities in both financial and non-financial sectors.

These offences generate the largest, most recurrent, and most banking-embedded criminal proceeds in South Africa, evidenced across suspicious transaction report (STR) and suspicious activity report (SAR) patterns, supervisory intelligence and case outcomes. Each of these threats have been profiled on Table 3 below, highlighting dominant typologies, channels and banking-sector exposure.

Based on STRs and SARs data received from the FIC for the review period, the following top 10 offences have been identified as posing the greatest financial crime risks to the banking sector.

Table 3: STR/SAR filed by type of offence

Offence	Number of reports filed	Percentage of reports filed
Fraud − general	104 638	47%
Cybercrime	22 360	10%

Fraud − front/fictitious companies	21 975	10%
Money laundering	20 293	9%
Fraud − public sector/ tenders	16 135	7%
Corruption/bribery	10 860	5%
Fraud − 419 scams	7 666	3%
Fraud − Ponzi scheme	4 048	2%
Theft/robbery	2 830	1%
Smuggling	1 973	1%

6.1.1 Fraud

Fraud is defined as unlawful and intentional misrepresentation which causes actual or potential prejudice to another. This can include various forms of deceit, such as false statements, concealment of information or any other deceptive practices intended to gain an unfair advantage or cause harm to another party.

Fraud is the most reported financial crime compared to other offences. According to the FIC, romance/love scams, advance fee fraud and lottery scams were prevalent in terms of in-flow transactions to South Africa. Out-flow of funds from South Africa were predominantly remitted to the Democratic Republic of Congo, Pakistan, China and Kenya, originating mostly from STRs filed in the Gauteng province.

Other prevalent crimes include Facebook scams, airtime and data scams, deposit scams, car sale scams and cybercrimes, which pose an ever-increasing threat to both businesses and individuals, due to evolving technological advancements and a lack of awareness.

Case Study 1: Unemployment insurance fraud
This case involved submission of fraudulent claims under the Unemployment Insurance Fund's Temporary Employment Relief Scheme, which when detected and analysed by the FIC, with support from the Fusion Centre and the South African Anti-Money Laundering Integrated Task Force (SAMLIT), resulted in 21 section 34 interventions, securing R26.5 million from multiple bank accounts for illicit transactions from 2015 to 2022.
Case Study 2: Online pyramid scheme collapses
Through regulatory reports filed by financial institutions, negative media coverage and a request for information from a law enforcement agency, the FIC became aware of a pyramid scheme with 21 individuals and one entity laundering the proceeds from the pyramid scheme. The FIC issued directives to secure some R8 million held across 54 bank accounts.
Case Study 3: Fraudulent Workman's Compensation Fund claims
Fraudulent Workman's Compensation Fund uncovered claims involving 77 primary bank accounts, with an additional 757 beneficiary accounts, used to disperse the proceeds between 2015 to 2022. Forfeiture orders were obtained against 15 bank accounts amounting to R3.39 million.
Case Study 4: Personal protection equipment fraud
Investigations into the unlawful awarding of a contract to two companies for the procurement of personal protection equipment (PPE) resulted in the Special Investigations Unit recovering R26.5 million. The proceeds of the unlawfully awarded PPE contract(s) were paid via the formal banking system into the service provider's

business account(s). The funds were then rapidly dispersed through multiple onward electronic transfers to other entities' bank accounts (i.e., "layering"/pass-through activity) in an apparent attempt to dissipate and obscure the audit trail before intervention. In PPE-related matters, the SIU described instances where substantial amounts were moved from a supplier's bank account to numerous other entities shortly after payment, prompting urgent freezing interventions and subsequent recovery/forfeiture processes.[5]

Case Study 5: Government buildings not sanitised

The detection of fraudulent allocation of tenders to sanitise government buildings during the COVID-19 pandemic, involving 46 companies and more than 500 accounts, resulted in 26 accounts being frozen, securing R65 million and eight vehicles to the value of R6 million.

Case Study 6: Theft of R2 million

A government department was defrauded of R2 million, which was laundered through 59 bank accounts, involving 27 individuals and 22 companies. R257 438.00 was recovered through a preservation order and criminal charges of fraud, theft and money laundering charges were laid.

6.1.2 Corruption and bribery

Corruption and bribery involve abuse of entrusted power or authority for personal gain, typically through solicitation or acceptance of bribes, kickbacks or other illicit payments.

Proceeds are commonly obscured through shell/repurposed companies, nominee accounts and complex transaction chains to conceal origin and frustrate accountability.

[5] See https://www.gov.za/news/media-statements/special-investigating-unit-release-report-finalised-investigations-and

SAMLIT's corruption analysis[6] shows persistent entry via public procurement and licensing abuses often featuring newly formed or repurposed companies, politically exposed persons (PEP) / prominent influential persons (PIP) and close associates, that bypassed weak supplier vetting controls. Frequent indicators include entities with less than 12 months' operating history, missing/invalid sector registrations, non-VAT-registered suppliers issuing VAT-inclusive invoices and pricing anomalies. Funds are moved through multiple personal, business and third-party accounts, with round-figure credits, rapid dispersals/cash-outs, dormant-to-active spikes, inter-account 'loan' transfers and occasional cross-border electronic funds transfer (EFTs), before integration via high-value asset purchases and early debt settlements. These features align with supervisory intelligence and STR/SAR patterns, explaining why corruption/bribery remains a banking-embedded ML threat.

Although progress has been made post State Capture[7], corruption continues to erode service delivery, investor confidence and institutional capacity. Transparency International's 2024 Corruption Perceptions Index (CPI) scored South Africa 41/100 (rank 83/180), signalling sustained governance pressure. The Zondo Commission documented the scale and mechanics of the State Capture, with a cost estimate of approximately R250 billion.[8] While prosecutions and recoveries continue, corruption/bribery remains an ongoing ML exposure for banks.

Key features and indicators (for risk assessment and monitoring):

- Entry typologies: Newly created/shelf companies winning emergency or irregular tenders; entities pivoting into unrelated goods/services shortly before award, beneficial ownership or effective control by PEPs/PIPs or close associates.

---

[6] See https://www.banking.org.za/wp-content/uploads/2023/11/SAMLIT-EWG-Corruption-Report-2023.pdf

[7] FATF (2021), Mutual Evaluation Report – South Africa, October 2021. The MER notes public-sector corruption (including 'State capture') as a significant AML/CFT weakness and records its substantial economic impact and negative effects on national security.

[8] Judicial Commission of Inquiry Report into allegations of State Capture, Corruption and Fraud in the Public Sector, including organs of state, also known to the public and the media as the Zondo Commission. Chairperson: Justice R.M.M. Zondo, Chief Justice of the Republic of South Africa. Part VI Vol. 4: Summary of Recommendations: Page 174-176. https://static.pmg.org.za/State_Capture_Commission_Report_Part_VI_Vol_IV.pdf.

- Process red flags: Pre-tender manipulation (specification rigging, compressed timeframes), exclusionary criteria, post-award change orders and inflated invoices, weak delivery/performance documentation.

- Banking red flags: Large round-amount credits from government/state-owned entity (SOE) payors, immediate automated teller machine (ATM)/cash-send withdrawals and bulk EFT dispersals to related parties, back-to-back 'loan' transfers among linked entities, dormant-to-active spikes, early settlement of vehicle/asset finance, cross-border wires with vague rationales (e.g. 'gift' and/or 'consulting').

- Regulatory gaps exploited: Missing/invalid sectoral registrations or licences, VAT anomalies (suppliers without VAT registration issuing VAT-inclusive invoices), fragmented supplier databases across spheres of government.

Case Study 7[9]: PPE tender to construction company (nepotism; missing sector registration)
A construction company owned by a provincial deputy chairperson's daughter received a COVID-19 PPE contract (R1.1 million) despite no medical-supply experience and the company was not registered with the South African Health Products Regulatory Authority (SAHPRA) to distribute medical devices. This highlights nepotism/patronage risk and weak supplier vetting.
Case Study 8: Soap bars procurement (ministerial family link; VAT anomaly)
A company directed by a former minister's family member was asked to quote for soap bars in March 2020 and was contracted for R2.79 million just seven months after incorporation; the firm was not VAT-registered and reportedly received R1.65 million from the former minister's personal bank account, profiting R1.14 million.

[9] All case studies can be found in *SAMLIT Corruption Expert Working Group Report:* https://www.banking.org.za/wp-content/uploads/2023/11/SAMLIT-EWG-Corruption-Report-2023.pdf

Case Study 9: Surgical masks contract 66 days after incorporation (regulatory non-compliance)
A newly registered supplier was awarded a R5.694 million mask contract and paid R5.4 million within weeks; the firm had no SAHPRA registration and charged VAT while not VAT-registered. Timing and regulatory gaps indicate elevated corruption/ML risk.
Case Study 10: Tender to politician's driver (experience versus requirement mismatch)
A well-known politician's driver was awarded a R27.8 million university renovation tender, despite an unrelated employment profile, illustrating influence/undue preference and a classic 'experience versus requirement' red flag.
Case Study 11: Water treatment works − PEP associate overpayments
A district municipality awarded a project where the winning company (linked to a prominent politician's associate) was paid R71.9 million after tendering for a contract valued at R47 million (overpayment R24 million). PEP proximity, pricing anomalies and post-award adjustments signal heightened corruption/ML exposure.

6.1.3 Theft/robbery

Theft involves unlawfully taking someone else's property with the intent to permanently deprive them of it. When theft occurs, the stolen assets or funds become illicit proceeds. Common scenarios include business email compromises, racketeering, currency speculation, credit card skimming, precious metals and minerals theft, stolen cars and smuggling.

Other notable crime trends involve fuel theft, with various methods employed. These include redirecting tanker trucks, fuel theft by employees, cloning fuel cards and engaging in fraud and corruption within the petroleum industry. Additionally, fuel scams and trading with sanctioned entities have been observed.

6.1.4 Drug trafficking

Drug trafficking remains a major concern for South Africa and is one of the most prevalent forms of transnational organised crime that has significantly proliferated in South Africa over the last decade, with the South African Police Service (SAPS) reporting 49 015 drug-related crimes for the fourth quarter of 2024.[10]

South Africa has seemingly evolved into a consumer, producer and transit country for drugs, driven by socio-economic factors such as poverty, inequality and unemployment. The rising demand for drugs has led to a surge in drug manufacturing, smuggling and consumption, posing significant threats to national security, economic growth and sustainable development.

The illicit drug trade generates substantial illicit cash proceeds, heightens ML risks and negatively impacts the country's economic development. Drug trafficking, intertwined with other forms of organised crime, drives illicit activities such as wildlife and human trafficking. Organised crime syndicates, linked to foreign networks, control the drug trade and fuel violence in gang-contested areas.

While South Africa has traditionally been a transit and consumer country, the proliferation of narcotics laboratories indicates its growing role as a producer. Cannabis, methaqualone, nyaope and crystal methamphetamine (tik) are prevalent, with nyaope and tik particularly concerning due to their widespread abuse by children and teenagers.[11]

The 2022−2024 SAMLIT Expert Working Group report on Illicit drug trade,[12] analysed 1 137 STR/STRAs linked to the illicit drugs trade, that indicated sustained interaction with bank accounts, e-wallets and remitters, with a reported value R2.74 billion across the sample.

[10] See Republic of South Africa Police Record Crimes Statistics (Q3 of 2024/2025),at: https://www.saps.gov.za

[11] See Africa Organized Crime Index 2021 (OCINDEX): 4.

[12] See https://www.fic.gov.za/wp-content/uploads/2025/10/EWG-report-Illicit-drugs-trade-2025.pdf

SAPS Crime Statistics point to persistent hotspots in the City of Cape Town and eThekwini, supporting a risk-based focus on cash placement and retail-distribution nodes.

The United Nations Office on Drugs and Crime (UNODC's) 2024[13] reporting adds a broader context, highlighting the continued growth in cocaine flows to Europe and expanding synthetic drug markets, both relevant to SA's transit role.

6.1.5 Smuggling

Smuggling generally refers to the illegal import or export of goods, including contraband, without proper declaration or in violation of customs laws.

The banking sector is exposed to elevated risks where proceeds from smuggling, particularly of high-value goods such as precious metals, wildlife products and counterfeit goods are funnelled through the formal financial channels, with transactions often involving complex layering techniques and cross-border movements, making detection and traceability challenging.

Case Study 12: Gold smuggling investigation
In March 2023, a report exposed a transnational network smuggling gold from Zimbabwe to South Africa and beyond, laundering hundreds of millions in illicit funds from activities such as untaxed cigarette sales. Using front companies, fake invoices and bribes, funds were moved offshore. The scheme involved bribing bank officials to facilitate transfers, delete records and evade scrutiny, highlighting vulnerabilities in financial institutions to cross-border crimes. The PA reviewed implicated banks' AML/CFT compliance activities, imposed fines for due diligence failures and prompted internal investigations leading to employee and client terminations. South African law enforcement authorities initiated criminal investigations in 2023, freezing assets and analysing transactions, with investigations continuing.

[13] https://www.unodc.org/unodc/press/releases/2024/June/unodc-world-drug-report-2024_-harms-of-world-drug-problem-continue-to-mount-amid-expansions-in-drug-use-and-markets.html?utm_source=chatgpt.com

6.1.6 Tax evasion

Tax evasion refers to the deliberate evasion of tax obligations by individuals, businesses or other entities through fraudulent means such as underreporting income, overstating deductions or concealing assets offshore.

ML associated with tax evasion may involve the concealment and integration of proceeds obtained from tax evasion activities into the formal economy. Criminals may use offshore bank accounts, complex corporate structures and tax havens to hide assets and evade detection by tax authorities.

South Africa's role as a financial hub has served as a gateway for funds flowing from sub-Saharan countries to the rest of the world, including potential foreign proceeds of crime.[14]

Over the years, there has been an increase in sophisticated financial crimes being carried out through complex and non-transparent structures, often across borders. These crimes may be facilitated by a small group of people in the professional services industry of lawyers, accountants, financial advisers and others, who help design the legal and financial structures are often seen in complex tax evasion crimes.

6.1.7 Modern slavery and human trafficking

Modern slavery and human trafficking (MSHT) encompass exploitation through forced labour, sex trafficking (including the commercial sexual exploitation of minors), forced marriage, sports trafficking and organ trafficking.
South Africa has been assessed as a Tier 2 country in the 2021 U.S. Trafficking in Persons Report.

In 2020/21, the Directorate for Priority Crime Investigation (DPCI) investigated 31 trafficking cases, with the National Prosecuting Authority (NPA) prosecuting 79 ongoing cases, involving predominantly sex trafficking.

[14] See Financial Action Task Force Mutual Evaluation Report of South Africa (FATF-MER), 2021.

Financial intelligence analysis indicates the rand value linked to MSHT involves billions of rands annually, with a sharply increase between 2018 and 2021, underscoring growing financial exposure for the sector.

Trafficking networks routinely leverage the formal financial system to move, conceal and extract proceeds often via funnel accounts, front/shell companies, third-party use, rapid movement of funds and structured payments (including frequent low-value deposits), as well as domestic and cross-border transfers inconsistent with customer profiles.

Indicative red flags for MSHT-linked activities are:[15]

- Accounts operating as funnel accounts, with rapid pass-through activity and atypical lump-sum withdrawals.

- Frequent low-value cash deposits (often in low denominations) and immediate cash-outs.

- Cross-border transfers to recurring counterparties or locations inconsistent with the customer profile or stated business activity.

- Use of front/shell/shelf companies or third-party accounts, including multiple deposits from distinct geographies indicative of smurfing.

- Inability to contact clients at registered numbers and frequently changing contact details.

6.1.8 Illegal Wildlife Trade

Illegal Wildlife Trade (IWT) involving rhino horn, abalone and reptiles remains a significant, transnational organised-crime threat with direct exposure for South African banks through cash-intensive supply chains and associated laundering activity.

[15] See https://www.fic.gov.za/wp-content/uploads/2023/09/2023.03-SL-MSHT-research-report-2023-1.pdf

Recent analysis highlights patterns relevant to monitoring and enhanced due diligence (EDD), include influx via large forex payments, real-time clearing (RTC) transfers, structured cash deposits (including at airports) and casino cash buy-ins, disposal via ATM withdrawals across regions, point-of-sale (POS) spend, online gambling, international transfers and remitters. Abuse of minors' accounts, shelf/courier companies and use of coded deposit references (e.g. 'Secret', 'MOOLA', 'hunting package' and 'villa payments') continue to recur.

IWT transactions clusters point to Gauteng (Johannesburg, Pretoria), Western Cape (Cape Town, Hout Bay) and Mpumalanga (Nelspruit, Sabie), with high-value activity often in Sandton, Stellenbosch and Bedfordview, with IWT networks leveraging legitimate businesses (e.g. logistics/air freight, restaurants and boating equipment dealers) as fronts and involve public-sector corruption risks.

Financial disruption is however yielding results. *Project Blood Orange* correlated with a 40% decline in rhino poaching in 2022 and 49% in 2023, following arrests for corruption/money-laundering; convictions and international cooperation increased, with money laundering charges more routinely added.

SAMLIT's report[16] shows both rising detection and a need to keep improving reporting quality. Phase 2 STR/SAR mining logged 139 IWT related reports (up from 118 in Phase 1) . Subsequently, new IWT reporting codes and sector training were introduced and Phase 3 (Jan 2022−Dec 2024) identified 439 IWT linked STRs/SARs.

6.1.9 Illustrative cases (typologies and flows)

- Abalone smuggling via Botswana to Zimbabwe: hidden truck compartment holding 1.35 tonnes of dried abalone, with false plates and courier-type profile.

- Reptile trafficking: Sungrazer lizard sold via e-commerce platform, with proceeds traced to local bank accounts.

[16] See https://www.fic.gov.za/wp-content/uploads/2024/08/EWG-IWT-case-study-digest.pdf

6.2 Terrorism financing threats

TF continues to pose a threat to South Africa's financial system with the 2024 TF NRA elevating the country's overall TF risk from moderate to high, reflecting the nation's status as a regional financial hub, its open economy and the increasing complexity of domestic and cross-border financial networks as prone to TF abuse.

While the number of confirmed TF cases within South Africa remains limited, both the TF NRA and PA's supervisory analyses indicate that the size, connectivity and product range of the banking sector expose it to exploitation by terrorist organisations, foreign operatives and domestic extremist networks.

6.2.1 External and domestic threats and sectoral vulnerabilities

TF risks stem from both external terrorist groups and domestic extremist movements.

External networks such as Al-Shabaab, ISIS-Mozambique, ISIS-DRC and ISIS-Somalia continue to operate in Southern and East Africa, with credible intelligence indicating supportive cells and fundraising facilitators based in South Africa. Domestically, individuals have reportedly travelled to conflict zones or channelled donations abroad using bank accounts to remit funds to affiliated entities.

Domestic right-wing extremist groups, including nationalist and separatist movements, have also been flagged for attempted fundraising and asset pooling, although the volume of confirmed cases remains low.

These threats intersect with banking-sector vulnerabilities, notably in high-risk customers, cross-border flows and non-face-to-face onboarding channels.

6.2.2 Sectoral vulnerabilities

- Anonymity and product complexity: Certain investment-linked or cash-value products allow fund layering through premium payments, policy loans or early surrenders, making it difficult to trace beneficial ownership or transaction purpose.

- Customers: Customers face greater TF exposure when they maintain connections with high-risk jurisdictions such as Iran, Somalia, Mozambique and the Democratic Republic of Congo (DRC). In addition, non-profit organisations (NPOs), Money or Value Transfer Services (MVTS) and crypto asset service providers (CASPs) remain highly susceptible to TF abuse, particularly for cross-border small-value transactions.

- Banking data collected through AML risk returns highlighted that institutions servicing NPO clients active in East Africa, the Middle East and Great Lakes regions reported higher TF risk ratings than peers with domestic-only charitable exposure.

- Complex legal structures: Shell companies, foreign-incorporated entities and trusts are often used to disguise the source and ownership of funds. These structures enable obscured transfers, layered ownership and distance from ultimate beneficiaries, increasing the difficulty of identifying TF-related flows.

- Products and services: TF typologies identified through risk-return analysis and thematic engagements show that transaction accounts, EFTs, cash deposits and third-party payments remain the most exploited products. In some instances, prepaid cards, mobile banking and crypto assets are used to accumulate and disperse small donations, a pattern consistent with international TF trends.

- Channels: Non-face-to-face onboarding and digital banking channels present heightened risk, particularly where remote verification or beneficial-ownership data is incomplete. Subsidiaries or points of presence in high-risk jurisdictions further compound exposure.

6.2.3 Non-profit organisations

NPOs remain a key TF exposure point within the banking sector due to reliance on donations, cross-border transfers and cash-based funding mechanisms.

Analysis of AML risk returns indicates that a subset of banks servicing internationally connected NPOs had identified transactions routed to high-risk regions, notably Somalia,

Mozambique and the Middle East, often under the guise of humanitarian aid or community support.

The 2024 TF NRA[17] noted that while most charitable activity is legitimate, a subset of NPOs, especially those operating cross border in conflict affected or under regulated environments, are vulnerable to abuse for TF. The NRA calls for vigilance and cooperation between banks and NPOs, noting that systems may be exploited to raise, move, store or use funds and goods in support of terrorist activity.

Common TF typologies observed or reported by institutions include:

- cash deposits into NPO accounts followed by rapid outward transfers, indicating potential layering or fund dispersion;

- use of crowdfunding platforms and mobile-money wallets to collect micro-donations before transferring consolidated amounts abroad;

- informal remittance services (hawala-type arrangements) leveraged to send funds to non-banking counterparts in high-risk regions; and

- third-party facilitation where NPO accounts are used to receive funds from individuals unconnected to the charity's stated objectives.

Key vulnerabilities within the NPO subsector include:

- unverifiable funding sources: cash and informal transfer methods obscure the origin of funds;

- limited governance: weak financial oversight and board controls hinder the detection of suspicious activity;

[17] See https://www.fic.gov.za/wp-content/uploads/2024/06/National-risk-assessment-%E2%80%93-Terrorist-financing-national-risk-assessment-2024.pdf

- cross-border donations: difficulty verifying donor legitimacy or tracing funds once disbursed internationally; and

- Limited formal registration: In South Africa, NPO registration is voluntary, and many voluntary associations operate without registration. This can reduce the availability of standardised reference information (e.g., registration details and governance disclosures) and may complicate customer verification and ongoing monitoring. Registration status should however not be used in isolation to deny access to banking services; banks should apply proportionate, risk-based due diligence.

6.2.4 Targeted financial sanctions

In the context of the South African financial system, only banks and authorised dealers with limited authority (ADLAs) in foreign exchange are allowed to provide transaction facilities that enable customers to perform cross-border funds transfers.

The PA also receives TFS data from its bilateral meetings held at least twice a year with the largest banks in South Africa, as well as via the risk return submissions received on a quarterly basis.

The PA conducted two sector-wide TFS reviews in 2023 and 2024 to assess the correlation between TFS implementation and TF risk mitigation.

The 2023 TFS review involved a system-based evaluation, which tested screening system performance against simulated United Nations Security Council (UNSC) listings, to assess alert generation, match accuracy and timeliness.

The 2024 TFS review conducted as a desk-based assessment, requiring banks to detail their screening processes, list management, escalation governance and real-time monitoring capabilities.

The reviews found that the banking sector's detection mechanisms have significantly improved over the past decade, with the use of third-party service providers to update their UN lists, with specific SLA timeframes for the updates to take place.

It was however noted that a small subset of banks still relied on manual list uploads and that some banks lacked clear escalation frameworks and independent model validation. These weaknesses are concentrated in small to medium banks with manual list uploads and gaps in escalation governance and independent model validation observed, with a small number of foreign bank branches also affected.

In contrast, large domestic banks generally demonstrated automated list ingestion, defined escalation frameworks and independent model-validation routines evidenced in the 2024 review.

In few instances involving small to medium sized banks, limited inclusion of beneficial owner (BO) data, account signatories and related parties in screening coverage were noted.

The PA has since highlighted these system deficiencies, requested remediation plans and conducted industry workshops and outreach and awareness sessions to improve TFS screening within the sector.

The PA also conducted an additional thematic review to establish the extent to which banks have effective controls to freeze funds without delay. The outcome of these exercises revealed that the sector was largely compliant and aware of their obligations.

6.3 Proliferation financing threats

PF poses a significant threat to global peace and security, facilitating the proliferation of weapons of mass destruction (WMDs) and related materials by sanctioned states, non-state actors and proxy networks.

The South African banking sector is exposed to PF risks through cross-border trade, correspondent banking and client relationships connected to high-risk jurisdictions and dual-use industries.

Although South Africa does not have a completed PF NRA, findings from the supervisory data, international typologies and the 2024 banking sector threat assessment indicate that PF risks are moderate-to-high, particularly where exposure to sanctioned jurisdictions, dual-use goods and complex ownership structures intersect.

6.3.1 PF Regulatory and Supervisory Framework

South Africa's PF framework aligns with international standards and implements financial sanctions under UNSCR 1718 against the Democratic People's Republic of Korea (DPRK) and UNSCR 2231 (Iran).

These obligations are recognised in South Africa through:

- section 26A of the FIC Act requiring accountable institutions to freeze assets and prohibit transactions with UN-designated persons and entities;

- the non-proliferation of Weapons of Mass Destruction Act 87 of 1993, which governs strategic goods and technologies;

- FIC Public Compliance Communication 54, which provides guidance on compliance measures aimed at combating PF and on activity-based PF risks beyond formal TFS lists; and

- PA Guidance Note 12/2022, which provides guidelines and outlines expectations for PF risk management in business risk assessments.

Sectoral thematic reviews conducted by the PA in 2023−2024, revealed progress in real-time sanctions screening, but residual weaknesses in ongoing list management, beneficial ownership look-through and alert dispositioning persists.

6.3.2 High-risk jurisdictions

Supervisory data and international intelligence identified the following jurisdictions as posing heightened PF risks to South African banks:

- Democratic People's Republic of Korea − subject to comprehensive UN sanctions, the DPRK remains the primary global PF threat actor. Its networks exploit front companies, foreign information technology (IT) workers, and cyber-enabled crime to raise and move funds. Open-source reporting indicates DPRK-linked networks have operated in Southern/Eastern Africa, including cyber-enabled revenue generation and instances of diplomatic involvement in illicit wildlife products (e.g., ivory/rhino horn), creating potential indirect exposure for banks.[18]

- Iran − although the UN nuclear-related sanctions were lifted under UNSCR 2231, Iran remains subject to US secondary sanctions and EU trade restrictions. Iranian state-linked enterprises retain stakes in uranium and energy projects in Southern Africa, raising concerns of dual-use procurement and sanctions evasion via intermediaries. Historical cases include attempted exports of restricted material from South Africa to Iran, illustrating the ongoing need for counter-party due diligence.

- Pakistan − with a documented history of illicit procurement of controlled items for its nuclear programme, case studies demonstrate how South African entities were used as intermediaries to acquire and re-export triggering devices and oscilloscopes, highlighting the risk of front-company misuse and dual-use trade financing.

- Afghanistan − PF risks stem mainly from informal value transfer systems and cash-based remittances amid ongoing instability. Humanitarian and non-governmental organisation (NGO) flows can obscure ultimate beneficiaries, requiring enhanced scrutiny of charitable payments and cross-border fund transfers.

[18] See https://static.rusi.org/OP-embassies-and-elephants-north-koreas-involvement-in-the-IWT-final-web.pdf

- Syria and Iraq − both jurisdictions are associated with chemical-weapon proliferation and non-state actor activity. Exposure arises indirectly via regional intermediaries or dual-use commodity trade. South African financial flows to these regions, although limited, require enhanced sanctions screening in light of persistent use of third-country routing to disguise end users.

- Myanmar – presents heightened PF and TF convergence risk due to military-linked conglomerates that are subjected to international sanctions. While direct exposure remains low, trade-finance transactions involving neighbouring Asian jurisdictions warrant caution.

6.3.3 PF product, service and sectoral exposure

The banking sector's exposure to PF risk is concentrated in:

- trade finance and open-account trade, particularly where goods may be of dual use (mechanical, chemical or electronic components);

- correspondent banking relationships, especially with banks in Asia and the Middle East, where due-diligence gaps may allow indirect exposure to sanctioned entities;

- virtual assets and fintech channels, which the BASA PF threat assessment identifies as emerging PF typologies for DPRK cyber-laundered proceeds;

- corporate and trust services, where opaque ownership structures can obscure sanctioned beneficiaries; and

- cross-border payments involving sanctioned or high-risk jurisdictions, requiring automated screening and name-matching algorithms capable of capturing transliteration variants.

6.3.4 PF risk justification and outlook

South Africa's interconnected financial system, cross-border trade links and manufacturing capacity in dual-use sectors, position it as a potential transit and facilitation jurisdiction for proliferation networks. In banking, PF exposure is most likely to arise through trade in dual-use goods, correspondent banking relationships (including with counterparties in Asia and the Middle East), and cross-border payments and corporate/trust structures where ownership and end-use/end-user may be obscured.

The outlook remains sensitive to evolving sanctions-evasion and procurement typologies; while thematic work shows progress in real-time screening, residual weaknesses persist in list management, beneficial ownership look-through and alert dispositioning, which can expose banks to indirect PF risk.

7. Vulnerabilities

Vulnerabilities represent weaknesses, deficiencies or gaps that can be exploited by illicit actors to facilitate ML/TF/PF activities. By identifying and analysing the factors that contribute to these vulnerabilities, the understanding of the systemic risks and challenges associated with illicit finance can be improved, thereby informing the development of targeted risk mitigation strategies.

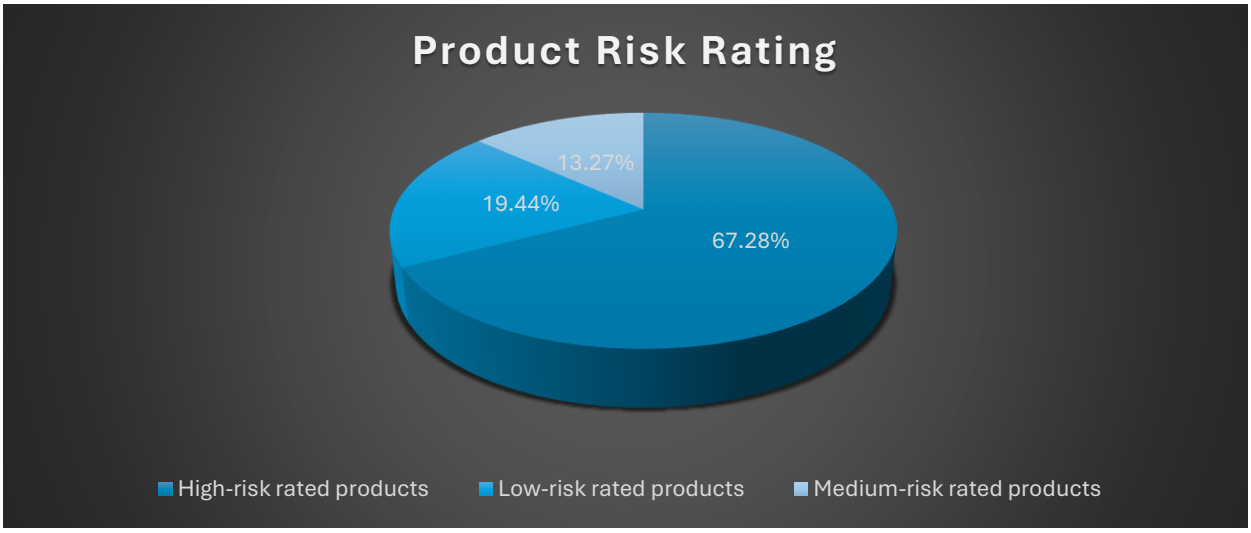
This assessment examines the vulnerabilities identified within the banking sector, and is primarily based on the data submitted through the quarterly risk returns from January 2022 to December 2024.

7.1 Product and services risks

The banking sector offers a diverse range of products and services, including personal and business banking facilities, savings accounts, cheque accounts, debit, credit and prepaid cards, investments, money remittance, Forex and trade finance accounts, home loans and personal loans, all of which carry inherently varying degrees of exposure to ML, TF and PF risks.

An analysis of the AML risk-return data for the review period indicates that 67.28% of the products and services offered by the banking sector were classified as high-risk by institutions in the banking sector.

Figure 3: Product and service risk offered by banking sector



Analysis of financial transaction trends indicates that local bank accounts are primarily receiving illicit proceeds through money remittances, SWIFT transfers, EFTs and cash deposits. These transactions are conducted daily from various provinces in South Africa and typically involve large high-value amounts. The transactions are executed rapidly, either from the same senders or multiple senders.

The following products/services were rated as high risk by the banking sector:

7.1.1 Cash intensive products

South Africa's financial system remains cash intensive, with banks offering products and services that enable high volumes of cash transactions and therefore present higher ML, TF and PF risks. These risks arise from the following:

- cash-intensive deposit products such as personal and business current accounts allow for frequent cash deposits, often from high-cash sectors like retail or transport, and may be exploited to place illicit funds into the financial system, especially through structured deposits or ATM transactions lacking clear source-of-funds disclosure;

- basic savings and entry-level accounts, including low-fee or 'Mzansi' type products, are often used by low-income individuals, which typically lack any electronic income streams and rely heavily on cash deposits and withdrawals;

- stokvel accounts are special deposit accounts designed for community-based savings clubs, where members collect cash and deposit it into the group's bank account and later withdraw cash lump sums for payouts. Some banks have tailored products to support this model, with features that facilitate frequent cash handling. The informal structure and reliance on physical cash make regulatory oversight more difficult, increasing the risk of misuse for ML or TF.

- cash-intensive lending products, particularly short-term micro-loans and unsecured credit often involve cash disbursements and repayments. Borrowers with cash-based incomes, such as informal traders, often repay loans in cash, making the

service of these products inherently cash-intensive. Additionally, niche products like cash-backed or collateral loans where customers pledge physical cash or bearer instruments as security, can be exploited to introduce illicit funds into the financial system. Although rare and tightly controlled, such arrangements require enhanced scrutiny, as they may be used to convert illicit cash into seemingly legitimate loan proceeds.

- over-the-counter cash deposits and withdrawals via traditional teller services remain a core banking function and are inherently cash intensive. Clients frequently deposit or withdraw large volumes of cash at branches, including third-party deposits and multiple transactions across different accounts.

- These patterns are recognised red flags. Multiple same-day deposits at different branches or sudden spikes in cash activity by typically low-cash businesses, are flagged by the FIC as high-risk indicators. While banks mitigate risk through identity document (ID) verification and mandatory reporting of cash transactions over R50 000, teller-based services continue to be a major conduit for physical cash entering the financial system, with depositor and source of funds remaining unknown.

- ATMs are operated by banks through extensive country-wide networks that not only dispense but also accept cash deposits. These services offer convenience but also introduce anonymity risks as depositors are not always required to identify themselves or disclose the source of funds. Criminals may exploit this by structuring deposits across multiple machines to avoid detection. Despite enhanced monitoring tools such as transaction pattern analysis and surveillance, ATM-based deposits remain a high-risk channel due to the sheer volume of transactions and limited face-to-face oversight.

- cash-in-transit and bulk cash services provided to banking clients in cash-intensive sectors like retail, fuel and gaming involve the physical movement of large sums of money by armoured vehicles to bank vaults or bulk teller counters. While these services reduce on-site cash risks for businesses, they concentrate large cash volumes within the banking system. These services are essential in a cash-intensive

economy but carry inherent ML risks due to the anonymity and scale of cash involved.

- prepaid cards, multi-currency travel cards and general-purpose prepaid debit cards are considered cash-intensive products. These instruments can be loaded with physical cash at branches or ATMs and can be used without being directly linked to a traditional bank account. This makes them attractive for laundering, as illicit cash can be digitised and spent or transferred in small, less detectable amounts. While banks have introduced controls such as Know Your Customer (KYC) requirements, load limits, usage tracking and prepaid cards remain a risk area due to their portability, anonymity and ease of cross-border use.

- foreign exchange services offered by banks and licensed dealers are another cash-intensive area, with customers able to convert large amounts of local currency into foreign currency or vice versa, often using physical cash. These transactions are vulnerable to abuse by criminals seeking to move funds across borders or obscure their origin. Regulatory frameworks require ID verification and reporting of high-value exchanges, but typologies such as structuring transactions to avoid thresholds or using forex drafts to launder funds remain concerns.

- banker's drafts and cheques, though rare in South Africa due to the phasing out of cheques, are considered guaranteed forms of payment and are often used in large transactions. When a customer uses cash to purchase a bank draft, it effectively converts untraceable cash into a traceable financial instrument. The FIC has documented numerous cases where individuals repeatedly bought bank cheques with illicit cash to obscure the origin of funds.

7.1.2 Trade finance

Trade finance in the South African banking sector facilitates cross-border movement of goods and value through instruments such as letters of credit, guarantees, standby credits, bills for collection and open-account arrangements. These activities are exposed to elevated money-laundering and sanctions-evasion risk since they span multiple jurisdictions, rely on documentary evidence that can be forged or manipulated and often

involve layered counterparties such as agents, freight forwarders and offshore intermediaries. International typology work highlights recurring abuse channels, including over or undervaluation of goods, false description or quantity, phantom or short shipments, duplicate invoicing, third-party settlements that obscure the origin or destination of funds and the use of front or shell companies to disguise beneficial ownership. These methods remain directly relevant to South Africa's trade corridors.

During the review period, a domestic bank disclosed (via SENS) that it had received administrative sanctions from the PA relating to FIC Act non-compliance within its foreign exchange business, followed by SARS's[19] instituting legal proceedings against the same institution following an investigation into taxpayers who allegedly colluded to expatriate funds offshore in a manner that obscured tracing and jeopardised tax recovery. These matters, widely reported in the public domain, underscore the ongoing vulnerability of trade and foreign-exchange processes to illicit practices. Specifically, they illustrate how collusion between parties, the use of falsified documentation, and complex value-transfer schemes can be misrepresented as legitimate commercial activity, ultimately facilitating regulatory evasion and financial crime.

Supervisory visibility over cross-border value flows increased during the period. The FIC's 2023/24 annual report recorded that banks filed approximately 842 125 international funds transfer reports in that year, with authorised dealers reporting a further 2 949 683 such transfers, with the FIC actively analysing these reports to detect illicit cross-border movements. This reporting stream, together with cash-conveyance analytics at ports of entry and exit, improves detection of trade-linked typologies and supports targeted follow-up by competent authorities.

Policy changes have also targeted advanced import payments, a key trade-based money laundering (TBML) pressure point. From 1 December 2023, importers are required to obtain a South African Revenue Service (SARS) Advance Payment Notification (APN) before banks can process an advance import foreign-exchange payment and authorised dealers are required to validate and report the APN when concluding payments. This closes an important channel through which funds could previously be expatriated on the strength of pro-forma invoices for goods that were never shipped, were mis-described or

[19] https://www.sars.gov.za/media-release/sars-confirms-legal-action/

were materially mis-valued. The SARB's FinSurv circulars issued in 2023 and 2024 further tightened authorised-dealer obligations around import payments and related balance-of-payments categories.

7.1.3 International payments and cross-border activities

Products that facilitate cross-currency and cross-border transactions pose higher ML, TF and PF risks because they involve complex processes, multiple jurisdictions with differing regulations and challenges in verifying parties involved, identifying beneficial owners and tracking fund source and destinations.

7.1.4 Correspondent banking relationships

Financial institutions that maintain correspondent banking relationships (CBRs) and provide banking services on behalf of another financial institution, typically in another country, add further risk to the banking sector. These services include international fund transfers, cheque clearing, currency exchange and treasury management, and are essential in the global payment system and vital to international trade and the global economy.

Potential ML, TF and PF risks include:

- cross-border transactions – transactions across multiple jurisdictions with varying regulatory standards, can lead to differences in AML/CFT controls, negatively impacting effective risk mitigation.

- Customer due diligence − identifying and verifying customers in cross-border transactions can be complex, especially in cases of nested accounts.

- Transaction monitoring − the large volumes of cross-border transactions can hinder effective monitoring and detection of suspicious activities.

- Targeted financial sanctions − correspondent banks may facilitate transactions involving sanctioned entities or jurisdictions due to inadequate due diligence or ineffective screening processes.

A total of 18 institutions across the banking sector hold correspondent banking accounts (nostro accounts) at foreign banks, enabling connectivity to the international banking system. These respondent banks primarily consist of large banks and foreign banks. Additionally, 14 South African banks served as correspondent banks, offering CBR services (vostro accounts) to foreign financial institutions.

Table 4: Correspondent banking relationships

Banks	No. of banks that have nostro accounts	No. of banks holding vostro accounts
Large banks	5	5
Small to medium banks	2	0
Foreign banks	11	9
Mutual banks	0	0
Total	**18**	**14**

As of December 2024, the sector held a total of 2 439 correspondent accounts, comprising of 643 nostro accounts and 1 796 vostro accounts. Large banks held most of this network with 2 009 accounts, while branches of foreign banks and foreign-controlled banks held 420 accounts. Small to medium sized banks held 10 accounts, with mutual banks reported none. On a proportional basis, large banks therefore accounted for about 82.3% of all correspondent accounts, branches of foreign banks for 17.2% and small to medium banks for 0.5%.

Vostro relationships materially outnumbered nostros, representing about 73.6% of all correspondent accounts, which is consistent with the role of large domestic institutions as providers of correspondent services to foreign banks.

Nested relationships and payable-through[20] accounts also present higher risks. As of December 2024, the South African banking sector held a total of 94 nested accounts and 12 payable-through accounts. These nested accounts were primarily managed by two large banks, with one small-to-medium-sized bank and one foreign bank also holding such accounts. Meanwhile, payable-through account services were offered by one large bank and one small-to-medium-sized bank.

Both types of accounts present significant ML/TF/PF risks. Nested accounts, where a foreign bank operates through the correspondent account of another foreign bank, complicate customer identification and verification, making it challenging to monitor and detect suspicious activities, particularly when distributed across institutions of varying sizes and jurisdictions.

7.1.5 Money remittance services

South Africa's 2024 TF NRA identifies a large cash-based informal economy, presence of informal money remitters/illegal MVTS and the use of cash couriers, as key vulnerabilities that terrorists and facilitators can exploit to raise and move funds across borders. These channels reduce transparency, weaken audit trails and complicate sanction implementation. The formal channels include ADLAs (e.g. Mukuru, Hello Paisa and WorldRemit), that operate under FinSurv and are obligated to comply with exchange control obligations as well as being supervised by the FinSurv for compliance with FIC Act obligations.

Authorised dealers currently comprise only banks and are supervised by the PA for compliance with FIC Act obligations, while the FinSurv supervises such institutions for compliance with the Exchange Control Regulations of 1961. Supervisory actions against non-compliant banks and ADLAs, further support discipline in the formal market.

[20] Payable-through accounts allow foreign banks to offer their customers access to the domestic banking system, often without the domestic bank having direct knowledge of the customers.

In contrast, informal money remitter channels like Hawalas operate outside regulated payment rails, often settle via netting or trade-based value (e.g. under/over-invoicing and offsetting obligations), with limited or no formal records, agent networks that may straddle jurisdictions with anonymity and cash intensity, third-party cash aggregation (market-day collections, community couriers etc.), and off-book settlement (trade or netting).

These characteristics create heightened TF/PF exposure and frustrate TFS implementation (e.g. inability to promptly screen/stop designated persons or freeze funds), aligning with TF NRA 2024 vulnerabilities.

The recent FinMark Trust paper[21] confirms that the formal South African to Southern African Development Community (SADC) remittances market more than tripled since 2016 (R6 billion to R19 billion in 2024), yet cash remains dominant with 80−90% of transactions in high-volume corridors such as Zimbabwe and Malawi. The study estimates the informal remittance market at R3.4 billion (17% of formal market) and notes signs of a shift back to informal channels in some markets, underscoring the continued materiality of informal flows despite digital progress.

FATF typologies and the MVTS risk-based guidance highlight elevated ML/TF exposure where operators are unlicensed, rely on cash pools and use non-bank settlement methods creating opacity that raises TF and PF risks. Banks should therefore treat flows plausibly linked to informal remittance ecosystems as elevated risk and calibrate controls accordingly.

7.1.6 Private banking

Private banking may be considered a high risk sector for ML, TF and PF. Its inherent vulnerabilities stem from high-net-worth clients, complex financial products and cross-border transactions. Key risk factors include a culture of confidentiality, use of opaque legal structures, exposure to PEPs and the potential for compliance to be compromised

[21] https://finmark.org.za/Publications/SA_to_the_rest_of_SADC_Remittances_Market_Assessment_2024_Report.pdf

by profit motives. These characteristics make private banking particularly attractive for illicit finance, underscoring the need for EDD and robust supervisory oversight.[22]

7.1.7 Virtual cards

Virtual cards present elevated ML/TF/PF exposure relative to chip-and-personal identification number (PIN) instruments because they operate in a predominantly card-not-present environment and can be issued and used rapidly, often across borders. Inherent vulnerabilities arise where programme responsibilities are fragmented between the issuer/bank identification number (BIN) sponsor, programme manager and processor, creating gaps in end-to-end oversight, sanctions screening accountability and data integrity.

Abuse typologies include high-velocity micro-purchases followed by rapid refunds or credit reversals to move value between instruments, proliferation of multiple virtual primary account numbers (PANs) mapped to the same underlying controller, and merchant misuse where weak due diligence or miscoded merchant category codes (MCCs) obscure the true nature of goods or services.

From a control perspective, institutions should ensure clear programme governance, strong CDD/EDD with device binding, one-to-one virtual PANs profile mapping, near-real-time TFS and monitoring focused on transaction velocity, refund/credit anomalies and PAN-proliferation patterns. Independent model validation and regular tuning are expected to evidence effectiveness rather than design intent.

7.1.8 E-wallets

E-wallets and stored-value accounts combine digital convenience with cash-intensive cash-in/cash-out points and agent networks, which, if weakly governed, can facilitate anonymous aggregation and third-party cash pooling. Inherent risks are amplified by tiered or remote onboarding that permits multiple wallets per controller, peer-to-peer

[22] FIC public compliance communication guidance, found here: https://www.fic.gov.za/wp-content/uploads/2023/09/2021.12-PCC-PCC-51-FPPO-DPIP.pdf

(P2P) transfers that can be circular, with linkages to other rails (card, bank, MVTS or crypto) that increase layering opportunities and jurisdictional reach. Typical misuse involves multiple unrelated cash-ins converging on a single wallet, rapid P2P fan-outs and immediate cash-out or cross-border payouts through higher-risk corridors.

7.1.9 Youth accounts

Youth, teen and student propositions expand financial inclusion but create distinct conduct and financial-crime risks when the legal account holder (a minor) is not the true controller of activity or is recruited as a money mule. Inherent vulnerabilities include third-party control risk under guardianship, small-value high-velocity movements typical of mule schemes, exposure to age-restricted merchants and on-ramp pathways to higher-risk channels via linked cards, wallets or crypto exchanges.

7.1.10 Investment products

Investment products include securities such as stock, bonds and mutual funds. They are seen as high risk as they can be used for ML and TF purposes by hiding illicit gains within complex financial structures, thus making it difficult to trace the origin of the funds.

7.1.11 Corporate finance

Corporate finance products are financial instruments and services offered by financial institutions to businesses such as loans, debt instruments, equity financing and investment banking services. These products facilitate financial transactions making them high risk due to the possible misuse for ML and TF purposes. The nature of these products creates opportunities for criminals to hide the source and ownership of illicit funds. The global reach of corporate finance products can lead to cross-border transactions and the use of complex financial structures that can make tracing source of funds and transactional flows difficult.

7.1.12 Credit products

Credit products are any financial instruments that involve a bank extending credit to a customer. They offer anonymity and the potential for structuring transactions as well as easily transferable transactions, which increase the potential for ML and TF, making credit products high risk.

7.1.13 Trust accounts

Trust accounts are legal arrangements where a trustee holds assets on behalf of beneficiaries. These often involve complex terms such as confidentiality provisions, making it difficult to track fund flows and beneficial owners. They can be used by criminals to obscure the true ownership and control of assets which can facilitate ML and TF.

7.1.14 New technologies

The integration of new technologies in the banking sector, such as artificial intelligence, blockchain and digital platforms, have introduced both opportunities and increased ML, TF and PF risks.

While these technologies can enhance efficiency, customer experience and fraud detection, they also present new vulnerabilities for criminal actors to exploit. The quick transit of funds may also be exploited by criminal actors. For instance, it might be possible for artificial intelligence and machine learning algorithms to be manipulated to bypass traditional compliance checks, while blockchain’s anonymity features can be exploited to obscure the origins of illicit funds.

Digital platforms and online transactions increase the speed and volume of transactions, making it more challenging to monitor and detect suspicious activities in real time. As banks adopt these technologies, it is crucial to implement robust risk management frameworks to mitigate the potential associated ML, TF and PF risks.

7.2 Customer risks

Customer risk refers to the potential vulnerabilities to ML/TF/PF that arise from the composition and characteristics of a bank's customer base.

As of December 2024, the South African banking sector served approximately 80.2 million customers across individuals, companies and trusts. South African customers account for about 78.6 million (98%), while foreign customers account for about 1.6 million (2%).

Table 5: Customer distribution by type

Customer type	Number of customers	% of customer base
South African customer	78 624 113	98%
Foreign customer	1 587 069	2%
Total customer base (exclusive of Co-Operative Banks)	**80 211 182**	**100%**

While Table 5 shows the customer base by nationality, AML/CFT/CPF exposure is driven by the risk characteristics of particular customer segments. In line with banks' risk-based approaches, customers often assessed as higher-risk include politically exposed persons (PEPs); non-resident customers (particularly where linked to higher-risk jurisdictions); high-net-worth individuals; legal persons and arrangements with complex or layered ownership/control; customers associated with adverse indicators (e.g., suspicious activity triggers); and customers operating in higher-risk sectors such as certain NPOs, cash-intensive businesses, and customers in higher-risk industries.

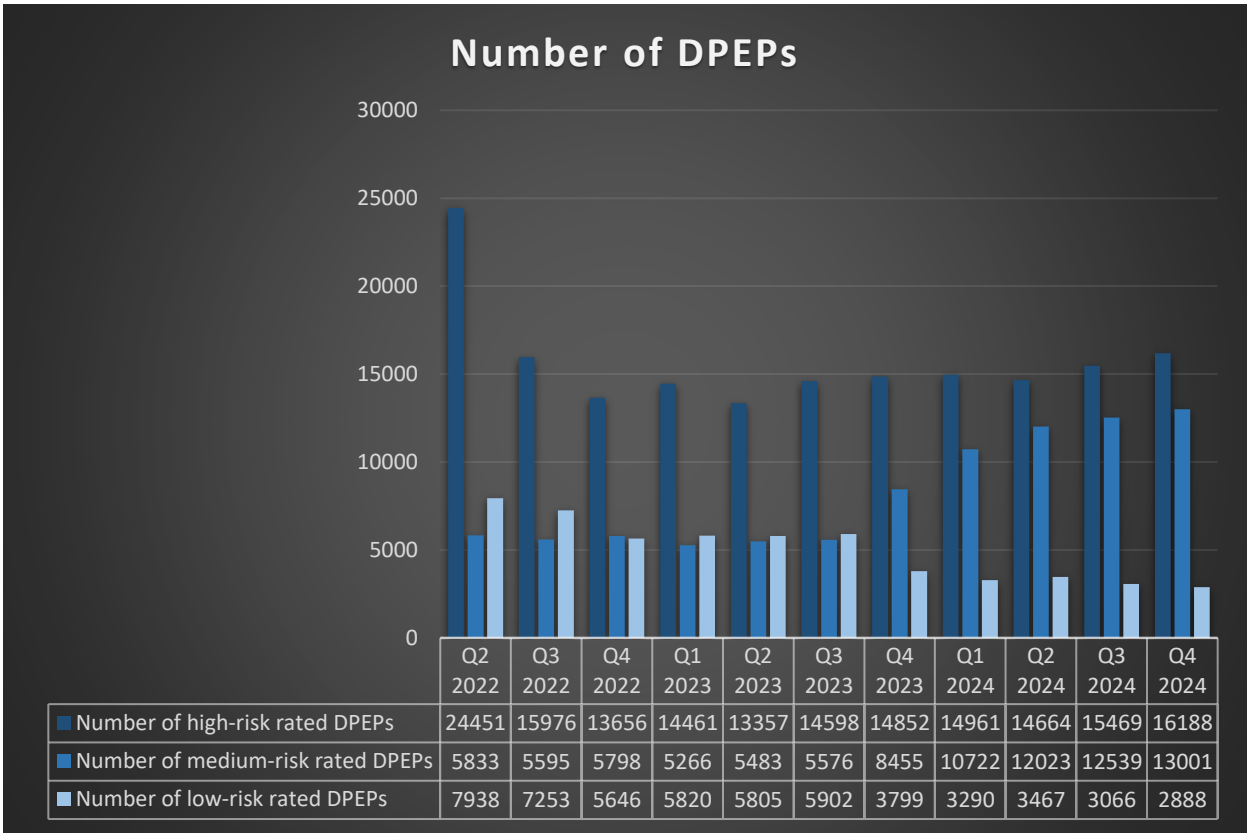
7.2.1 Politically exposed persons

Politically exposed persons (PEPs) (both domestic and foreign) present significant ML, TF and PF risks within the banking sector. Due to their influential positions and access to substantial financial resources, PEPs are often targets for corruption and bribery, which can lead to the accumulation of illicit funds. These individuals may use banking products to launder their proceeds from corruption.

Domestic PEPs are individuals holding prominent public positions within South Africa, such as government officials, senior executives in state-owned enterprises and key political figures. Their positions expose them to a higher risk of involvement in corruption, bribery, and money laundering, necessitating enhanced due diligence (EDD) measures by banks to mitigate associated risks.

As of December 2024, the banking sector held approximately 32 077 domestic PEPs, representing only 0.04% of the sector's 80.2 million customer base.

Figure 4: Domestic PEPs

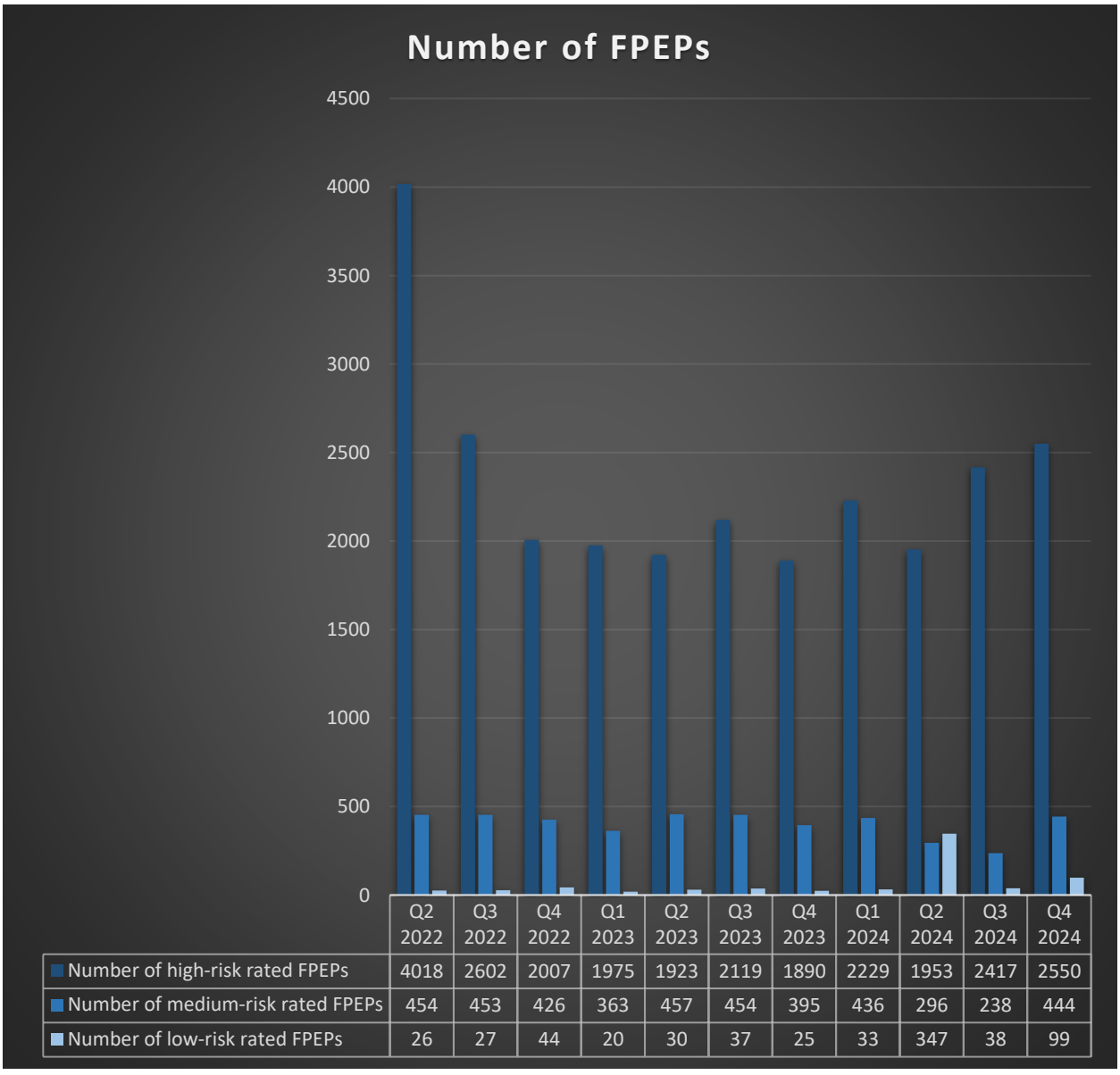


	Q2 2022	Q3 2022	Q4 2022	Q1 2023	Q2 2023	Q3 2023	Q4 2023	Q1 2024	Q2 2024	Q3 2024	Q4 2024
Number of high-risk rated DPEPs	24451	15976	13656	14461	13357	14598	14852	14961	14664	15469	16188
Number of medium-risk rated DPEPs	5833	5595	5798	5266	5483	5576	8455	10722	12023	12539	13001
Number of low-risk rated DPEPs	7938	7253	5646	5820	5805	5902	3799	3290	3467	3066	2888

Foreign PEPs include individuals holding or having held prominent positions in foreign countries, such as government officials, senior political figures, military leaders and heads of state-owned enterprises. Foreign PEPs pose additional risks due to the complexities of foreign political environments, jurisdictional variations in regulation and heightened susceptibility to cross-border financial crimes, including ML and TF.

As of December 2024, the banking sector held approximately 3 093 foreign PEPs, a customer segment that represents important risks even though constituting a relatively small portion of the sector's entire 80.2 million customer base.

Figure 5: Foreign PEPs



	Q2 2022	Q3 2022	Q4 2022	Q1 2023	Q2 2023	Q3 2023	Q4 2023	Q1 2024	Q2 2024	Q3 2024	Q4 2024
Number of high-risk rated FPEPs	4018	2602	2007	1975	1923	2119	1890	2229	1953	2417	2550
Number of medium-risk rated FPEPs	454	453	426	363	457	454	395	436	296	238	444
Number of low-risk rated FPEPs	26	27	44	20	30	37	25	33	347	38	99

7.2.2 Money or value transfer services providers

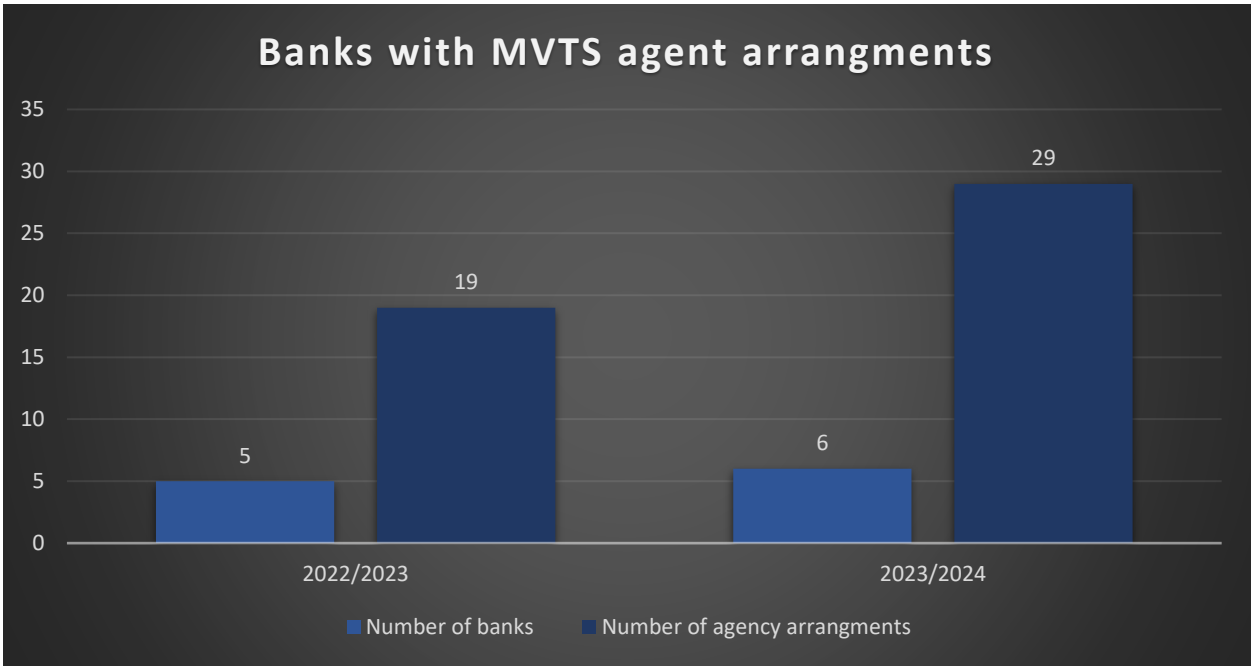
MVTS providers are non-banking entities or agents that offer financial services involving the acceptance of cash, checks and other monetary instruments, followed by the payment of the corresponding amount to a beneficiary through communication, messaging, transfer or a clearing network to which the MVTS provider belongs.
MVTS providers typically offer the following products and services on behalf of the banks:

- automated teller machines (ATMs);
- electronic fund transfers (EFTs);
- interbank electronic credit payment/real-time clearing (RTC);
- Society for Worldwide Interbank Financial Telecommunications (SWIFT);
- mobile money;
- instant money (cash out) that allows users to send money to anyone with a valid South African cell phone number, enabling recipients to withdraw the funds without needing a bank account;
- money transfer (cash send) that allows users to send money to another person's bank account, mobile wallet or for cash pickup, either domestically or internationally, and includes instant transfers, bank-to-bank transaction and cash pickup options through agent locations or retail partners; and
- vouchers, which include prepaid certificates, cards or other devices issued in exchange for payment and may be used only to pay for goods or services.

In South Africa, the PA's Directive 9/2022 mandates MVTS providers to operate only through formal contractual arrangements with South African banks.

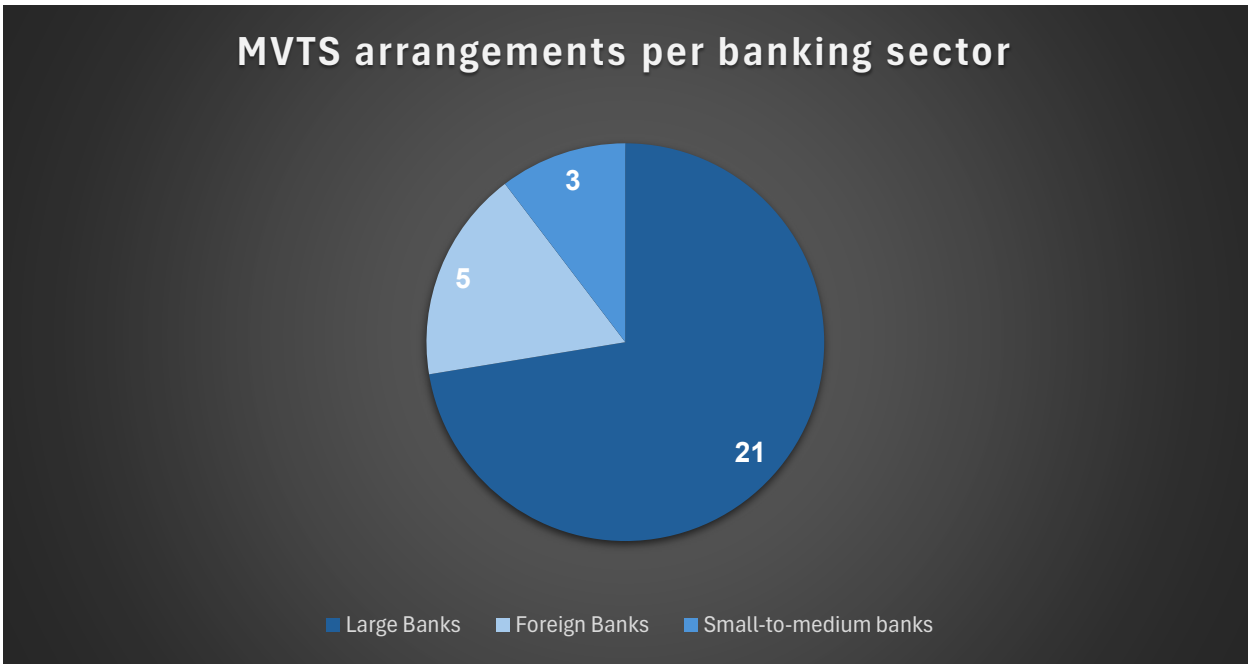
As of December 2024, six banks in South Africa had arrangements with MVTS providers, with a total of 29 MVTS arrangements.

Figure 6: Banks with MVTS arrangements



Large banks held 21 of the MVTS arrangements, with small-to-medium banks holding 3 MVTS arrangements and foreign banks holding 5 MVTS arrangements.

Figure 7: Banks with MVTS arrangements, per banking sector



Banks that hold domestic MVTS arrangements introduce additional risk to their business operations as MVTS providers pose a higher risk due to the significant transaction volumes they handle, coupled with the limited visibility and oversight banks have over these transactions.

7.2.3 Crypto asset service providers and emerging technologies

In South Africa, a crypto asset is understood to be a digital representation of value that is not issued by a central bank and is traded, transferred and stored electronically for purposes such as payment, investment or other utilities using cryptographic techniques.

Crypto assets are not legal tender, which in South Africa is limited to banknotes and coins issued by the SARB. In October 2022, the FSCA declared crypto assets to be a 'financial product' under the Financial Advisory and Intermediary Services Act (FAIS), bringing related financial services into the conduct-supervision perimeter.

Following the declaration, amendments to the FIC Act took effect on 19 December 2022, adding Crypto Asset Service Providers (CASP) as accountable institutions. The FSCA began licensing CASPs under FAIS on 1 June 2023. On 15 November 2024, the FIC issued Directive 9 on the implementation of the 'Travel Rule' for crypto-asset transfers, effective from 30 April 2025. In its 2024 follow-up report, the FATF re-rated South Africa's recommendation 15 on new technologies from partially compliant to largely compliant, reflecting these reforms.

By 10 December 2024, the FSCA reported the receipt of 420 CASP licence applications, with 248 approvals, 9 declines and the balance in progress, with published list of authorised CASPs being maintained. This expanding licensed perimeter provides regulated domestic on-and-off ramps for banked customers, while sharpening supervisory visibility over higher-risk business models.

Direct balance-sheet exposure to crypto assets within banks remains limited, however, banks face material indirect exposure through customer transactions that fund or realise crypto-asset activity (including EFTs and card payments), banking relationships with CASPs and selective pilots in tokenisation, custody or wallet services. These channels present potential ML, TF, PF, fraud, sanctions evasion and cyber/operational risks, given the speed, cross-border reach and pseudonymous nature of certain crypto-asset activities. Supervisory engagements and banks' own risk assessments indicate that most exposure arises from retail on-/off-ramping, with residual exposures linked to offshore, unregulated platforms and peer-to-peer activity beyond licensed CASPs.

The formalisation of the CASP licensing regime, inclusion of CASPs as accountable institutions and the commencement of Travel-Rule obligations have strengthened the control environment and improved transparency of crypto-asset transfers.

Nonetheless, the banking sector's residual risk from customer-driven crypto-asset activity and CASP relationships remain a concern due to persistent exposure to cross-border, fast-moving flows (conversion from fiat to crypto and vice versa) and potential data gaps where activity occurs off-exchange or with non-compliant crypto-asset counterparties. Continued application of a risk-based approach covering CASP specific onboarding standards, targeted transaction monitoring, blockchain-analytics coverage, TFS controls and Travel-Rule conformance testing, remains central to maintaining risk within appetite.

7.2.4 Dormant and frozen accounts

Dormant accounts refer to customer accounts that remain inactive for extended periods with little or no activity, and may pose significant ML, TF and PF risks. Due to their inactivity, dormant accounts often receive less scrutiny and inadequate customer verification upon reactivation, making them attractive targets for unauthorised access, identity thefts or account manipulation.

Criminals seeking to obscure the origin of illicit funds or conduct fraudulent activities may reactivate dormant accounts with minimal oversight, move illicit funds before closing the accounts again.

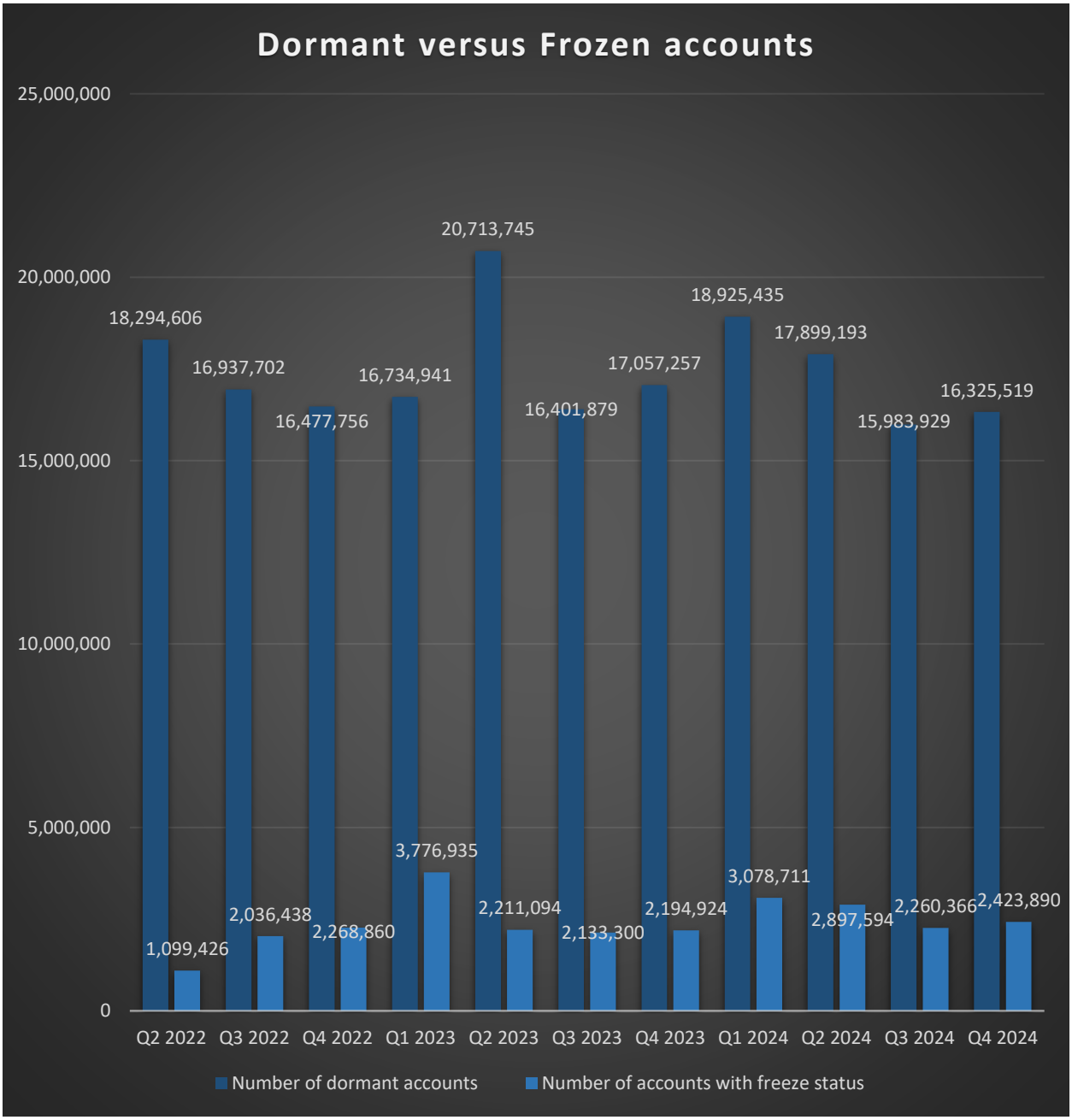
As of December 2024, the banking sector reported 16 325 519 dormant accounts which is 20.36% of the sector's 80.2 million customer accounts. This confirms a sustained decline from 17 057 257 dormant accounts a year earlier. The notional value attached to dormant accounts fell from R21 billion in Q4 2023 to R19 billion in Q4 2024, a reduction of R2 billion, alongside a 4.29% contraction in the number of dormant accounts, with 731 738 fewer accounts.

Frozen accounts refer to accounts that are temporarily restricted due to regulatory intervention, compliance concerns or suspicious activity. While freezing an account is often a protective measure to prevent further unauthorised transactions, criminals may

manipulate the reasons for the freeze's removal or use false documentation to regain access. Additionally, funds in frozen accounts could be linked to illicit activities.

As of December 2024, the banking sector held approximately 2.4 million frozen accounts, representing 3.02% of the sector's total client base of 80.2 million. The data indicates a continuous upward trend in the number of frozen accounts, suggesting increased regulatory or compliance concerns and suspicious activities.

Figure 8: Dormant and frozen accounts



7.3 Geographical risks

This section focuses on the banking sector's geographic risk exposure, particularly through the physical movement of cash and the cross-border movement of funds, which involves the transfer or flow of money across national borders to facilitate international trade, foreign direct investments, remittances, both of which create pathways for illicit financial flows.

South Africa's position as a regional financial and trading hub results in substantial inward and outward financial flows, which increases the banking sector's exposure to ML/TF/PF risk when transactions involve multiple jurisdictions with uneven AML/CFT/CPF capability, opaque ownership structures, complex payment-routing arrangements, or where funds are linked to higher-risk commodities and trade corridors.

7.3.1 Cash transportation

The cross-border movement of cash and other bearer negotiable instruments, presents elevated ML/TF/PF risk because it can circumvent formal financial channels, reduce audit trails and limit the ability of banks and authorities to identify the origin, destination and purpose of funds.

While cash movements can arise from legitimate activity (e.g., tourism, cross-border commerce and the import/export of funds), the physical transport of cash is also a well-established mechanism for laundering the proceeds of crime, supporting illicit trade, and facilitating value transfer outside regulated payment systems. This risk is heightened where cash movements intersect with organised crime networks, illicit commodities or conflict-driven supply chains.

From a supervisory and control perspective, banks' residual exposure to cash transportation risk typically manifests indirectly, through subsequent cash deposits that are inconsistent with a customer's profile, cash-intensive businesses with unexplained cross-border linkages, and customer activity that suggests informal value transfer arrangements (e.g., rapid cash-in/cash-out with limited economic rationale).

7.3.2 Cross-border exposure

South Africa is a major regional conduit for cross-border payments, trade settlement and foreign exchange activity. This creates structural exposure to ML/TF/PF risks because cross-border activity often depends on third-party information (e.g., invoices, shipping documents and beneficiary details), relies on intermediaries, and can involve complex ownership and control chains. These features increase the risk of trade-based money laundering (TBML), concealment of beneficial ownership, third-party payment arrangements and payment-routing designed to obscure the true originator/beneficiary.

Cross-border risk is further amplified through correspondent banking channels and international payment messaging chains, where transaction visibility may be reduced if upstream controls are uneven or if payment messages are incomplete. In practice, this elevates the importance of payment transparency, effective screening (including look-through to related parties where appropriate), and transaction monitoring scenarios designed for cross-border typologies (e.g., trade mispricing indicators, round-tripping, rapid movement through multiple jurisdictions, and unusual settlement patterns relative to the customer profile).

Cross-border flows are material in both value and volume and therefore create a large "surface area" for ML/TF/PF exploitation. Table 6 summarises the key inward and outward flows (excluding card transactions).

Table 6: Cross-border flows

Year	Inward transactions	Inward flow (ZAR)	Outward transactions	Outward flow (ZAR)
2019	8 243 994	11 220 213 382 206	15 920 714	10 672 961 461 649

2020	7 741 612	12 413 474 594 245	19 625 549	11 558 223 240 782
2021	8 294 966	13 081 952 304 034	24 406 564	12 146 099 875 368
2022	9 607 373	12 994 376 875 383	25 121 837	12 257 777 676 863
2023	10 002 424	15 267 964 455 954	21 151 768	14 547 113 579 779

Over the period, inward flow values increased from R11.2 trillion to R15.3 trillion, while outward flow values increased from R10.7 trillion to R14.5 trillion.

These increases (in both value and transaction volumes) reflect growing cross-border financial integration and reinforce the need for robust cross-border controls, particularly for higher-risk corridors and customer segments.

Inward transaction volumes increased from 8.2 million to 10.0 million transactions from 2019 to 2023. Outward transaction volumes increased materially between 2019 and 2022, followed by a decline in 2023; this pattern underscores the importance of monitoring not only absolute volumes but also shifts in payment behaviour and corridor usage over time.

7.3.3 Cross-border flows with FATF jurisdictions under increased monitoring

Cross-border financial flows involving jurisdictions under increased monitoring by FATF, as well as other high-risk corridors and sanctioned countries, present substantial geographical risks and vulnerabilities to the banking sector.

These jurisdictions may have strategic deficiencies in their AML/CFT/CPF frameworks, increasing the risk of illicit financial activity. Weak regulatory oversight in these jurisdictions can hinder the effective CDD and transaction monitoring, exposing banks to heightened ML, TF and PF exposure.

Based on cross-border transaction data, the banking sector in South Africa has some exposure to jurisdictions identified by the FATF as having significant AML/CFT/CPF deficiencies and subject to calls for action.

Table 7 sets out inward and outward flows to/from jurisdictions that were under increased monitoring (FATF Grey List) during the review period.

Table 7: Cross-border flow to/from jurisdictions under increased monitoring

	Inward		Outward		FATF grey list status as at Dec 2024[23]
	Total Flow (ZAR)	Number of Transactions	Total Flow (ZAR)	Number of Transactions	
Albania	R313 700 089	3 265	R367 274 299	2 079	Removed Oct 2023
Algeria	R3 122 724 611	5 964	R358 649 711	3 194	Still on FATF grey list
Barbados	R1 874 967 545	3 832	R1 547 823 480	1 716	Removed Feb 2024
Bulgaria	R4 626 682 470	11 235	R5 532 118 467	17 329	Still on FATF grey list
Burkina Faso	R5 268 070 722	14 990	R809 959 174	11 632	Still on FATF grey list
Cameroon	R2 674 275 836	19 911	R1 977 247 091	329 954	Still on FATF grey list
Cambodia	R472 780 271	6 605	R140 513 750	4 571	Removed Feb 2023

[23] The FATF "Jurisdictions under Increased Monitoring" ("grey list") is updated three times per year. The status shown reflects each jurisdiction's position at the end of the SRA review period (31 December 2024), based on FATF public statements up to 25 October 2024 (the last FATF update in 2024). Statuses may have changed after the review period and before publication; readers should consult the most recent FATF statement for current status.

Cayman Islands	R23 454 745 764	18 484	R30 096 522 099	5 668	Removed Oct 2023
Côte d'Ivoire	R14 555 980 064	38 743	R49 227 139 489	26 968	Still on FATF grey list
Democratic Republic of Congo	R94 935 971 315	408 867	R92 654 397 631	530 394	Still on FATF grey list
Croatia	R526 681 714	7 016	R2 046 937 705	11 362	Still on FATF grey list
Gibraltar	R2 325 769 820	11 316	R1 360 917 696	1 588	Removed Feb 2024
Haiti	R93 127 755	864	R43 700 452	531	Still on FATF grey list
Jamaica	R215 921 471	4 211	R462 628 545	2 329	Removed Jun 2024
Jordan	R2 482 833 995	9 333	R2 494 447 272	13 503	Removed Oct 2023
Kenya	R75 067 780 599	294 377	R64 574 450 263	3 934 121	Still on FATF grey list
Lebanon	R2 351 705 843	10 200	R1 360 026 784	10 857	Still on FATF grey list
Mali	R3 375 505 978	12 741	R109 610 809 416	7 869	Still on FATF grey list
Malta	R11 185 046 111	16 775	R20 776 044 069	11 255	Removed Jun 2022
Mozambique	R184 004 673 698	327 134	R120 105 239 088	4 614 010	Still on FATF grey list
Monaco	R4 253 033 483	8 235	R4 667 544 107	2 316	Still on FATF grey list
Morocco	R5 442 392 116	9 719	R7 695 036 717	32 002	Removed Feb 2023
Namibia	R745 843 760 858	340 606	R610 431 821 259	435 675	Still on FATF grey list

Nicaragua	R28 432 729	390	R37 166 205	461	Removed Oct 2022
Nigeria	R84 401 779 779	142 725	R75 453 729 460	896 254	Still on FATF grey list
Panama	R5 878 338 280	7 140	R2 141 438 031	7 179	Removed Oct 2023
Pakistan	R1 942 441 424	9 619	R34 119 292 496	3 439 413	Removed Oct 2022
Philippines	R13 741 827 326	24 372	R5 365 545 313	75 541	Still on FATF grey list
Senegal	R6 042 179 631	20 813	R3 297 476 791	7 179	Removed Oct 2024
South Sudan	R686 804 519	5 049	R245 305 908	2 783	Still on FATF grey list
Syria	R50 988 980	704	R114 248 384	240	Still on FATF grey list
Tanzania	R44 984 138 154	157 925	R37 910 733 902	875 412	Still on FATF grey list
Türkiye	R28 304 794 993	62 503	R40 904 562 151	193 467	Removed Jun 2024
Uganda	R27 320 307 950	106 856	R20 682 841 582	1 378 112	Removed Feb 2024
United Arab Emirates	R483 712 199 575	928 723	R411 517 361 709	303 714	Removed Feb 2024
Venezuela	R18 447 840	708	R96 549 467	1 071	Still on FATF grey list
Vietnam	R3 888 831 912	25 857	R7 262 177 092	29 096	Still on FATF grey list
Yemen	R385 206 567	1 354	R84 758 075	1 997	Still on FATF grey list
Zimbabwe	R181 162 250 368	1 172 279	R191 631 845 537	29 568 581	Removed Mar 2022

The top 10 countries under increased monitoring for inward and outward flows are detailed in Table 8 below, with specific country-level risks associated with financial flows and related vulnerabilities.

Table 8: Top 10 inward and outward flow of funds from jurisdictions under increased monitoring

No.	Inward flow of funds	Outward flow of funds
1.	Namibia	Namibia
2.	United Arab Emirates (removed February 2024)	United Arab Emirates (removed February 2024)
3.	Mozambique	Zimbabwe (removed March 2022)
4.	Zimbabwe (removed March 2022)	Mozambique
5.	Democratic Republic of Congo	Mali
6.	Nigeria	Democratic Republic of Congo
7.	Kenya	Nigeria
8.	Tanzania	Kenya
9.	Türkiye (removed June 2024)	Côte d'Ivoire
10.	Uganda (removed February 2024)	Türkiye (removed June 2024)

- Namibia: Namibia represents the largest inward and outward flow by value within the FATF increased monitoring dataset, reflecting deep economic and financial integration and high levels of legitimate cross-border activity. The materiality of this corridor means that any weaknesses in payment transparency, trade documentation integrity, or customer risk classification can have an outsized impact on residual risk. Banks should therefore ensure strong corridor-specific monitoring for trade settlement patterns, third-party payments and anomalous FX activity, and apply EDD where customer/product risks warrant.

- United Arab Emirates: South Africa's transactional links with the United Arab Emirates (UAE) remain significant given the UAE's status as a major re-export, gold-trading and financial hub. A significant share of African gold exports goes through Dubai, raising concerns of conflict gold or undeclared artisanal production entering formal value chains. South African entities involved in bullion trading or jewellery manufacturing may indirectly interact with these flows. Furthermore, transactions historically routed through UAE-based companies underscore vulnerabilities in beneficial ownership opacity, trade mispricing and use of offshore shell vehicles. South African counterparties may be exposed to risks when engaged in precious metals trade, real-estate investment vehicles or cross-border remittance services. Large-value gold-linked payments or transfers to UAE free zones should trigger EDD.

- Mozambique: the country's proximity and integration into South Africa's financial and transport systems make cross-border risks material. The 'Tuna Bonds' corruption and laundering case illustrates the misuse of state-backed financing and offshore intermediaries, patterns that could similarly arise in state-linked SOE or procurement flows. Informal cash and remittance movements across the Komatipoort, Lebombo and Kosi Bay corridors remain substantial, often linked to wage remittances, small trade and contraband smuggling, blurring licit and illicit funds. Additionally, the Cabo Delgado insurgency has generated TF and PF-adjacent risks, with proceeds from illegal mining, wildlife trafficking and foreign donations possibly channelling through South African-based facilitators or NPOs.

- Zimbabwe: The SA-Zimbabwe corridor is large and proximate, with well documented illicit economy channels. Public reporting and official releases point to gold smuggling and laundering schemes in the SA-Zimbabwe-UAE triangle (e.g. the 'Gold Mafia'[24] investigations and the South African authorities' announcement of an inquiry), as well as persistent tobacco/cigarette smuggling across Beitbridge, the latter evidenced by SARS' destruction of R43m of illicit cigarettes in June 2023.[25] These typologies convert easily into cash-intensive deposits, trade-based ML through commodity trades and complex remittance layering, warranting EDD on gold/tobacco linked counterparties, BO corroboration and targeted transaction monitoring rules.

- Democratic Republic of Congo: The DRC is exposed to conflict-mineral typologies, particularly concerning gold sourced from its eastern provinces, which is frequently smuggled through neighbouring countries before entering South Africa's jewellery, refinery or banking sectors. Payments for gold and other commodities frequently transit through regional intermediaries or offshore structures, masking origin and ownership. South African individuals and firms have been named in media and civil-society investigations for offshore holdings or trading arrangements connected to DRC extractives, highlighting cross-border beneficial-ownership and trade-based ML risks. Supervisors need to monitor commodity trade settlements, substantial cash deposits connected to mining supply chains and transactions from Congolese trading houses, especially when originating documentation appears incomplete or inconsistent.

- Nigeria: South Africa maintains extensive trade and remittance corridors with Nigeria, particularly through informal value transfer services and personal remittances that often bypass regulated channels. Nigeria has systemic vulnerabilities in TF, BO and supervision, which can spill over through bank-to-bank and MVTS corridors. Cash-intensive sectors, including used-vehicle trade and electronics, are prone to trade-based ML. Nigerian nationals operating in South Africa have also featured in cyber-enabled fraud and romance-scam proceeds, with funds remitted through low-value, high-frequency transfers. While no large-scale SA-specific laundering cases are

[26] See https://ofac.treasury.gov/system/files/2023-06/africa_gold_advisory_06272023.pdf

[26] See https://ofac.treasury.gov/system/files/2023-06/africa_gold_advisory_06272023.pdf

public, structuring, remittance layering and correspondent exposures warrant sustained monitoring.

- Kenya: Kenya represents a high-activity corridor within the FATF increased monitoring dataset, with inward flows of R75.1 billion (294 377 transactions) and outward flows of R64.6 billion (3 934 121 transactions) over 2022–2024, and remained on the FATF grey list as at December 2024. The markedly higher outward transaction volumes relative to value suggests a corridor characterised by high-frequency, lower-value transfers (consistent with remittance-like or payment-rail activity), which increases exposure to structuring/smurfing, mule-account usage and rapid pass-through layering, particularly where funds are sent to recurring beneficiaries with weak economic rationale. Banks should apply corridor-specific monitoring focused on velocity, repeat counterparties, and “many-small-to-one” or “one-to-many” transfer patterns, and trigger EDD where the customer’s profile does not support the frequency of cross-border payments, where third-party funding is present, or where beneficiary information and payment messages are incomplete.

- Tanzania: South Africa’s trade and remittance ties with Tanzania centre on gold exports, tourism and diaspora remittances. Tanzania has historically been a transit and smuggling route for East and Southern African gold, which may be laundered through legitimate export channels or offshore intermediaries before reaching South African refineries or markets. Informal cash and hawala networks servicing migrant workers can obscure beneficial ownership and create parallel settlement channels outside regulated payment systems. Although Tanzania exited the FATF grey list in 2025, supervisors should remain alert to gold-linked trade-based ML, over/under-invoicing in trade data and cash-intensive small-value cross-border transfers indicative of layering.

- Türkiye: Türkiye’s strategic role as a trade bridge between Africa, the Middle East and Europe, creates indirect exposure for South Africa through commodity trading, automotive parts and electronics imports. Türkiye vulnerabilities include cross-border fund movements, crypto-asset supervision and TF/PF financial controls. South African corporates importing from or exporting to Turkish partners should be screened for payment transparency completeness, especially when intermediated via third-country banks or digital-asset platforms, layering via over-invoicing in bilateral trade,

and crypto-exchange-linked payments reflecting residual weaknesses in CASP oversight.

- Uganda: The Uganda-South Africa corridor is characterised by diaspora remittances, NGO/NPO transactions and small-trade settlements. Uganda demonstrated notable weaknesses in its oversight of TF and NPO, particularly in relation to transfers within the non-profit sector. South African banks and remitters handling NPO funding into Uganda should verify purpose, project partners and end beneficiaries, ensuring alignment with TF risk-based approaches rather than blanket de-risking. Additionally, cash courier movements between Johannesburg and Entebbe remain active, posing structuring and declaration risks.

- Côte d'Ivoire: Côte d'Ivoire shows material outward value within the increased monitoring dataset, with inward flows of R14.6 billion (38 743 transactions) and outward flows of R49.2 billion (26 968 transactions) over 2022–2024, and remained on the FATF grey list as at December 2024. The relatively low transaction counts compared to value indicate a corridor more consistent with higher-value corporate/trade settlement behaviour, which heightens vulnerability to trade-based money laundering (over/under-invoicing, third-party payments, use of intermediaries) and to beneficial-ownership opacity where corporates or layered structures are involved.

- Mali: the inclusion of Mali under FATF monitoring reflects systemic vulnerabilities in AML/CFT effectiveness amid political instability. For South Africa, the main risk channel lies in conflict-gold and Sahel-region illicit economies, where gold mined in Mali may be co-mingled with other sources and exported via regional hubs to Dubai or Johannesburg. NPO and humanitarian-aid flows into Mali also carry potential TF diversion risks in high-risk provinces. South African banks facilitating such transfers should apply risk-based monitoring, confirming implementing partners and project end-use and view gold-related trade finance involving Mali as a high-priority EDD domain.

7.3.4 Additional high-risk corridors

South African banks maintained only modest interactions with Iran and Myanmar in 2024, with both jurisdictions currently subject to FATF calls for action.

- Iran: Classified by FATF as a high-risk jurisdiction subject to calls on members to apply effective countermeasures under recommendation 19, with materially heightened controls and, where warranted, limiting or declining correspondent and trade-related financial activity. In parallel, UN Security Council Resolution 2231 (2015) retains specific Iran-related restrictions, with many jurisdictions applying additional national sanctions regimes.
-

  Iran's total financial flows with South Africa are relatively small, with approximately R15.6 million in credits and R8.1 million in debits. Based on available transactional data, there is no indication that these flows were associated with sanctions evasion or other illicit activities. However, given the elevated risk profile, continued monitoring of payment routing, counterparties and sanctions-screening controls remain prudent.

  Banks must therefore apply TFS screening, route-checking and scrutiny of documentation for potential evasion through third-country banks, trading companies and trans-shipment.

- Myanmar: Listed by FATF as a high-risk jurisdiction subject to calls on members to apply EDD proportionate to risk, Myanmar's total financial flows with South Africa indicate R18.3 million in credits, compared to just R4.0 million in debits. These transactions are primarily related to travel and services for South African residents traveling abroad, with no indication that these flows are associated with sanctions evasion or other illicit activities.

  Banks should nevertheless apply strengthened sanctions and proliferation-financing controls, verify beneficial ownership where trading companies are used, scrutinise routing through third countries and ensure complete payment-message data, while avoiding indiscriminate de-risking of legitimate humanitarian or NPO flows.

Table 7: Cross-border flows between FATF high risk jurisdictions

Year	Iran		Myanmar	
	Inward (ZAR)	**Outward (ZAR)**	**Inward (ZAR)**	**Outward (ZAR)**
2022	8 748 271	12 496 757	12 329 526	1 281 802
2023	13 802 545	8 586 072	18 973 442	4 612 397
2024	15 636 568	8 062 022	14 846 934	3 830 876

- DPRK (North Korea): The DPRK sits on FATF's call for action list and under broad UNSCR 1718 sanctions. Transactions are therefore generally prohibited and residual risk arises mainly through indirect exposure (e.g. trade diversion via third countries, mis-declared goods or shell entities with concealed DPRK links). For South African banks, the principal controls include robust TFS screening, enhanced scrutiny of maritime/shipping anomalies and payment transparency, with a strong default bias to exit relationships where DPRK nexus is suspected.

- China (and Hong Kong SAR): China is South Africa's largest goods-trading partner, with two-way trade measured in the tens of billions of US dollars, dominated by SA mineral exports and Chinese manufactured imports. At this scale, even a low ML base rate yields a material absolute exposure to trade-based money laundering (TBML), with risks including over/under-invoicing, phantom/over-shipments, carousel trades and complex third-party settlement chains, all classic TBML patterns per FATF/Egmont typology work.

- Ghana: As a West Africa gold route exemplar, the growing body of research shows systemic under reporting and smuggling of African gold to the UAE and other hubs, with Ghana repeatedly highlighted. SWISSAID's 2024 analysis estimates 435 tonnes of African gold were illicitly exported in 2022 (majority to the UAE), and 2025 reporting quantifies multi-year losses for Ghana stemming from smuggling via regional transit routes (e.g. Togo, Burkina Faso and Mali) and hand-carried shipments to Dubai. For SA banks, the risk is indirect but real, with SA refineries, traders or counterparties exposed to co-mingled with conflict/artisanal and small-scall gold mines (ASGM) gold, and payments may transit SA correspondents even when physical flows bypass SA.

7.3.5 Illicit gold dealing

Beyond any single jurisdiction, illicit gold dealing in sub-Saharan Africa is repeatedly identified as high-risk for ML, TF and PF circumvention.

The US Inter-Agency Africa Gold Advisory (2023) warns of systemic corruption, smuggling and conflict-financing linkages across the gold supply chain and urges EDD. Recent UNODC work highlights the embedding of organised crime and money laundering in minerals supply chains.

For SA, which is a regional trading, refining and payments hub, this translates into supervisory expectations that banks treat precious-metals-linked flows as EDD triggers, test provenance and chain-of-custody claims, apply sector-specific trade management scenarios (cash-for-gold, scrap/refining inflows, atypical refiners/dealers), and monitor for routing via the UAE/Türkiye/Swiss hubs where trade-data discrepancies persist.[26]

7.4 Delivery channel risks

Delivery channel risks refer to the potential for ML/TF/PF activities to be facilitated through the methods and channels used by banks to distribute their products, interact with clients and the methods of account origination.

[26] See https://ofac.treasury.gov/system/files/2023-06/africa_gold_advisory_06272023.pdf

Delivery channels are typically divided between face-to-face and non-face-to-face channels that pose certain unique vulnerabilities for abuse. Illicit actors may exploit delivery channels that limit an institution's understanding of its customers' identities and activities. These channels significantly influence the sector's risk profile, as some may offer higher levels of anonymity or reduced transparency.

7.4.1 Face-to-face delivery channels

The banking sector's delivery channels have evolved over time, with the typical use of face-to-face or in-branch visits by clients decreasing greatly, while contactless or remote and virtual onboarding of clients increasing substantially. The COVID-19 pandemic has also affected the use of face-to-face banking channels within the sector. Although traditional face-to-face or branch interactions remain and are utilised by a large population of clients, there has been a sharp uptake in non-face-to-face banking.

7.4.2 Non-face-to-face delivery channels

With the adoption of new technologies in South Africa, the banking sector's delivery channels have seen significant movement to non-face-to-face banking, which are generally higher risk for illicit finance since such channels make it harder for institution to verify customer's identity and activities. Increasing reliance on digital onboarding heightens the risk of identity fraud and insufficient customer verification.

An analysis of the risk return data for the review period showed that the following delivery channels were identified as being used by most clients:

- ATMs enable anonymous cash deposits and withdrawals without face-to-face interaction, allowing criminals to structure transactions just below the R49 999 reporting threshold or use multiple machines to avoid detection. This tactic supports the placement of illicit funds into the financial system. Additionally, ATMs facilitate cross-border smurfing, where large sums are broken into smaller transactions and moved internationally using issued cards. Criminals may also exploit retail customers as money mules or use shell companies to deposit illicit funds, sometimes with insider

help to bypass controls. Despite monitoring efforts, the 24/7 availability and limited real-time oversight of ATMs remain key vulnerabilities.

- Internet banking facilitates rapid, remote transfers that can be exploited for layering illicit funds across accounts and jurisdictions, complicating detection and traceability. Criminal actors increasingly leverage digital onboarding channels, employing stolen or synthetic identities, deepfake technologies and forged documents to bypass CDD controls. This typology has been observed to be growing across the African region, particularly where remote verification systems are less robust. South African banks should therefore ensure that customer identification and verification processes for non-face-to-face channels are commensurate with the institution's assessed level of ML/TF/PF risk. In higher-risk scenarios, this may include the use of multi-factor authentication, biometric verification or enhanced fraud monitoring, while for lower-risk or well-controlled products, simplified measures may suffice. The emphasis should remain on a risk-based application of controls, ensuring that technology-driven channels are subject to ongoing monitoring, anomaly detection and periodic review proportionate to the risk exposure of each service type.

- Mobile banking offers fast, 24/7 access through mobile applications and unstructured supplementary service data (USSD) and short message services (SMSs), which support financial inclusion but can also enable rapid layering of illicit funds, especially outside regular banking hours. Criminals may exploit SIM-swap fraud to hijack mobile numbers, intercept one-time passwords and take over accounts, often moving funds quickly once access is gained. While banks are shifting to app-based and biometric authentication to counter this, risks remain. Mobile wallets and instant money services can also be abused, particularly when recipients withdraw cash without formal accounts, using fake identities or unregistered SIMs to bypass controls. Though banks apply KYC and transaction monitoring, the speed and volume of mobile transactions pose ongoing challenges. Corporate mobile banking, though less common, carries risks if devices are compromised, prompting businesses to adopt strong device security and dual authorisation for high-value payments.

- Telephonic banking, though less commonly used, still poses notable risks. Without face-to-face verification, telephonic banking is vulnerable to impersonation and social engineering, where criminals use stolen personal data to bypass security checks. Fraudsters may also pose as bank staff to trick customers into revealing credentials or authorising transfers, leading to unauthorised fund movements and potential ML or TF. Strong multi-factor verification, limiting high-risk actions over the phone and requiring secondary confirmations like call-backs or SMS codes mitigate the risks. Staff training and transaction monitoring is vital to mitigate against this risk.

- Intermediaries pose a high risk due to their ability to obscure the true identity of clients and the source of funds. Acting on behalf of multiple parties, they complicate client due diligence (CDD) and increase exposure to ML, TF and PF, especially when operating across jurisdictions with varying regulatory standards.

- Agents often operate in informal or remote areas with limited oversight, leading to inconsistent KYC practices and high volumes of cash transactions. These cash-intensive operations, combined with weak integration into bank compliance systems, heighten third party and monitoring risks.

- Fintech and third-party platforms pose additional integration challenges to banks, resulting in fragmented CDD and transaction monitoring. Rapid onboarding, regulatory gaps and opaque ownership structures may further complicate risk assessments and due diligence.

- Mobile service provider partnerships can create compliance gaps. Weak SIM registration controls, limited transaction visibility and exposure to telecom-sector risks, such as fraud and identity theft, add to the complexity of managing these partnerships.

7.5 Sub-sector vulnerabilities

The vulnerabilities and inherent ML, TF and PF risks for each of the five banking sub-sectors are detailed below.

7.5.1 Large domestic banks

This subsector comprises of the six largest domestic banks in South Africa, which as at December 2024, held approximately R7 607 billion in total assets (92.78% of sector assets) and served approximately 64.5 million customers (80.37% of the sector's customer base).

Large banks also account for the majority of the sector's cross-border connectivity. As of December 2024, the sector held 2 439 correspondent accounts (including 643 nostro and 1 796 vostro accounts), of which large banks held the largest share (2 009 accounts/82.3%). In addition, the sector had 29 MVTS arrangements as of December 2024, with large banks accounting for 21 of these arrangements, which increases exposure to higher-risk payment flows where visibility over underlying customers and transactions may be constrained.

Due to their systemic footprint, product diversity and cross-border linkages, large banks exhibit the following inherent ML, TF and PF risks:

- *Money laundering risk = High*

  The inherent ML risk is high due to the combination of scale, breadth of products and services, and the complexity of customer and transactional activity handled by large banks. Their product suites include higher-risk corporate and cross-border services (including corporate finance and investment products), which create opportunities to obscure beneficial ownership, layer transactions across jurisdictions, and disguise the source and ownership of funds.

  Large banks also channel a material share of the sector's higher-risk cross-border activity through correspondent banking and MVTS arrangements. While the PA notes that the automated monitoring systems of larger banks are generally more sophisticated than the rest of the sector, material exposure remains given transaction scale and product complexity. Notwithstanding the relative sophistication of large banks' monitoring systems, deficiencies remain in the design and application of transaction monitoring rules. These gaps can undermine the effectiveness of

automated controls, leaving vulnerabilities that may be exploited for illicit financial activities.

- *Terrorist financing risk = High*

  The inherent TF risk is high because large banks are the primary conduits for cross-border payments and higher-risk international channels (including correspondent banking and MVTS-type corridors), increasing the probability of attempted TF routing through high-risk geographies, intermediaries or layered payment chains. The PA's 2024 thematic work on TFS screening indicates the sector generally relies on automated tools and established processes, but it also identified vulnerabilities at some banks linked to manual interventions, delayed updates and less frequent screenings, which can elevate exposure in high-volume environments.

- *Proliferation financing risk = High*

  The inherent PF risk is high given large banks' role in facilitating cross-border corporate activity and trade-related flows, where PF typologies can be embedded through dual-use goods, complex supply chains, third-party payments, and sanctions-evasion techniques. Their scale and connectivity (including correspondent banking and MVTS arrangements) means that even low-incidence PF attempts can translate into material exposure if payment transparency, beneficiary controls, or sanctions screening are not consistently effective across the chain. Sector-wide, the PA's thematic work highlights the importance of consistent and robust TFS practices to safeguard against sanctions evasion and related financial-crime risks.

7.5.2 Small to medium domestic banks

This subsector comprises smaller domestic banks with broad retail reach but less systemic footprint and generally lower cross-border connectivity than large banks. As of December 2024, small-to-medium banks held approximately R109 billion in total assets (1.33% of sector assets) and served approximately 15.5 million customers (19.35% of the sector's customer base).

Compared to large banks, their international channels are more limited. As of December 2024, small-to-medium banks accounted for a small share of correspondent accounts (10 accounts/0.4%) and hold 3 of the sector's 29 MVTS arrangements.

- *Money laundering risk = High*

  The inherent ML risk is high because, despite a smaller asset footprint, these banks service a large retail customer base and process high volumes of cash and digital transactions, increasing exposure to placement (including structuring), fraud proceeds, and mule-account typologies—particularly through non-face-to-face channels where identity verification can be more difficult. Notably, this subsector contains the highest number of clients without assigned risk ratings, indicating gaps in customer profiling and periodic review. This subsector also reports fewer CTRs but relatively higher STR/SAR ratios, implying reactive detection rather than systemic monitoring.

- *Terrorist financing risk = Medium*

  The inherent TF risk is medium, largely due to reduced cross-border flows compared to large banks. However, smaller banks' less sophisticated screening engines and manual sanctions updates increase residual risk of processing TF-linked transactions, particularly low-value remittances or diaspora transfers to high-risk regions.

- *Proliferation financing risk = Medium*

  The inherent PF risk is assessed as medium. While small-to-medium banks typically have reduced exposure to complex trade finance and global supply-chain activity compared to large banks, they still participate in cross-border payments and may service import/export customers or corporate clients whose transactions can involve sanctions touchpoints, intermediaries and third-party documentation. The PA's thematic observations on sanctions-screening vulnerabilities reinforce the need for consistent practices, particularly among smaller banks.

7.5.3 Foreign banks

Foreign banks generally operate a wholesale/corporate model and participate in cross-border activity, including intra-group flows and correspondent banking connectivity. As of December 2024, foreign banks held approximately R479 billion in total assets (5.84% of sector assets) and served approximately 61 648 customers (0.08% of the customer base), which is consistent with a primarily institutional/corporate customer profile.

Foreign banks also account for a material share of the sector's correspondent connectivity (420 correspondent accounts; 17.2%).

- *Money laundering risk = Medium-high*

  The inherent ML risk is assessed as medium-high. Retail cash exposure is generally lower than in domestic retail-focused banking, but inherent risk is elevated by cross-border transactions, intra-group flows, and corporate products that may involve complex legal structures and beneficial-ownership chains. Products such as corporate finance and investment services are recognised as higher-risk because they can embed layering opportunities and obscure ownership through complex structures and cross-border reach.

- *Terrorist financing risk = Medium*

  The inherent TF risk is assessed as medium because foreign banks' cross-border payments and group connectivity can be exploited for routing attempts through multiple jurisdictions, including via correspondent networks. The PA's thematic observations highlight that vulnerabilities can arise where screening depends on manual interventions, delayed updates or less frequent screening cycles.

- *Proliferation financing risk = Medium*

  The inherent PF risk for foreign banks is assessed as medium. Although this subsector represents a smaller share of the banking sector and typically offers a narrower product suite, foreign banks are predominantly corporate and institutional in focus and participate in cross-border payments and correspondent banking activity, which the SRA identifies as higher-risk channels for PF due to multi-jurisdictional routing, reliance on third-party documentation, and reduced transparency in underlying parties. The sector's correspondent banking data indicates that foreign banks hold a material share of correspondent connectivity. Consistent with the SRA's PF threat framing, the key inherent exposure arises through trade-related corporate clients and cross-border activity linked to dual-use goods and sanctions-sensitive jurisdictions, even where overall scale is below that of large domestic banks.

7.5.4 Mutual banks

This subsector comprises 3 mutual banks, holding 0.05% of the sector's assets (R4.1 billion) and 0.19% of customers (154 000), and reflect the following inherent ML, TF and PF risks:

- *Money laundering risk = Medium*

  The inherent ML risk is medium because mutual banks often serve cash-intensive customer segments and may rely more on manual onboarding and due diligence processes. While volumes are typically lower than in larger institutions, the reduced automation and potential CDD gaps increase vulnerability to fraud, structuring and insufficient source-of-funds substantiation over the customer lifecycle.

- *Terrorist financing risk = Low*

  The inherent TF risk for mutual banks is assessed as low for the review period, with business models concentrated in domestic retail deposits and lending, and limited exposure to higher-risk products or geographies. As of December 2024, mutual banks held no foreign correspondent accounts, eliminating a principal cross-border transmission channel for TF. During the review period, the legal and supervisory framework for TFS was strengthened (including the FIC's consolidated TFS list and notices under the POCDATARA framework), and FATF recommendation 6 was re-rated to 'largely compliant' in October 2024, further supporting sector-wide mitigation of TF risk.

- *Proliferation financing risk = Low*

  The inherent proliferation financing risk for mutual banks is assessed as low, with small domestically focused and simple deposit and lending products. As of December 2024, this subsector held no foreign correspondent accounts, removing primary cross-border channels through which PF typologies typically propagate. Consistent with the SRA's narrative, exposure is largely indirect and sanctions-screening awareness is still maturing.

7.5.5 Co-operative banks

The 5 co-operative banks licensed under the Co-operative Banks Act, holds 0.01% of banking-sector assets and serves a low-income, geographically dispersed client base.

Following their designation as accountable institutions under item 7A of schedule 1 of the FIC Act in 2023, the PA initiated sectoral AML/CFT/CPF risk assessment that reflected the following inherent ML, TF and PF risks:

- *Money laundering risk = Medium-Low*
  The inherent ML risk is assessed as medium-low, reflecting the subsector's small scale and domestic focus, but with heightened vulnerabilities where onboarding and monitoring controls are under-developed or manual. Risks include cash deposits, member-to-member transfers and incomplete CDD practices, which can weaken customer profiling and reduce the detection of anomalous patterns.

- *Terrorist financing risk = Low*
  The inherent TF risk is low due to the domestic focus of co-operative banks, their limited product offerings, and the absence of foreign correspondent accounts, which significantly reduce exposure to cross-border terrorist financing channels.

- *Proliferation financing risk = Low*
  The inherent PF risk is low because the business models are domestically oriented and do not typically involve trade finance, cross-border corporate activity or international routing vulnerability. Exposure is largely limited to indirect TFS obligations, emphasising the importance of baseline sanctions awareness and screening practices appropriate to scale.

8. Mitigating controls

Assessing the impact of identified mitigating controls on the threats and vulnerabilities faced by banks is essential and involves evaluating the controls in place to ensure they are effective, adequate and functioning as intended to protect against financial crimes and ML/TF/PF risks.

8.1 Regulatory environment

South Africa's banking sector operates under a robust regulatory framework designed to protect consumers, ensure financial stability and prevent financial crimes, with the following key components:

Prudential Authority: The PA is established in terms of section 32 of the Financial Sector Regulation Act 9 of 2017 (FSRA), and is responsible for the prudential regulation of all banks and includes licensing, issuing prudential standards, and prudential supervision focused on safety and soundness, governance, and risk management. The PA is also the designated supervisory body for life insurers in terms of the FIC Act.

Financial Surveillance Department: Operating under the SARB, FinSurv administers exchange controls in South Africa in terms of the Exchange Control Regulations, 1961. The department has the authority to appoint registered banks as Authorised Dealers (ADs) in foreign exchange. The PA supervises the banks as ADs for compliance with their FIC Act obligations and the FinSurv supervises the ADLAs.

National Payment System Department: The National Payment System Department (NPSD), operating under the SARB, regulates payment systems, financial market infrastructures, settlement systems, payment clearing house operators, designated clearing settlement participants, system operators, third-party payment providers, e-money providers, settlement participants and clearing system participants. The PA and NPSD have a Memorandum of Understanding in place that requires the PA to supervise banks for compliance with FATF Recommendation 16.

Financial Sector Conduct Authority: Responsible for market conduct regulation, the Financial Sector Conduct Authority (FSCA) ensures that banks treat customers fairly and offer transparent, priced products.

The FIC Act: Banks, mutual banks and co-operative banks are designated as AIs under items 6, 7 and 7A of schedule 1 of the FIC Act. The FIC Act requires the establishment of effective AML/CFT/CPF programmes, CDD, transaction reporting, training and record keeping, with the PA, as the supervisory body, ensures compliance with these FIC Act obligations.

Financial sector legislation: The Banks Act regulates the licensing and operational conduct of banks in South Africa, including local banks and branches of foreign banks or foreign-controlled banks. The Mutual Banks Act regulates the licensing and operational conduct of mutual banks in South Africa. The Co-operative Banks Act regulates the licensing and operational conduct of cooperative banks in South Africa. The Financial Sector Regulation Act provides overarching financial regulations over the banking sector to preserve and enhance financial stability.

8.2 Market entry

Market entry requirements serve as the front line of defence for regulators and supervisors, ensuring that only entities meeting specific criteria are permitted to operate within the banking sector. This includes implementing appropriate market entry policies and procedures, such as licensing, registration and fit and proper checks to assess the suitability of individuals and entities seeking entry.

The PA is responsible for regulating and supervising financial institutions as informed by the relevant empowering financial sector legislations, to enhance and protect financial stability in South Africa. The licensing requirements for banks in South Africa are robust and comprehensive, ensuring that only institutions meeting stringent criteria can operate within the sector.

The PA oversees the licensing process, which includes rigorous assessments of an applicant’s financial resources, governance structures, risk management practices and internal control systems. Applicants are expected to demonstrate their fitness and

propriety, their ability to maintain financial stability and adhere to sound risk management protocols.

8.3 Internal controls

The FIC Act obligates banks to establish effective AML/CFT/CPF programmes, conduct CDD, report relevant transactions to the FIC, provide training to its employees and keep records of all prescribed documents, with the board of directors and/or senior management of banks required to ensure that the institution and its employees comply with these FIC Act obligations.

The PA, as the supervisory body, ensures compliance by banks with the FIC Act obligations by conducting FIC Act inspections to assess levels of compliance with the various obligations. FIC Act inspections conducted by the PA over the review period highlight the following common non-compliance areas.

8.3.1 Risk Management and Compliance Programme

One of the most initially pervasive non-compliance issues identified was the inadequate development, documentation and implementation of a bank's Risk Management and Compliance Programme (RMCP) in terms of section 42 of the FIC Act, with many institutions failing to develop, maintain and/or implement effective RMCPs that fully complied with the requirements of the FIC Act. However, since 2019, banks, in particular larger banks have made improvements to their RMCPs, as evidenced by the outcome of inspections showing reduced compliance findings.

8.3.2 Business risk assessments

In accordance with section 42 of the FIC Act, all banks are required to identify, assess, monitor, mitigate and manage the risk that their products or services could be exploited for ML, TF or PF. A well-structured business risk assessments (BRA) is therefore critical in ensuring that institutions understand their ML/TF/PF risk and that this forms the foundation upon which the RMCP is premised. Failure to appreciate the risks will result in the incorrect controls being implemented.

The PA conducted thematic reviews in 2022 and 2024 to evaluate the adequacy, maturity and effectiveness of BRAs across the banking sector. The 2024 review identified notable improvements in the quality, structure and contextual relevance of BRAs compared to the 2022 baseline. Most banks demonstrated a stronger identification and assessment of ML and TF risks, improved articulation of methodology and a more systematic approach to risk rating and control assessment. However, residual challenges remain, particularly in linking control effectiveness to residual risk, weighting inherent risk factors and contextualising typologies to South Africa's unique threat environment.

Money laundering risks: The sector's ML risk exposure remains high, shaped by both domestic predicate-crime trends and cross-border financial linkages. Most banks effectively identified traditional inherent risk categories, customers, products, delivery channels and geographies in their BRAs, but some BRAs remained generic and insufficiently tailored to the South African context.

Where maturity was stronger, BRAs captured the key domestic ML threats, including:

- corruption and public-sector fraud, particularly in procurement and politically exposed client segments;
- cyber-enabled fraud and business email compromise, where illicit funds are layered through multiple accounts via EFTs and online banking;
- bribery and kick-back schemes in state-linked or high-value sectors such as mining, logistics and infrastructure;
- Ponzi and pyramid schemes, leveraging retail deposits and social investment networks;
- trade-based laundering, tax evasion and informal cross-border value transfers;
- illegal wildlife trade, gold smuggling and other commodity-linked laundering typologies; and
- virtual asset transactions, which pose traceability and BO-verification challenges.

Key vulnerabilities highlighted by BRAs include high transaction volumes, diverse delivery channels, complex customer structures and variable control depth across business lines. While improvements were observed in beneficial ownership identification, data integration gaps persist where group-wide systems are not fully aligned. Some banks continue to rely on aggregate risk scoring in their BRAs rather than disaggregating product-specific or jurisdiction-specific threats, which can obscure risk concentration areas.

Terrorist financing risks: The sector's TF exposure is moderate, though contextually significant given regional vulnerabilities and growing transnational linkages. BRAs increasingly acknowledge TF risks but many still underestimate non-traditional channels, particularly where small value, high-frequency transactions intersect with charitable or remittance flows.

Commonly identified TF risk channels include:

- cross-border remittances and low-value transfers to and from East Africa, the Horn of Africa and the Middle East, where designated or conflict-affected jurisdictions are present;

- NPOs with weak beneficiary due diligence, unclear funding chains or limited transaction monitoring;

- layering via correspondent banking or third-party payments, masking the ultimate beneficiary or origin; and

- legacy accounts with incomplete CDD where ongoing sanctions screening or periodic review is inconsistent.

Despite BRA improvements, TF risk is often assessed collectively with ML, leading to limited granularity in typology analysis. Only a subset of institutions demonstrated a clear understanding in their BRAs of regional TF threats, local recruitment or facilitation risk and funding through front entities. The PA observed a need for enhanced scenario-based testing and better calibration of transaction monitoring rules to detect TF-linked behaviour patterns.

Proliferation financing risks: Thematic reviews show growing awareness of PF obligations, but institutional responses remain uneven. Except for the majority of the largest banks, BRAs recognise PF primarily through the lens of TFS compliance without fully assessing the transactional, trade-finance and supply-chain risks associated with dual-use goods or high-risk jurisdictions.

Key PF exposure points include:

- trade finance instruments, including letters of credit and documentary collections involving dual-use goods;

- cross-border corporate clients operating in strategic industries (engineering, manufacturing and chemicals);

- correspondent relationships with banks in higher-risk regions, where screening scope is limited to counterparty rather than underlying client; and

- insufficient staff training on PF typologies and UNSCR 1718/2231 obligations.

While larger institutions have begun mapping PF-sensitive product lines and conducting TFS screening assurance, smaller and foreign banks remain reactive, often limiting PF coverage to static list screening. The absence of dual-use goods code mapping and weak escalation frameworks suggest that PF risk management is still at an early stage of maturity across parts of the sector.

Residual risk and control assessment weaknesses: Although BRA structures have improved, many banks still struggle to link inherent and residual risk ratings to control evidence. In several cases, methodologies describe risk-scoring logic but do not operationalise weighting or data thresholds. Control assessments are frequently aggregated, masking performance differences across business lines or products.

Notable BRA weaknesses include:

- inconsistent weighting of control categories (CDD, EDD, ODD, client screening and governance);

- limited quantitative data inputs (e.g. transaction volumes, STR trends or exposure metrics);

- insufficient commentary on the design and operating effectiveness of specific controls; and

- lack of periodic validation between BRA residual ratings and actual reporting outcomes (e.g. STR/SAR submissions).

More advanced institutions have adopted integrated dashboards, segment-specific risk scoring and mitigation plans tied to identified vulnerabilities. However, a sector-wide gap persists in documenting control performance at granular level, reducing transparency on how residual risk is derived.

8.3.3 Beneficial ownership

Incomplete or inaccurate beneficial ownership (BO) information remains a material vulnerability, particularly for complex corporate structures and trusts. A significant proportion of clients with undetermined BO increases inherent ML/TF/PF risk because it weakens banks' ability to understand who ultimately owns or controls the customer and whether the relationship or transactions may be linked to predicate criminality, terrorism financing or proliferation financing.

PCC 59[27] specifically highlights that criminals frequently abuse legal persons, trusts and partnerships to obscure ownership and control, including the e creation of multiple layers of ownership that make it difficult to identify the ultimate beneficial owner and increase the susceptibility of certain structures to misuse.

In addition to ownership, banks should identify "effective control" (i.e., the ability to influence or direct an entity's activities through ownership, voting rights, decision-making

[27] https://www.fic.gov.za/wp-content/uploads/2024/08/PCC-59-Beneficial-ownership.pdf

authority and/or informal influence) and treat control indicators as a core component of the BO determination under a risk-based approach.

PCC 59 also reinforces that the level of scrutiny applied to BO should be risk-based and, where necessary, supported by corroboration from multiple information sources (including public sources and additional documentation to validate the stated ownership/control structure). Where a bank is unable to identify a beneficial owner and take reasonable steps to verify that person, the bank must not establish the business relationship or proceed with a single transaction and should consider submitting a suspicious and unusual transaction report. PCC 59 further emphasises the need to scrutinise BO information to assess exposure to targeted financial sanctions.

During the review period, the PA noted improvements in banks' BO determination, suggesting stronger compliance behaviour and a better appreciation of the risk posed by opaque ownership and control chains.

8.3.4 Targeted financial sanction screening

South Africa gives effect to United Nations Security Council (UNSC) TFSs through sections 26A, 26B, 26C and 28A of the FIC Act and related provisions of the Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004, with the FIC publishing the South African TFS List and issues notices under section 26A of the FIC Act.

Accountable institutions must screen against the FIC's TFS List, freeze property without delay on a true match, not make funds or services available to such clients/beneficiaries, and file a section 28A report with the FIC.

For banks, the client and the BO of the client must be screened at on-boarding. At transaction stage, the payee and payor must be screened before the transaction is processed, with screening done promptly against the FIC TFS List and against any List updates

The use of additional foreign lists, such as those of the US Office of Foreign Assets Control (OFAC) or European Union (EU), is optional and may be applied as a risk-based overlay, but it is not a South African legal requirement.[28]

In 2024, the PA conducted a thematic review of the effectiveness of the TFS screening mechanisms across the banking sector, revealing the following key insights:

- Most institutions screen against comprehensive lists, including those from the UNSC, OFAC, the EU, HM Treasury and the FIC.

- Some institutions also use specialised lists addressing high-risk jurisdictions or sector-specific risks.

- The banking sector's reliance on automated tools and established processes helps mitigate TFS-related risks.
- For some banks, there are gaps in manual interventions, delayed updates and less frequent screenings, which increases vulnerabilities.

The deficiencies expose a few banks to TFS risk, introducing vulnerability and underscoring the need for consistent sanction-screening application and robust practices to safeguard against sanctions evasion and associated financial crime risks. The PA has however taken action to address areas of weaknesses identified, particularly amongst the smaller banks, and required these to be addressed.

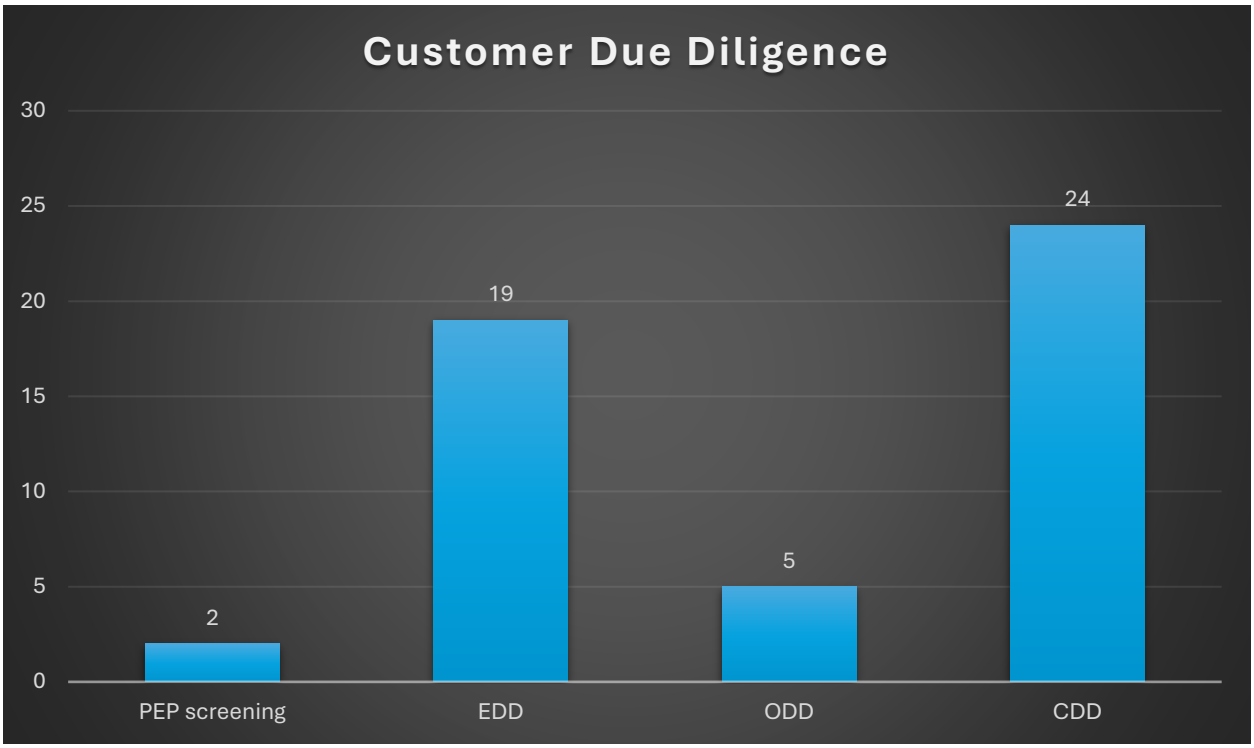
8.3.5 Customer due diligence

The PA has seen that although there are several non-compliance findings made in terms of sections 20A, 21 and 21A to H of the FIC Act, there were improvements with the rate of compliance across more mature banks decreasing, attributable to guidance and enforcement action undertaken by the PA.

During the review period, inspections conducted by the PA on the banking sector revealed CDD as the most prevalent non-compliance issue as detailed below.

[28] See https://www.fic.gov.za/wp-content/uploads/2024/02/2027.2-PCC-PCC-44A-Targeted-financial-sanctions.pdf

Figure 9: CDD non-compliance



8.3.6 Transaction monitoring

Banks are required to establish policies, procedures, processes and systems to continually monitor customer transactions, identify patterns and red flags that may indicate ML, TF, PF or other illegal activities by identifying deviations from expected customer activities or behaviours.

During the review period, the inspections conducted by the PA noted that 18 banks had deficient or non-compliant transaction monitoring rules.

8.3.7 Reporting requirements

The FIC Act obligates banks to report certain types of transactions or activities to the FIC, within a stipulated period. During the review period, the inspections conducted by the PA noted the following reporting non-compliance:

- **Cash threshold reporting**

Section 28 of the FIC Act places an obligation on all AIs to file CTRs for cash transactions received or paid above R49 999.99, within three business days of becoming aware of the transaction.

Over the review period, the banking sector submitted more than 7.2 million CTRs, accounting for approximately 89% of all CTRs filed with the FIC.

Although this CTR reporting volume remains substantial, it represents a marked decline compared to earlier reporting cycles occasioned by the 2017 amendments to the FIC Act and Directive 2 of 2017, which raised the single-transaction reporting threshold from R24 999.99 to R49 999.99 and removed the requirement to report aggregated cash transactions. These changes were intended to reduce administrative burden and refocus reporting on higher-value, higher-risk cash activities.

Table 8: CTRs filed

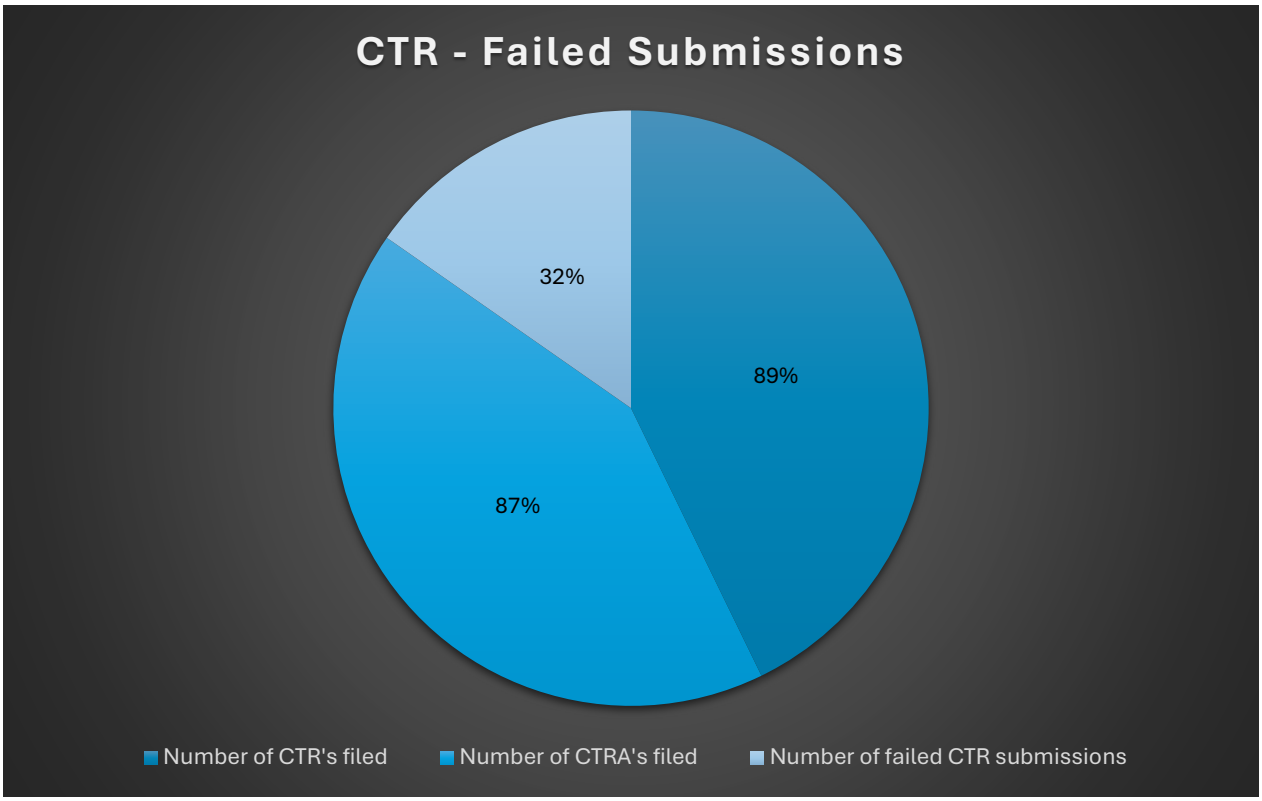
Quarter	Automated CTR filings	Manual CTR filings	Late CTR filings
Q2 2022	537 910	1 789	12
Q3 2022	552 168	2 500	84
Q4 2022	620 278	1 080	42
Q1 2023	690 626	366	53
Q2 2023	613 156	245	427
Q3 2023	663 417	321	3 520
Q4 2023	677 620	264	955

Q1 2024	623 411	458	216
Q2 2024	698 708	327	376
Q3 2024	723 978	327	5 164
Q4 2024	797 978	317	90

Notably, the majority of CTRs are submitted through automated submissions, with a small number filed manually. Overall and in comparison, to the number of CTRs filed, the banking sector has a low incidence of late CTR reporting.

The high rate of failed CTR submissions is however of concern, with 32% recorded during the review period. These failures are primarily due to the omission of mandatory information sets, such as Swift Code, client ID/passport number and transaction mode or fund type. These omissions cause the submissions to fail the FIC's reporting system's validation checks and prevent successful submission.

Figure 10: Failed CTR submission



During the review period, inspections conducted by the PA revealed the following CTR non-compliance issues:

- Failure to timeously report CTRs to the FIC − with 78 banks found to be non-compliant.
- Failure to report CTRs to the FIC − with 2 banks found to be non-compliant.
- Incorrect reporting of CTRs − with 1 bank found non-compliant.
- CTR data issues were identified at 2 banks during the review period.

- **Suspicious and unusual transaction reporting**

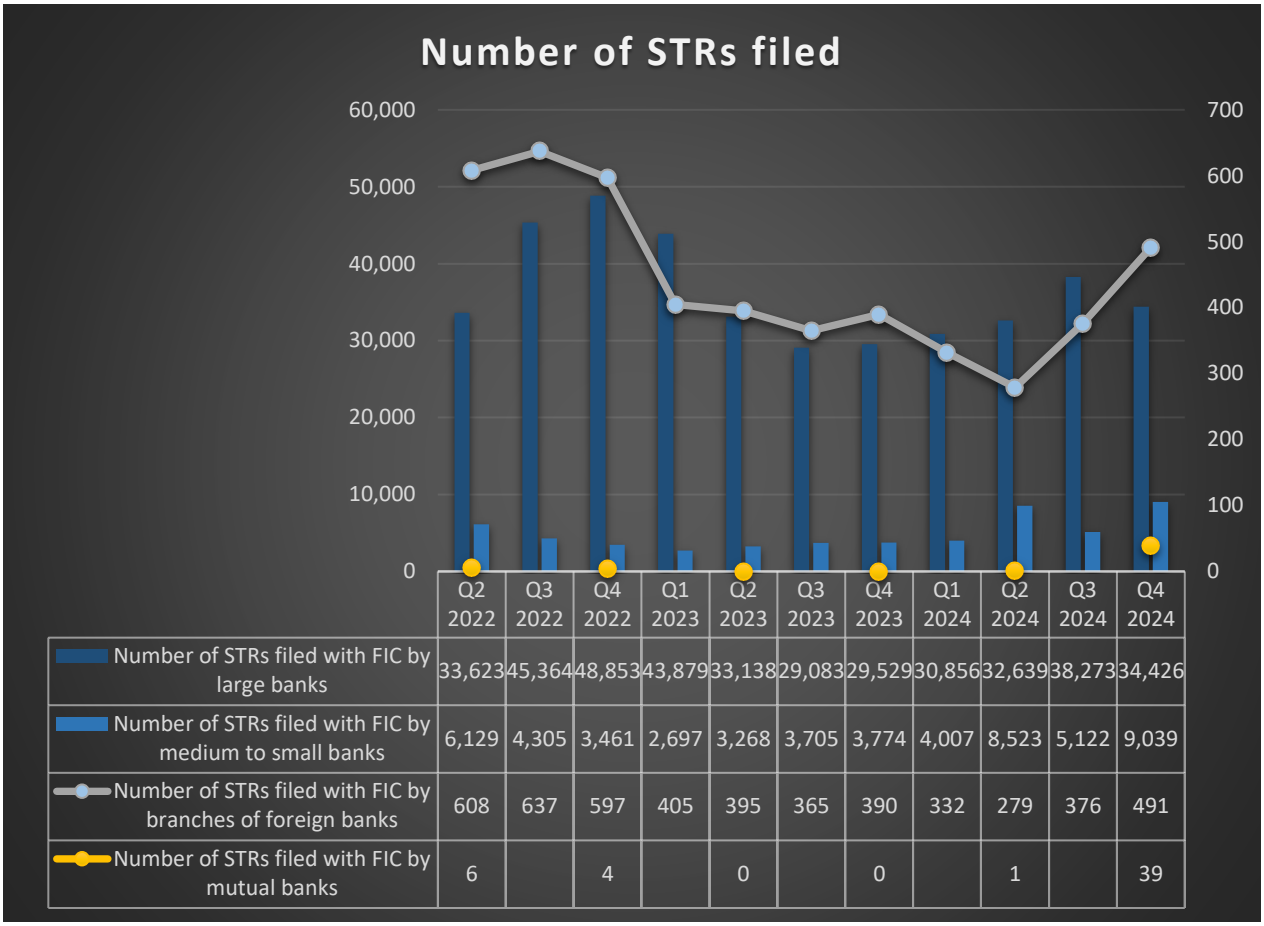
Section 29 of the FIC Act obligates AIs to file STRs and SARs with the FIC, within 15 days of becoming aware that there are reasonable grounds to suspect that they have received or facilitated the payment of the proceeds of crime or other identified types of illicit activities.

The banking sector filed 76% of all STRs and 77% of all SARs across all Ais, with the majority of high quality, containing sufficient information for effective analysis. Additionally, the banks provide supplementary information in support of section 29 reports, which assists the FIC in mapping the flow of funds.

The PA has noted that the automated transaction monitoring systems of the larger banks are more sophisticated than the rest of the banking sector.

However, there are still instances where banks failed to comply with regulatory obligations, including not adhering to reporting timelines, submission of incomplete reports due to missing client or transaction information, failure to identify all products and services and submitting reports to the FIC without proper quality assurance and completeness checks.

Figure 11: Number of STRs filed



	Q2 2022	Q3 2022	Q4 2022	Q1 2023	Q2 2023	Q3 2023	Q4 2023	Q1 2024	Q2 2024	Q3 2024	Q4 2024
Number of STRs filed with FIC by large banks	33,623	45,364	48,853	43,879	33,138	29,083	29,529	30,856	32,639	38,273	34,426
Number of STRs filed with FIC by medium to small banks	6,129	4,305	3,461	2,697	3,268	3,705	3,774	4,007	8,523	5,122	9,039
Number of STRs filed with FIC by branches of foreign banks	608	637	597	405	395	365	390	332	279	376	491
Number of STRs filed with FIC by mutual banks	6		4		0		0		1		39

During the review period and according to the FIC, 1.7 million STRs were filed through automated reporting systems, with approximately 147 000 submitted manually and 2 905 STR/SARs filed late.

The PA's inspections on the banks during the review period revealed non-compliance with STR obligations in several areas:

- Inadequate alert investigation processes − with 14 banks found to be non-compliant.
- Failure to submit STRs to the FIC in a timely manner − with 14 banks found to be non-compliant.
- Failure to address alerts within 48 hours − with 10 banks found to be non-compliant.
- STR data issues identified at 10 banks during the review period.

- Alerts closed after more than 15 days − with 9 banks found to be non-compliant.

- Incorrect STR reporting − with 2 banks found to be non-compliant.

- Failure to report STRs − with 2 banks found to be non-compliant.

- Inadequate governance and oversight over ATMS − with 2 banks found to be non-compliant.

In addition to institution-specific follow ups, the PA has also undertaken industry-wide awareness initiatives to promote consistent understanding of FIC Act compliance obligations and strengthen the sector's overall AML/CFT maturity.

- **Terrorist property reporting**

Section 28A of the FIC Act places an obligation on all AIs to file a report with the FIC if the AI knows that it possesses or controls property linked to a person or entity that has committed an offence in terms of the POCDATARA or linked to a person or entity that is identified pursuant to a UNSCR contemplated in section 26A(1) of the FIC Act.
During the review period and according to the FIC, a total of 14 TPRs were filed, with 9 TPRs coming from the banking sector.

The inspections on the banking sector, conducted by the PA during the review period, revealed that four banks were found to be non-compliant with section 28A of the FIC Act.

- **International funds transfer reporting**

Section 31 of the FIC Act obligates AIs to report to the FIC all electronic fund transfers, either inbound and/or outbound from the borders of South Africa, exceeding R19 999.99 or its foreign currency equivalent, as soon as possible but not later than three days after the AI becomes aware of the transaction.

The international funds transfer reporting (IFTR) obligations came into effect in February 2023 and apply to banks that engage in cross border EFTs as per above.

The PA's inspections in 2024 revealed that most banks were still in the process of fine tuning their reporting systems to enable full compliance with their IFTR obligations.

8.3.8 Training

In terms of section 43 of the FIC Act, AIs must provide ongoing training to its employees to enable them to comply with the provisions of the FIC Act and the institution's RMCP.

Training programmes are crucial for ensuring employees understand their AML/CFT/CPF roles and responsibilities as well as how internal controls manage illicit finance risks. These programmes should enable employees to identify and report red flags signalling illicit activity.

Training should include new hire sessions, annual refreshers, and role-based training for staff with financial crime compliance-related duties and sessions for the BoD and senior management.

During the review period, inspections conducted by the PA revealed that six banks were found to be non-compliant with their AML/CFT training obligations, with several deficiencies were noted in AML/CFT/CPF training programmes. Many institutions also failed to provide ongoing or refresher training, with no evidence of regular training updates. Training was often generic and not tailored to specific job functions, leaving high-risk roles such as those in trade finance or cross-border payments without targeted guidance. Training records were inadequate, with training registers, attendance logs and certificates either missing or incomplete, and there was no centralised system to track staff training.

Furthermore, training effectiveness was rarely assessed, with no post-training evaluations or feedback mechanisms, and attendance was often the only measure of compliance.

Lastly, training was not well integrated into the banks' RMCP, which frequently lacked clear details on training scope, frequency, responsible parties and evaluation methods.

8.3.9 Record keeping

In terms of sections 22, 22A, 23 and 24 of the FIC Act, AIs must keep CDD and transaction records for at least five years and inform the FIC and the supervisory body if a third party is appointed to fulfil the AI's record-keeping obligations.

Proper, accurate and comprehensive record keeping helps banks maintain transparency, manage risks, prevent financial crimes, provide clear audit trails, support regulatory inspections and protect customer information.

During the review period, inspections by the PA revealed that 7 banks were non-compliant with their record-keeping obligations by failing to maintain the prescribed records or did not inform the PA and the FIC about the appointment of a third-party record keeper.

8.3.10 Governance

Section 42A of the FIC Act obligates the BoD and/or senior management of a bank to ensure that the institution and its employees comply with the provisions of the FIC Act and require the appointment of a compliance officer, with sufficient competence and seniority, to assist the BoD and/or senior management in ensuring compliance with the FIC Act.

A strong governance framework ensures that bank's compliance departments have the authority, independence, resources and information needed to manage financial crime compliance risks. It includes clearly documented AML/CFT/CPF roles, responsibilities, reporting lines and escalation channels to the board and/or senior management. A clear compliance structure and the role of senior management in setting the 'tone from the top' are crucial for effective governance of banks.

8.4 Supervision

8.4.1 Supervisory resources and activities

The PA is responsible for regulating and supervising the banking sector, as informed by the financial sector legislation of South Africa. The PA is a dedicated and empowered supervisor with sufficient financial, human and material resources. The AML/CFT/CPF Division of the Financial Conglomerate Supervision Department within the PA has a team of 27 staff focusing on both on and off-site supervision of banks.

The PA also imposes remedial actions on banks post inspections where required, along with administrative sanctions where appropriate to do so.

The PA led several specific thematic reviews on banks, including a detailed review of their BRAs, followed up with dedicated general and individual outreach sessions to help banks understand how to improve their BRAs.

Additional thematic reviews included a review of the implementation by banks of their TFS obligations and a review of their sanction-screening systems.
During the reporting period, the AML/CFT division hosted a series of sector-wide engagements which reached the following number of participants:

Table 9: Outreach session participation

Calendar year	Participants	Average participants per engagement
2022	546	109.2
2023	865	96
2024	857	95.2

The following key topics were covered:

Table 10: Outreach session topics

2022	2023	2024
• Regulatory expectations on ML and TF risk assessment. • Requirements for reporting as soon as possible. • Building an RMCP for a foreign bank. • NPSD EFT Directive. • Terrorist and proliferation risk financing. • Correspondent banking due diligence expectations.	• The business risk assessment exercise. • Modern slavery and human trafficking. • The National Risk Assessment. • STR reporting quality. • The BO registers. • Ransome payments in the banking sector.	• Expectations of targeted financial sanctions. • The role of MVTS and the risks posed by MTVS. • Trust BO register. • Terrorist financial national risk assessment and the non-profit risk assessment. • Tax-related crimes and risks for banks. • Insights from the risk returns submitted.

As a result, the PA effectively supervises the banking, ensuring compliance with supervisory standards and promoting the integrity of the industry. Through regular inspections, thematic reviews and ongoing monitoring, the PA identifies and addresses compliance deficiencies, enhances risk management practices and supports institutions in implementing robust controls. This comprehensive oversight helps to mitigate financial crime risks and ensures the banking sector's resilience against ever-evolving ML/TF/PF threats.

9. Risk Ratings

9.1 Inherent Risk

Based upon the assessment, the threats and vulnerabilities flowing from the ML, TF and PF risks are rated as follows:

Threat assessment

Threats	Domestic banks		Foreign banks	Mutual banks	Co-operative banks
	Large banks	Small to medium banks			
Money Laundering	High	High	Medium-high	Medium-low	Low
Terrorist Financing	High	Medium-low	Medium-low	Low	Low
Proliferation Financing	High	Medium-low	Medium-low	Low	Low

Vulnerability assessment

Vulnerabilities	Domestic banks		Foreign banks	Mutual banks	Co-operative banks
	Large banks	Small to medium banks			
Money Laundering	High	High	Medium	Medium	Medium-low
Terrorist Financing	High	Medium	Medium	Low	Low
Proliferation Financing	High	Medium	Medium	Low	Low

The inherent ML, TF and PF risks for each banking subsector, are as follows:

Inherent risk assessment

Inherent Risks	Domestic banks		Foreign banks	Mutual banks	Co-operative banks
	Large banks	Small to medium banks			
Money Laundering	High	High	Medium-high	Medium	Medium-low
Terrorist Financing	High	Medium	Medium	Low	Low
Proliferation Financing	High	Medium	Medium	Low	Low

9.2 Mitigating controls

Based upon the assessment, the ML, TF and PF mitigating controls for each banking sub-sector are rated as follows:

Mitigating Controls	Domestic banks		Foreign banks	Mutual banks	Co-operative banks
	Large banks	Small to medium banks			
Money Laundering	Adequate	Adequate	Adequate	Adequate	Non-existent
Terrorist Financing	Adequate	Adequate	Adequate	Adequate	Non-existent
Proliferation Financing	Adequate	Weak	Weak	Weak	Non-existent

9.3 Residual risk

The residual ML, TF and PF risks for each banking subsector are therefore rated as follows:

Residual Risks	Domestic banks		Foreign banks	Mutual banks	Co-operative banks
	Large banks	Small to medium banks			
Money Laundering	Medium-high	Medium-high	Medium	Medium-low	Medium-low
Terrorist Financing	Medium-high	Medium-low	Medium-low	Low	Low
Proliferation Financing	Medium-high	Medium	Medium	Low	Low

Annexure 1: Licensed banks in South Africa as at December 2024

Large local banks	
1.	Absa Bank Limited
2.	Capitec Bank Limited
3.	FirstRand Bank Limited
4.	Investec Bank Limited
5.	Nedbank Limited
6.	Standard Bank of South Africa Limited
Small to medium local banks	
1.	African Bank Limited
2.	Bidvest Bank Limited
3.	Discovery Bank Limited
4.	Sasfin Bank Limited
5.	Tyme Bank Limited
Branches of foreign banks	
1.	Access Bank South Africa Limited
2.	Al Baraka Bank Ltd
3.	Bank of China Limited – JHB Branch
4.	Bank of Communications Co. Ltd – JHB Branch
5.	Bank of Taiwan – South Africa Branch
6.	China Construction Bank Corporation – JHB Branch
7.	Citibank NA
8.	Deutsche Bank AG
9.	Goldman Sachs International Bank – JHB Branch

10. HBZ Bank Limited
11. HSBC Bank Plc – JHB Branch
12. JPMorgan Chase Bank – JHB Branch
13. Standard Chartered Bank
14. State Bank of India
Mutual banks
1. Bank Zero Mutual Bank
2. Finbond Mutual Bank
3. GBS Mutual Bank
Cooperative banks
1. Ditsobotla Primary & Credit Co-operative Bank
2. GIG Co-operative Bank Ltd
3. KSK Kooperatiewe Bank Beperk
4. OSK Koöperatiewe Bank Beperk
5. Ziphakamise Savings & Credit Co-operative Bank

Annexure 2: Banking sector red flags

Based on data received from the FIC and other law enforcement authorities, the following financial crime typologies and trends within the banking sector have been identified within the banking sector:

1. Inconsistent account activity

- Flow of funds which does not match the customer's profile.
- Transactional volume exceeding projected activity.
- Activity inconsistent with declared business or occupational information.
- Sudden changes in financial profile or transaction patterns.
- Conducting transactions outside residential or employment area without explanation.

2. Use of accounts for illicit activities

- Unemployed individuals' accounts used for business activities linked to illicit funds and tax evasion.
- Accounts receiving proceeds from scams (e.g. change of banking details scams).
- Accounts credited with illicit proceeds, followed by rapid withdrawals or transfers and then closed.
- Dormant accounts receiving large deposits and rapid withdrawals.
- Use of third-parties' accounts (e.g. spouses) to hide proceeds of crime.

3. Unusual transaction patterns

- Multiple high round figure amounts from unknown sources, rapidly withdrawn.
- Suspicious inward tele-transmissions categorised as 'gifts'.
- Large and unusual cash deposits followed by rapid withdrawals.
- Early settlement of asset-based finance accounts.
- Rapid movement of funds through multiple accounts.

4. High-value asset acquisition (property and/or motor vehicles)

- Dormant accounts receiving sudden huge deposits and followed by rapid withdrawals.
- Concealment of funds within company structures or with relatives, using business ventures as fronts.
- Structuring funds into accounts by making cash deposits at different branches of banks to avoid raising suspicions.
- Use of third-parties' accounts to hide proceeds of crime (e.g. spouses' accounts).
- Large and unusual cash deposits into accounts and rapid withdrawals thereafter.
- Change of account behaviour without explanation.
- Early settlement of asset-based finance accounts.
- Transacting pattern inconsistent with client's profile.

5. Cryptocurrency transactions

- Customers engage in cryptocurrency transactions.

6. Structuring funds

- Cash deposits at different bank branches to avoid suspicion.

Abbreviations

AD	Authorised Dealer
ADLA	Authorised Dealer With Limited Authority
AI	Accountable Institution
AML	Anti-Money Laundering
APN	Advance Payment Notification
ASGM	Artisanal and Small-Scale Gold Mining
ATM	Automated Teller Machine
ATMS	Automated Transaction Monitoring System
Banks Act	Banks Act 94 of 1990
BASA	Banking Association of South Africa
BCBS	Basel Committee on Banking Supervision
BIN	Bank Identification Number
BoD	Board of Directors
BRA	Business Risk Assessment
CASP	Crypto Asset Service Providers
CBR	Correspondent Banking Relationship
CDD	Client Due Diligence
CFI	Co-Operative Financial Institution
CFT	Counter Financing of Terrorism
Co-operative Banks Act	Co-Operative Banks Act 40 of 2007
CPF	Counter Proliferation Financing
CPI	Corruption Perceptions Index

CTR	Cash Threshold Report
CTRA	Cash Threshold Report Aggregation
DPCI	Directorate For Priority Crime Investigation
DPEP	Domestic Politically Exposed Person
DRC	Democratic Republic of Congo
EDD	Enhanced Due Diligence
EFT	Electronic Funds Transfer
EU	European Union
FAIS	Financial Advisory And Intermediary Services Act 37 of 2002
FATF	Financial Action Task Force
FI	Financial Institution
FIC	Financial Intelligence Centre
FIC Act	Financial Intelligence Centre Act 38 of 2001
FinSurv	Financial Surveillance Department
Fintech	Financial Technology
FSCA	Financial Sector Conduct Authority
FSRA	Financial Sector Regulation Act 9 of 2017
GN	Guidance Note
IFTR	International Fund Transfer Report
ISIL	Islamic State Of Iraq and The Levant
IT	Information Technology
IWT	Illegal Wildlife Trade
KYC	Know Your Client

MCC	Merchant Category Codes
ML	Money Laundering
MoU	Memorandum of Understanding
MSHT	Modern Slavery and Human Trafficking
Mutual Banks Act	Mutual Banks Act 124 of 1993
MVTS	Money or Value Transfer Services
NPA	National Prosecuting Authority
NPO	Non-Profit Organisation
NPSD	National Payment System Department
NRA	National Risk Assessment
OCINDEX	The Organized Crime Index
OFAC	The United States' Office of Foreign Assets Control
P2P	Peer-To-Peer
PA	Prudential Authority
PAN	Primary Account Number
PEP	Politically Exposed Person
PF	Proliferation Financing
PIN	Personal Identification Number
PIP	Politically Important Person
POCDATARA	Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 Of 2004
POS	Point-of-Sale
R	Rand

RMCP	Risk Management and Compliance Programme
RTC	Real-Time Clearing
SADC	Southern African Development Community
SAHPRA	South African Health Products Regulatory Authority
SAMLIT	South African Anti-Money Laundering Integrated Task Force
SAR	Suspicious Activity Report
SARB	South African Reserve Bank
SARS	South African Revenue Service
SIM	Security Information Management
SLAs	Service Level Agreements
SOE	State Owned Entity
SRA	Sector Risk Assessment
STR	Suspicious Transaction Report
TBML	Trade-Based Money Laundering
TF	Terrorist Financing
TFS	Targeted Financial Sanctions
TFAR	Terrorist Financing Activity Report
TPR	Terrorist Property Report
UNODC	United Nations Office on Drugs and Crime
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolutions
WMD	Weapons of Mass Destruction