DOCUMENT OF INTERNATIONAL MONETARY FUND AND FOR OFFICIAL USE ONLY

FOR INFORMATION

SM/21/176

September 24, 2021

To: Members of the Executive Board

From: The Secretary

Subject: **South Africa—Detailed Assessment Report on Anti-Money Laundering and Combating the Financing of Terrorism**

Board Action:	Executive Directors' **information**
Publication:	Yes, after Wednesday, September 29, 2021
Questions:	Mr. Dawe, LEG (ext. 39334) Ms. Chen, LEG (ext. 37814)

INTERNATIONAL MONETARY FUND

SOUTH AFRICA

September 24, 2021

DETAILED ASSESSMENT REPORT ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM

Prepared By
Legal Department

This Detailed Assessment Report was prepared in the context of an IMF Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) assessment mission in South Africa during October 22 to November 12, 2019, led by Steve Dawe, IMF and overseen by the Legal Department, IMF. Further information on the IMF's AML/CFT program can be found at:

http://www.imf.org/external/np/exr/facts/aml.htm

CONTENTS

Glossary 6

EXECUTIVE SUMMARY 11

KEY FINDINGS 11

DETAILED ASSESSMENT REPORT 23

ML/TF RISKS AND CONTEXT 23

A. ML/TF Risks and Scoping of Higher Risk Issues 25

B. Materiality 29

C. Structural Elements 30

D. Background and Other Contextual Factors 30

NATIONAL AML/CFT POLICIES AND COORDINATION 43

A. Key Findings and Recommended Actions 43

B. Immediate Outcome 1 (Risk, Policy and Coordination) 44

C. Overall Conclusion on IO.1 53

LEGAL SYSTEM AND OPERATIONAL ISSUES 54

A. Key Findings and Recommended Actions 54

B. Immediate Outcome 6 (Financial Intelligence ML/TF) 57

C. Overall Conclusion on IO.6 65

D. Immediate Outcome 7 (ML investigation and Prosecution) 66

E. Overall conclusion on IO.7 76

F. Immediate Outcome 8 (Confiscation) 76

G. Overall Conclusion on IO.8 85

TERRORIST FINANCING AND FINANCING OF PROLIFERATION 85

A. Key Findings and Recommended Actions 85

B. Immediate Outcome 9 (TF investigation and Prosecution) 90

C. Overall Conclusions on IO.9 96

D. Immediate Outcome 10 (TF Preventive Measures and Financial Sanctions) 96

E. Overall Conclusions on IO.10 101

F. Immediate Outcome 11 (PF Financial Sanctions) 102

G. Overall Conclusion on IO.11 106

PREVENTIVE MEASURES 106
A. Key Findings and Recommended Actions 106
B. Immediate Outcome 4 (Preventive Measures) 108
C. Overall Conclusions on IO.4 119

SUPERVISION 120
A. Key Findings and Recommended Actions 120
B. Immediate Outcome 3 (Supervision) 122
C. Overall Conclusion on IO.3 140

LEGAL PERSONS AND ARRANGEMENTS 140
A. Key Findings and Recommended Actions 140
B. Immediate Outcome 5 (Legal Persons and Arrangements) 142
C. Overall Conclusion on IO.5 147

INTERNATIONAL COOPERATION 148
A. Key Findings and Recommended Actions 148
B. Immediate Outcome 2 (International Cooperation) 149
C. Overall conclusions on IO.2 159

BOXES
1.1. Krejcir Case Study – Predicate Crime and Asset Recovery 63
2.1. Case Example – Procurement Fraud 68
3.1. Case Example – Abalone 68
4.1. Case Example – Illegal Mining 72
5.1. Case Example—VAT Fraud 72
6.1. Case Example—Corruption 75
7.1. Case Example—Virtual Assets 78
8.1. Case Example 1—"State Capture" 79
9.1. Case Example 2—"State Capture" 79
10.1. The Conviction of Henry Okah 91
11.1. The Prosecution of the Thulsie Twins 91
12.1. Fraud Case Example 151
13.1. State v XYZ and Others 152
14.1. Bobroff Matter 153
15.1. Financial Supervisor Cooperation 157
16.1. John Gregory Stouch: Incoming Request 159

TABLES

1. Effectiveness Ratings 21
2. Technical Compliance Ratings 22
1.1. Sector Risk Ratings 28
1.2. Financial Institutions and VASPs (March 2019 unless stated otherwise) 36
1.3. Designated Non-Financial Businesses and Professions (March 2019) 38
1.4. Company Statistics Report (as at June 14, 2019) 41
1.5. Trusts Registered Annually with Master of High Court, 2012 – 2019 41
3.1. Requests Made to the FIC by South African LEAs 2014–2018 58
3.2. Proactive Disclosures made by the FIC to South African LEAs – Five Years to March 31, 2018 59
3.3. Section 205 Subpoenas Obtained by SAPS (2014–2018) 60
3.4. Section 29 Reports Received by FIC from AIs and RIs (Six Years to March 31, 2019) 60
3.5. Section 28 Reports Received by the FIC from AIs and RIs (2014 to 2019) 61
3.6. Intelligence Requests Made to the FIC by South African LEAs – Five Years to March 31, 2018 63
3.7. Section 35 Monitoring Orders: Terrorism & TF Investigative Inquiries—Six Years to March 31, 2019 64
3.8. Feedback on Requests: NPA:AFU Five Years – April 1, 2014 to March 31, 2019 64
3.9. SAPS:DPCI Predicate Offense Investigation Activity Resulting in ML Charge – Jan 1, 2014 to Dec 31, 2017 67
3.10. Number of ML Investigations, Prosecutions, and Convictions—Five Years to March 31, 2019 69
3.11. ML Convictions—Number of Natural People Convicted – Five Years ending March 31, 2019 73
3.12. Sanctions Imposed for Persons Convicted of ML Only – March 2014 – October 2019 75
3.13. NPA:AFU POCA Activity – Five Years ending March 31, 2019 80
3.14. NPA:AFU Activity Involving ML Related Cases—Five Years to March 31, 2019 80
3.15. Cases Involving Funds Repatriated—Five Years to March 31, 2019 81
3.16. SIU Recoveries through Civil Litigation—Six Years to March 31, 2019 82
3.17. SARS:Customs, Border Cash Seizures—Five Years to March 31, 2019 84
4.1. Source of Terrorism and TF Investigative Inquiries—Five Years to March 31, 2018 92
4.2. Requests to FIC for Terrorism Related Intelligence—Six Years to March 31, 2019 93
4.3. Reasons for Closing National Security Inquiries—Five Years to March 31, 2019 93
4.4. Financial and Trade Flows with Iran and DPRK in the Four Years ending March 31, 2018 102
5.1. CMA: Total Inwards Transaction Values and Volumes in 2018 (excl. card transactions) 115
5.2. CMA: Total Outwards Transaction Values and Volumes in 2018 (excl. card transactions) 115
5.3. Number of STRs and Suspicious Activity Reports Filed per Type of AI: Five Years ending March 31, 2019 117
6.1. Supervisory Resourcing and Activities by Sector—Time Periods Vary 128
6.2. SARB:PA AML/CFT Inspections 2012 to 2019 (year ending Dec 31) 130
6.3. SARB:FinSurv ADLA AML/CFT Inspections- Five Years ending Dec 31 132

6.4. FSCA—Onsite Examinations that included Aspects of AML/CFT—Five Years ending Dec 31 _____ 133
6.5. FIC—Number of Onsite Examinations—Four Years ending March 31_____ 134
6.6. EAAB Inspections that Include AML/CFT Elements—Five Years ending March 31, 2019 ___ 134
6.7. Gambling—Number of AML/CFT Inspections that Covered AML/CFT—Five Years ending Dec 31_____ 135
6.8. Supervisory Inspections and Enforcement Actions by Sector—Periods Vary_____ 135
6.9. Monetary Penalties Imposed by the SARB:PA to Banks for AML/CFT Breaches _____ 137
8.1. Number of FIC Requests Sent to Other FIUs—Five Years ending March 31, 2018_____ 154
8.2. FIC Requests Received from Other FIUs Five Years ending March 31, 2018_____ 156
8.3. FIC Spontaneous Disclosures to Other FIUs—5 Years ending March 31, 2018 _____ 157
8.4. Foreign Information Requests Received by the SARB:PA—Five years to December 31, 2018 _____ 158

ANNEXES

I. Technical Compliance Annex_____ 161
II. Summary of Technical Compliance – Key Deficiencies_____ 243

Glossary

ACTT	Anti-Corruption Task Team
ADLA	Authorized Dealer with Limited Authority
AI	Accountable Institution in terms of the Financial Intelligence Centre Act, 2001
AML	Anti-Money Laundering
AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism
AML/CFT NRA WG	Inter-departmental National Risk Assessment Working Group
AUs	Authorized Users (of an exchange – i.e., securities companies)
BNI	Bearer negotiable instruments
BO	Beneficial Owner/ship
C	Criterion for technical compliance in the FATF Methodology
C&E Act	Customs and Excise Act, 1964
CARA	Criminal Assets Recovery Account
CDD	Customer due diligence
CEO	Chief executive officer
CFI	Cooperative Financial Institution
CFT	Combating the Financing of Terrorism
Ch	Chapter
CIPC	Companies and Intellectual Property Commission
CIS	Collective Investment Scheme
CMA	Common Monetary Area (or Rand Common Monetary Area)
CPA	Criminal Procedure Act, 1977
CSP	Company service provider
CTFC	Counter Terrorism Functional Committee
CTR	Cash Transaction Report
CTRA	Cash Threshold Aggregate Reports
DHA	Department of Home Affairs
DIRCO	Department of International Relations and Cooperation
DNFBP	Designated non-financial businesses and professions
DoJ&CD	Department of Justice and Constitutional Development
DPP	Director of Public Prosecutions
DPMS	Dealers in Precious Metals and Stones
DPSA	Department of Public Service and Administration
DSD	Department of Social Development
EAAB	Estate Agency Affairs Board
EFT	Electronic Funds Transfer
EFT Directive 1	EFT Directive 1 of 2015 for conduct in the national payment system in respect of the FATF Recommendations for EFTs

Egmont	Egmont Group of Financial Intelligence Units
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
ESW	Egmont Secure Web of the Egmont Group of FIUs
FAIS Act	Financial Advisory and Intermediary Services Act, 2002
FATF	Financial Action Task Force
FI	Financial institution
FIC	Financial Intelligence Centre
FIC Act	Financial Intelligence Centre Act, 2001
FinTech	Financial Technology
FIU	Financial intelligence unit
FSCA	Financial Sector Conduct Authority
FSP	Financial services provider
FSR Act	Financial Sector Regulation Act, 2017
FT	Financing of Terrorism
FTE	Full Time Equivalent (staff member)
G20	Group of Twenty Nations
GN	Guidance Note
goAML	IT system developed by UNODC for use by FIUs
IDC	Inter-Departmental Committee
IDWG-CT	Inter-Departmental Working Group on Counter Terrorism
IFFTT	Illicit Financial Flows Task Team
IFWG	Intergovernmental Fintech Working Group
ICCMA	International Cooperation in Criminal Matters Act, 1996
IMF	International Monetary Fund
IO	Immediate Outcome
Interpol	International Criminal Police Organization
ISOC	Ithala SOC Limited, a subsidiary of Ithala
Ithala	Ithala Development Finance Corporation Limited
JCPS	Justice, Crime Prevention and Security Cluster
JSE	Johannesburg Stock Exchange Limited
KYC	Know your customer
KRD	Krugerrand dealer
LEA	Law Enforcement Agency/(ies)
LPA	Legal Practice Act
LPC	Legal Practice Council
Master	Master of the High Court of the Department of Justice and Constitutional Development
ME	Mutual Evaluation
MER	Mutual Evaluation Report
ML	Money laundering

MLA	Mutual Legal Assistance
MOU	Memorandum of Understanding
MVD	Dealers in motor vehicles
MVTS	Money Value Transfer Services
NCOP	National Council of Provinces
NCTS	National Counter Terrorism Strategy
NGB	National Gambling Board
NICOC	National Intelligence Co-ordination Committee
NIE	National Intelligence Estimate
NPA	National Prosecuting Authority
NPA:AFU	Asset Forfeiture Unit of the NPA
NPA:ID	Investigative Directorate of the NPA
NPA:NPS	National Prosecuting Services of the NPA
NPA:PCLU	Priority Crimes Litigation Unit of the NPA
NPA:SCCU	Specialized Commercial Crime Unit of the NPA
NPA Act	National Prosecuting Authority Act, 1998
NPC	South Africa Council for the Non-Proliferation of Weapons of Mass Destruction
NPO	Non-profit organization
NPO Act	Non-profit Organizations Act, 1998
NPOTT	NPO Task Team
NPS	National Payment System
NPS Act	National Payment System Act, 1998
NRA	National Risk Assessment
NT	National Treasury Department
Palermo Convention	United Nations Convention Against Transnational Organized Crime, 2000
Para.	Paragraph
PCC	Public Compliance Communication
PEP	Politically exposed person
PGI	Prosecutor Guided Investigations
PIC	Public Investment Corporation
PLA	Provincial Licensing Authorities
POCA	Prevention of Organized Crime Act, 1998
POCDATARA	Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004
POPI Act	Protection of Personal Information Act, 2012
Postbank	Post Office Bank
R	South African Rand
R.	FATF Recommendation

RBA	Risk-Based Approach
RMCP	Risk Management and Compliance Program
Reg.	Regulation
RI	Reporting Institution in terms of FIC Act s.29
s.	Section
ss.	Sections
SADC	Southern African Development Community
SAPO	South African Post Office
SAPS	South African Police Service
SAPS:DPCI	SAPS Directorate of Priority Crimes Investigations
SAPS:DPCI – FAFI	SAPS DPCI – Financial and Asset Forfeiture Investigation
SAPS:DPCI – CATS	SAPS DPCI – Crimes Against the State unit
SAPS:DPCI – PCMC	SAPS DPCI Priority Crime Management Centre
SAPS:DPCI – PCSI	SAPS DPCI Priority Crime Specialized Investigation Unit
SARB	South African Reserve Bank
SARB:FinSurv	Financial Surveillance Department of the SARB
SARB:NPSD	National Payments Systems Department of the SARB
SARB:PA	Prudential Authority of the SARB
SARPCCO	Southern African Region Police Chiefs Cooperation Organization
SARS	South African Revenue Service
SARS:Customs	SARS Customs and Excise Division
Sch	Schedule
SFTP	Secure File Transfer Protocol
SIU	Special Investigating Unit
SOE	State-owned Enterprise
SRA	Sector risk assessment
SRB	Self-regulatory body
SSA	State Security Agency (previously National Intelligence Agency (NIA))
STR	Suspicious transaction report
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TF Convention	International Convention for the Suppression of the Financing of Terrorism, 1999
TFS	Targeted Financial Sanctions of the United Nations Security Council
TOR	Terms of Reference
TPC Act	Trust Property Control Act, 1988
TSP	Trust Service Provider
UN	United Nations
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolution
USD	United States dollar

VA	Virtual Asset
VASP	Virtual Asset Service Provider (known as Crypto Asset Service Provide (CASP) in South Africa)
Vienna Convention	United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988
ZAR	South African Rand

EXECUTIVE SUMMARY

This report summarizes the AML/CFT measures in place in the Republic of South Africa (South Africa) as at the date of the onsite visit (October 22 to November 12, 2019). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of South Africa's AML/CFT system and provides recommendations on how the system could be strengthened.

KEY FINDINGS

1. The main domestic money laundering (ML) crime threats are consistently understood by the key authorities but the understanding of their relative scale, ML vulnerabilities, and the threats from foreign predicates is limited. Understanding of terrorist financing (TF) risks is underdeveloped and uneven. Some ML risks are being mitigated but some significant risks remain to be addressed. TF risks are not being adequately addressed.

2. South Africa has suffered from a sustained period of "*State capture*",[1] which helped to generate substantial corruption proceeds and undermined key agencies with roles to combat such activity. Government initiatives from 2018/19 were starting to address the situation as of the onsite, including by replacing key staff and increasing resources at key law enforcement and judicial agencies.

3. The Financial Intelligence Centre (FIC) effectively produces operational financial intelligence that Law Enforcement Agencies (LEAs) use to help investigate predicate crimes and trace criminal assets, but the LEAs lack the skills and resources to proactively investigate ML or TF.

4. A reasonable number of ML convictions is being achieved but only partly consistent with South Africa's risk profile. Cases largely concern self-laundering and few cases of third-party ML and foreign predicate offenses are prosecuted. The proactive identification and investigation of ML networks and professional enablers is not really occurring. Most ML convictions relate to fraud cases and there are fewer investigations and successful prosecutions relating to other high-risk crimes. In particular, ML cases relating to "State capture" have not been sufficiently pursued.

5. South Africa has achieved some good results proactively pursuing confiscation of criminal proceeds, particularly using civil forfeiture powers but has had less success recovering assets from "*State capture*" and proceeds which have been moved to other countries. Some recent cases suggest that this situation is improving.

6. Use of cash is prevalent in South Africa and it has been assessed as high risk for ML and TF, including cross-border movement. Detecting and recovering cash proceeds of crime

[1] See below for more about the phenomenon described as "State capture".

remains challenging and efforts to detect and confiscate falsely or undeclared cross-border movement of currency needs substantial improvement.

7. South Africa has convicted one person for TF since the last ME and was prosecuting one case as of the onsite which is inconsistent with its significant TF risks. A conservative approach to classifying politically motivated acts of violence as terrorism negatively impacts the investigation and prosecution of potential terrorist financiers. Targeted Financial Sanctions (TFS) are not used to any great extent to fight terrorism; and implementation of United Nations Security Council Resolutions (UNSCRs) for TF has not occurred since 2017.

8. Law enforcement faces challenges to readily obtain accurate and updated beneficial ownership (BO) information about companies and trusts adequate to enable effective investigation of ML and TF.

9. Larger banks are more developed at understanding their ML risks and implementing mitigating measures commensurate with those risks. Most smaller Financial Institutions (FIs) and Designated Non-Financial Businesses and Professions (DNFBPs) are focused on compliance, not on identifying and understanding risks. TF risk is understood by the private sector to some extent. Overall, the risk-based approach (RBA) is inadequately implemented. Basic customer due diligence (CDD) is applied by many accountable institutions (AIs) satisfactorily but BO requirements only to some extent. Larger banks and Authorized Dealers with Limited Authority (ADLAs) meet suspicious reporting obligations to a large extent, but some high-risk sectors rarely report. The potentially high-risk sectors of Dealers in Precious Metals and Stone (DPMS) and Company Service Providers (CSPs) are not AML/CFT regulated, save for a general reporting obligation, as is also the case for Virtual Asset Service Providers (VASPs).

10. Risk-based AML/CFT regulation and supervision is relatively new. Most supervisory activities occur for banks and ADLAs but none of the supervision of FIs or DNFBPs uses a proper RBA. Inspections in other sectors are too infrequent and focus on the presence of basic controls not the soundness of AML/CFT programs. The FIC is a key coordinator amongst supervisors and provides a wide range of well-regarded guidance. Market entry controls to screen out criminality need fundamental improvements.

11. South Africa provides constructive mutual legal assistance (MLA) which has helped to resolve some criminal cases in other countries, but it is sometimes slow. Seeking international cooperation in investigations is not a priority, inconsistent with South Africa's risk profile, and following up on requests made needs major improvement.

12. Since April 2019, South Africa has implemented TFS for proliferation financing (PF) fairly well, most of the time without delay, but some major improvements are needed, as the private sector's understanding is uneven, and supervision of PF-related obligations is new.

Risks and General Situation

13. South Africa has a relatively high volume and intensity of crime and more than half of reported crimes fall into categories that generate proceeds. The main domestic proceeds-generating predicate crimes are tax crimes, corruption and bribery, fraud, then trafficking in illicit drugs, and environmental type crimes. As a large economy and a regional financial hub for sub-Saharan Africa, South Africa has a notable exposure to the threat of foreign proceeds of crime generated in the region being laundered in or through the country. South Africa is exposed to TF risks associated with the financing of foreign terrorism, foreign terrorist fighters (FTFs), and potential domestic terrorism.

14. There is widespread use of cash and a large informal economy including informal cross-border remittances in the region which often involve physical cash movement. Banks offer a diverse suite of products and services and act as the main entry point of the financial system including from abroad. Insufficient BO transparency is an acute vulnerability as companies and trusts are often misused for ML or to carry out predicate crimes, making attorneys and trust and company service providers inherently vulnerable to misuse. Estate agents are also exposed with many known ML cases involving real estate. Public sector corruption represents a major weakness in the AML/CFT system, with the key LEAs being the most impacted over the past decade. The RBA and many key preventive requirements were introduced in the legal framework only recently.

Overall Level of Compliance and Effectiveness

Assessment of Risk, Coordination and Policy Setting (Chapter 2; IO.1, R.1, 2, 33 & 34)

15. Corruption, tax related crimes and fraud are understood as the main domestic ML threats by the key AML/CFT authorities consistently, but their understanding of the relative scale of such threats as well as the vulnerabilities or channels exploited to launder the proceeds is less developed. The threats arising from proceeds of foreign predicates is understood only to a very limited extent. The authorities' understanding of TF threats is underdeveloped and uneven with the supervisors being the most unsensitized. The authorities identify TF risks as mainly stemming from international terrorism but lack due appreciation of those from domestic terrorism. They note some high-level vulnerabilities that could be exploited for TF but are unable to determine if, or to what extent, such vulnerabilities are being exploited. South Africa has yet to conclude its first national ML and TF risk assessments (NRAs). A summary of preliminary findings of the ML NRA has been shared with some private sector representatives while those of the TF NRA have not.

16. South Africa has yet to develop coordinated and holistic national AML/CFT policies informed by ML/TF risks, though some existing policies or measures mitigate some aspects of the risks identified. However, significant ML risks remain largely unaddressed for beneficial owners of legal persons and trusts, cross-border movement of cash, and criminal justice efforts are not yet directed towards effectively combating higher risks such as ML related to corruption, narcotics, and tax offenses. The authorities were challenged to show how TF risks are proactively addressed, and TF is not properly integrated into the National Counter Terrorism Strategy (NCTS). Some financial

sectors,[2] DNFBPs,[3] and VASPs are yet to be subject to most AML/CFT obligations and their exclusion is not justified based on risk.

17. The extent to which competent authorities' priorities and objectives are aligned with national ML/TF risks and policies is uneven. Some ML cases have been identified but overall, the National Prosecution Authority (NPA) and LEAs have been focused mainly on predicate offenses rather than ML. Furthermore, complex and higher risk ML activities are not targeted partly owning to some key performance indicators that might divert effort away from such cases. LEAs' activities are aligned with the TF risk only to the extent such risks are recognized. While some supervisors have addressed certain - in some cases isolated - aspects of ML risk, the extent to which they have targeted TF risks has been very limited owing to their lack of understanding of such risks.

18. The authorities cooperate and coordinate on AML/CFT to some extent on policy and better on operational matters. An Inter-Departmental Committee (IDC) on AML/CFT, which includes most stakeholders, was established in 2017 to understand and mitigate ML/TF risks. It plays a central role in coordinating the ML NRA and TF NRA but is yet to generate any strategic AML/CFT policy initiatives. So far, its agenda has been driven mainly by financial regulatory issues with little focus on law enforcement and judicial matters, which fall under the Justice, Crime Prevention and Security (JCPS) Cluster. AML/CFT cooperation and coordination at the operational level works well in general, though some stakeholders are not involved in certain aspects of the operations and the often-formal nature sometimes prolongs the process. The level of coordination among authorities on PF remains at its initial stages.

Financial Intelligence, ML Investigations, Prosecutions and Confiscation (Chapter 3; IO.6, 7, 8; R.1, 3, 4, 29–32)

19. The use of financial intelligence plays an important part in addressing predicate crimes, ML, TF, and the identification of criminal assets. The FIC obtains a large number of obligatory reports and possesses tools and has access to additional information that allows it to analyze such reports and effectively produce operational financial intelligence. Given however, the identified risk pertaining to cash, particularly cross border cash transactions, the fact that the FIC is not routinely receiving reports on cash courier activity, as well as the low volume of reporting from high risk DNFBPs, significant gaps in financial intelligence exist.

20. The South African Police Service (SAPS), the South African Revenue Service (SARS) and other authorities routinely use financial intelligence to mainly support their investigations and activities related to predicate crimes, and not on proactively identifying and supporting ML and TF cases. LEAs require additional skills and resources to more effectively use the information

[2] These include CFIs, FinTech companies offering financial services that are not VASPs or licensed as financial service providers (FSPs), and credit providers other than money lenders against securities.

[3] These include: DPMS beyond KRDs as reporting institutions (RIs), accountants (for activities other than providing financial services), and CSPs other than attorneys.

that is generated to conduct their financial investigations. For example, the SAPS:DCPI only had around 2,000 out of 5,000 positions in its special investigative units occupied as of the on-site.

21. The authorities identify and investigate ML cases to some extent. Emphasis is placed on investigating predicate offenses. Parallel financial investigations (PFIs) are undertaken in all cases of organized crime, serious commercial crime, and serious corruption. However, the authorities have not sufficiently demonstrated the proactive identification and investigation of ML cases as a primary objective. Investigation and prosecution of ML activity is partly consistent with South Africa's threat and risk profile. ML cases relating to fraud form the bulk of cases investigated and prosecuted. There are fewer ML prosecutions relating to other high-risk areas such as serious corruption, narcotics, and tax offenses. ML cases relating to *"State capture"* have not been sufficiently pursued in the past, and cases referred to the NPA by the Special Investigating Unit (SIU) have not been dealt with expeditiously. The NPA has suffered from major resource and staffing constraints, which is now being addressed by the establishment of the Investigative Directorate (NPA:ID) and an increased budget allocation for hiring of prosecutors. Nevertheless, a reasonable number of convictions is being achieved, albeit the cases largely concern self-laundering. Standalone ML cases are prosecuted, but few cases of third-party ML and foreign predicate offenses are prosecuted, the latter being a concern in the context of South Africa's role as a regional financial hub. Overall, this appears to be a consequence of the focus on the investigation of predicate offenses rather than the proactive identification and investigation of wider ML networks and professional enablers. Sanctions applied against natural persons convicted of ML offenses are to some extent effective, proportionate, and dissuasive. However, the majority of sentences imposed by the courts involve non-custodial or suspended sentences for the ML offense.

22. South Africa proactively pursues confiscation of criminal proceeds as a policy objective and some good results have been achieved. The NPA's Asset Forfeiture Unit (NPA:AFU) places emphasis on its civil forfeiture powers under the Prevention of Organized Crime Act (POCA) which targets tainted property. Less emphasis is placed on criminal confiscation of property of equivalent value, which is dependent upon a conviction for the ML or predicate offense. Whilst the authorities have demonstrated positive results for recovery of proceeds of crime in the area of fraud and economic crime including ML, efforts for recovery of assets from *"State capture"* and proceeds which have been moved to other countries have been less successful to date due to the phenomenon of *"State capture"* itself and resource constraints. Recent efforts by the authorities are beginning to show positive results in some major cases, but these efforts are still at the early stage. In addition, recovering the proceeds of criminal offenses occurring outside South Africa are not being sufficiently targeted taking account of South Africa's role as a regional financial hub. South Africa has not positively demonstrated that confiscation of falsely declared or undeclared cross-border movement of currency is being addressed and applied as an effective, proportionate, and dissuasive sanction. Use of cash is prevalent in South Africa and it has been assessed as high risk from a ML and TF perspective, including cross-border movement. Overall, confiscation of proceeds of crime partially reflects South Africa's ML/TF risk and national AML/CFT policies and priority.

Terrorist and Proliferation Financing (Chapter 4; IO.9, 10, 11; R.1, 4, 5–8, 30, 31 & 39.)

23. The pursuit of TF in South Africa is done in a coordinated way through the use of the Counter Terrorism Functional Committee (CTFC) which includes all the relevant security cluster government stakeholders.[4] However, pursuing TF investigations is not very well integrated with strategies to combat terrorism in South Africa and authorities are failing to produce results reflective of the country's identified TF risk. The low level of viable investigations and prosecutions into TF in South Africa is not consistent with the countries recognized TF risk profile as a country with FTFs and which is being used by terrorist groups as a transit point and a base for planning and logistics.

24. South Africa has failed to demonstrate that it is effectively identifying, investigating, or prosecuting terrorist financiers or addressing TF through alternative measures.

25. South Africa's implementation of TFS against TF is not effective and suffers from deficiencies that are inherent to the applicable framework. Terrorists are identified and deprived of their resources and means to finance or support their activities only to a negligible extent considering the TF risk and activities under monitoring in the country. The measures implemented for TFS and to combat abuse of non-profit organizations (NPOs) are not in line with South Africa's TF risk profile.

26. Authorities responsible for combating TF do not consider administrative TFS designations as a relevant tool to manage the TF risk in practice. While designation is not conditional upon the existence of a criminal investigation, they favor an approach that requires obtaining compelling evidence and testing that in court through a criminal proceeding before they would consider making a designation under UNSCR regimes for TFS. Authorities have used alternative processes to deprive terrorist of their assets only to a limited extent relative to South Africa's TF risk.

27. South Africa, through the formation of an NPO Task Team (NPOTT), has begun the process of identifying NPOs that, based on their characteristics and activities, are at risk of TF abuse. The authorities, however, have not applied specific measures, nor commenced monitoring or supervision, of those organizations they deemed to be at risk of TF abuse.

28. Since April 2019, South Africa has implemented TFS for PF fairly well, but some major improvements are needed. Implementation without delay occurs most of the time for existing UNSCRs but is unlikely to be without delay for new UNSCRs.

29. Early detection of PF activities is to some extent ongoing, relying mostly on STRs and foreign intelligence. The authorities' ability to proactively identify and detect PF-related assets is challenged by limited access to BO information.

[4] The committee comprises representatives from the State Security Agency (SSA - chair), the SAPS:DPCI – CATS, the SAPS:Criminal Intelligence Division, the NPA:PCLU, Defense Intelligence, the DHA, the Department of International Relations and Cooperation (DIRCO), and the FIC.

30. Despite positive and repeated outreach efforts by the FIC, the level of understanding in the private sector remains uneven, with only larger FIs with international exposure having a more developed understanding and a likely appropriate level of compliance. Supervision and compliance monitoring of PF-related obligations is still at an early stage.

Preventive Measures (Chapter 5; IO.4; R.9–23)

31. The larger banks (collectively, materially important) show a developed understanding of ML risks and seem better at implementing mitigating measures commensurate with their risks. Most smaller FIs, including the materially important financial services providers (FSPs) and collective investment scheme (CIS) managers, show a basic understanding of ML risk, and are predominantly rule-based compliance and not risk focused when implementing such measures. Overall, DNFBP's understanding of ML risks and AML/CFT obligations is underdeveloped and mitigating measures are not risk-based, with casinos as a positive outlier. The high-risk estate agents and attorneys have a poor understanding of risks and obligations. AIs understand and mitigate TF risk commensurate with their risks to some extent.

32. Overall, preventive measures are applied by the larger banks in a risk-based manner to some extent, but the majority of other AIs (including FSPs and CIS managers, attorneys and estate agents) do not, as they fail to adequately assess their ML/TF risks.

33. In general, many AIs apply basic CDD measures satisfactorily, but all only apply BO requirements to some extent. Only the larger banks seem to apply a broader range of CDD measures that could be regarded as somewhat sufficient, including risk based ongoing due diligence, and specific measures towards correspondent banking relationships (CBRs), new technologies, wire transfers, and high-risk jurisdictions. However, politically exposed persons (PEPs) are in general, insufficiently identified partially due to the deficient legal definition, but where PEP-status is determined AIs seem to take enhanced measures. AIs play down the risks of operating internationally and larger banks' group controls may not be adequately applied in their foreign entities in all instances.

34. Only the larger banks and ADLAs are reporting sufficient STRs and Suspicious Activity Reports. Other high-risk or materially important sectors underreport substantially, with the casino sector as a positive outlier. The larger banks file the best quality reports and the worst are filed by attorneys and estate agents. Banks could further improve their reporting by providing better information to link both ends of reported transactions.

35. The FIC Act was significantly amended in 2017 (enforced since April 2019) to provide for: a risk-based approach to CDD; institutional (or, business) risk assessments; and to put in place a full range of CDD measures. Several exemptions to the preventive measures regime were removed, but as mentioned above some sectors are still out of scope. South Africa has specifically applied reporting obligations on dealers in motor vehicles (MVDs) and Krugerrand dealers (KRDs), while CSPs, other DPMS and VASPs – as any business in South Africa – are subject to a general reporting

requirement but are not classified as AIs under the FIC Act nor required to be registered with the FIC.

Supervision (Chapter 6; IO.3; R.14, R.26–28, 34, 35)

36. While fit and proper criteria are in place for many sectors, these often do not apply to beneficial owners. Even though there was an isolated case where a bank application was rejected due to BO issues, the authorities could not demonstrate that they implement adequate controls to prevent criminality from infiltrating FIs and DNFBPs. Most regulators rely to a large extent on self-disclosure, and there is little verification done by competent authorities on criminal record checks. Unlicensed cross-border MVTS are not being systematically identified, sanctioned, or removed from the market.

37. As of the onsite, interim sector risk assessments (SRAs) were completed for most sectors covered in the South African regime. Supervisors demonstrated varied levels of understanding of ML risks for their respective sectors with the South African Reserve Bank's (SARB) Prudential Authority (SARB:PA) having a relatively good understanding with respect to banks at the sector level, while risks in the potential high-risk DNFBP sectors (estate agents, attorneys and trust service providers (TSPs)) are understood by their supervisor to a limited or negligible extent. The Financial Sector Conduct Authority's (FSCA's) and the Financial Surveillance Department's (SARB:FinSurv's) risk understanding is less developed. Banks and ADLA are the only AIs rated for ML/TF risks at the institutional level but with limited consideration of their inherent risks. All supervisors understand AML/CFT controls better than inherent and residual ML/TF risks and their TF risk understanding is very limited.

38. All supervisors in South Africa need major or fundamental improvements to conduct AML/CFT risk-based supervision effectively. The SARB:PA's supervision of the materially important banking sector checks compliance with AML/CFT requirements thoroughly but not yet using a proper RBA. The SARB:FinSurv's inspections adequately cover ADLAs but are based on risks only to a limited extent. For all other supervisors, inspections are too infrequent to be effective, and attorneys are subject to essentially no AML/CFT oversight. Except for those conducted by the SARB:PA, all inspections conducted are primarily focused on existence of basic AML/CFT controls rather than soundness of the AML/CFT program. The effectiveness of supervision by the FSCA and the Estate Agency Affairs Board (EAAB - for estate agents) is hampered by a severe lack of resources. The SARB:PA and the FSCA coordinate or share information with each other on AML/CFT but not yet on supervision of FIs that belong to the same group nor do they coordinate their inspections.

39. The SARB:PA has applied a range of remedial actions and sanctions against banks for AML/CFT breaches, but the sanctions are not always proportionate or dissuasive. Most other supervisors, except those for attorneys and casinos, apply remedial actions, but the sanctions imposed are often too low and infrequent to be dissuasive or effective. Financial supervisors demonstrated some impact in improving FIs' compliance with basic obligations. Enforcement of the amended FIC Act only started in April 2019 and supervisory impact that improves compliance with the new risk-based obligations was not demonstrated.

40. The FIC provides a wide range of AML/CFT guidance and conducts outreach nationally, supplemented by other supervisors, to promote a consistent understanding of AML/CFT obligations in the FIC Act. However, only limited information has been provided to help the private sector identify and understand ML/TF risks due in part to a lack of a completed NRA.

Transparency and Beneficial Ownership (Chapter 7; IO.5; R.24, 25)

41. Different types of legal persons can be created in South Africa, whilst creation of trusts mostly relate to inter-vivos and testamentary trusts. Information on the creation of the different types of legal persons and trusts is publicly available. The majority of LEAs have a general understanding of the exposure of legal persons and arrangements to possible ML misuse. However, the understanding is not extended to identification and assessment of the specific ML/TF vulnerabilities that lead to such exposure. The legal framework prevents legal persons and arrangements from being misused for ML/TF to a limited extent only. Where there are measures, they are at different levels of implementation. Legal persons and arrangements remain vulnerable as they are frequently cited in ML schemes, but limited information is known on misuse for TF. Some basic information on companies and trusts can be obtained as it is publicly available. However, there is a challenge with the turnaround time for information about most companies registered before 2016 as the information has not been uploaded to the public system. It should be noted that the Master's Office maintains a register of trusts containing basic information that is publicly available which is a positive feature of the regime. Obtaining of adequate, accurate and current BO information compared to basic, also varies but in the majority of cases it is not easily available and when available, it often takes a long time to obtain. The authorities could not demonstrate that they apply sanctions for failure to comply with information requirements.

International Cooperation (Chapter 8; IO.2; R.36–40)

42. South Africa provides constructive MLA and extradition in response to international requests. The assistance has resulted in resolution of some criminal cases in other jurisdictions but is sometimes slow; turnaround time averages over one year. There is an absence of an effective case management system and overall responsibility for the timely execution of the requests. Outgoing requests for MLA have only been made in a limited number of instances, which is inconsistent with South Africa's risk profile and the authorities have not adequately demonstrated that seeking international cooperation in the investigation of ML, associated predicate offenses, and TF is a priority. They need to use MLA more, especially for recovery of the proceeds of crime from "State capture" which have been moved abroad. While the authorities have recently increased the volume of ML/TF MLA requests that they make, those requests often suffer from delays in getting responses, and follow-up on outgoing requests needs major improvement. The competent authorities exchange information informally with foreign counterparts more in keeping with South Africa's risk profile. South African authorities can share some basic information on companies and trusts in a timely way because it is publicly available, but they have a limited ability to share BO information in a timely manner because this information is not readily available (see section on Legal Persons and Arrangements).

Priority Actions

- Develop policies to address higher ML/TF risks for: (i) BO; (ii) use of cash and its cross-border movement (physically and through illegal MVTS); (iii) third-party ML; (iv) foreign predicate crimes; (v) and TF. Ensure that all FIs, DNFBPs and VASPs are subject to AML/CFT obligations unless they pose proven low risks.

- Analyze how to substantially improve the availability of information on domestic PEPs and then support AIs to identify such PEPs. Remove the time limit in the definition of PEP in the FIC Act.

- Provide the SAPS Directorate for Priority Crimes Investigations (SAPS:DPCI) with more staff, especially financial investigators and forensic accountants, so that it can better use financial intelligence and place more emphasis on proactively identifying and investigating ML cases, particularly high level and complex cases such as those related to *"State capture"* and others involving third party laundering, foreign predicates, ML networks, and professional enablers.

- Keep prioritizing efforts to stem the flow of and recover assets from "*State capture*", including assets transferred to countries outside of South Africa, until satisfactory results are achieved.

- Actively seek formal and timely MLA for ML, associated predicate offenses and TF that have transnational aspects and follow-up on such requests, including proactively pursuing *"State capture"* requests through all available channels.

- Make major enhancements to the effectiveness of measures at borders to detect and seize illicit cash flows and to identify and address unlicensed cross-border MVTS.

- Greatly improve ability to proactively identify TF activity and reconsider the policy of not pursuing the domestic designations as a tool to counter terrorism or TF.

- Revise the TFS legal framework to address the major shortcomings identified in R.6 and create robust procedures for implementing UN listings without delay.

- Establish much better mechanisms to collect BO information about companies and trusts, and train relevant LEAs about complex structures and how they can be abused for ML/TF purposes.

- South Africa should ensure that AIs adequately implement an RBA, including through better assessing and understanding their inherent risks and refining and implementing their risk management and compliance programs (RMCPs) to mitigate their risks. The authorities should provide better guidance on these matters and on major ML/TF risks such as corruption.

- Supervisors should improve how they conduct risk-based AML/CFT supervision, including by improving their understanding of inherent ML/TF risks at sector and institutional levels and using that to prioritize their supervisory activities.

- Ensure the securities sector, attorneys, estate agents, TSPs, CSPs, and DPMS are supervised or monitored for AML/CFT commensurate with their risk profiles, by increasing supervisory resources and closing gaps in sector coverage.

Effectiveness & Technical Compliance Ratings

Table 1. South Africa: Effectiveness Ratings

IO.1 - Risk, policy, and co-ordination	IO.2 International cooperation	IO.3 - Supervision	IO.4 - Preventive measures	IO.5 - Legal persons and arrangements	IO.6 - Financial intelligence
Moderate	Moderate	Moderate	Moderate	Low	Moderate
IO.7 - ML investigation & prosecution	**IO.8 - Confiscation**	**IO.9 - TF investigation & prosecution**	**IO.10 - TF preventive measures & financial sanctions**	**IO.11 - PF financial sanctions**	
Moderate	Moderate	Low	Low	Moderate	

1: Effectiveness ratings can be either a High – HE, Substantial – SE, Moderate – ME, or Low – LE, level of effectiveness.

Table 2. South Africa: Technical Compliance Ratings

R.1 - assessing risk & applying risk-based approach	**R.2** - national cooperation and co-ordination	**R.3** - money laundering offence	**R.4** - confiscation & provisional measures	**R.5** - terrorist financing offence	**R.6** - targeted financial sanctions – terrorism & terrorist financing
PC	**PC**	**LC**	**LC**	**PC**	**NC**
R.7- targeted financial sanctions - proliferation	**R.8** -non-profit organizations	**R.9** – financial institution secrecy laws	**R.10** – Customer due diligence	**R.11** – Record keeping	**R.12** – Politically exposed persons
PC	**NC**	**LC**	**PC**	**LC**	**NC**
R.13 – Correspondent banking	**R.14** – Money or value transfer services	**R.15** –New technologies	**R.16** –Wire transfers	**R.17** – Reliance on third parties	**R.18** – Internal controls and foreign branches and subsidiaries
LC	**PC**	**NC**	**LC**	**NC**	**PC**
R.19 – Higher-risk countries	**R.20** – Reporting of suspicious transactions	**R.21** – Tipping-off and confidentiality	**R.22** - DNFBPs: Customer due diligence	**R.23** – DNFBPs: Other measures	**R.24** – Transparency & BO of legal persons
LC	**LC**	**C**	**PC**	**PC**	**PC**
R.25 - Transparency & BO of legal arrangements	**R.26** – Regulation and supervision of financial institutions	**R.27** – Powers of supervision	**R.28** – Regulation and supervision of DNFBPs	**R.29** – Financial intelligence units	**R.30** – Responsibilities of law enforcement and investigative authorities
PC	**PC**	**PC**	**PC**	**LC**	**C**
R.31 – Powers of law enforcement and investigative authorities	**R.32** – Cash couriers	**R.33** – Statistics	**R.34** – Guidance and feedback	**R.35** – Sanctions	**R.36** – International instruments
C	**PC**	**LC**	**LC**	**LC**	**LC**
R.37 – Mutual legal assistance	**R.38** – Mutual legal assistance: freezing and confiscation	**R.39** – Extradition	**R.40** – Other forms of international cooperation		
LC	**LC**	**LC**	**LC**		

1: Technical compliance ratings can be either a C – compliant, LC – largely compliant, PC – partially compliant or NC – noncompliant.

DETAILED ASSESSMENT REPORT

Preface

This report summarizes the AML/CFT measures in place as at the date of the onsite visit. It analyses South Africa's level of compliance with the FATF 40 Recommendations and the level of effectiveness of the AML/CFT system and recommends how the system could be strengthened.

This evaluation was based on the 2012 FATF Recommendations and was prepared using the 2013 Methodology. The evaluation was based on information provided by the country, and information obtained by the evaluation team during its onsite visit to the country from October 22 to November 12, 2019. The team visited Pretoria and Johannesburg during the onsite visit.

The evaluation was conducted by an assessment team consisting of:[5] Stephen Dawe, Senior Financial Sector Expert, IMF (team leader); Ke Chen, Financial Sector Expert, IMF (financial expert and deputy team leader); Pierre Bardin, Policy Analyst, FATF Secretariat (legal expert); Alastair Bland, Consultant (law enforcement and NPO expert); Alexandra Campbell, Consultant (financial expert); Joseph Jagada, Principal Expert, ESAAMLG (legal expert); Susan Mangori, Assistant Director of Public Prosecutions, Botswana (legal expert); Ruth McElwain, Advanced Associate, Financial Conduct Authority, UK, (financial expert); Marijn Ridderikhof, Consultant, (financial expert); and Wayne Walsh, Consultant (legal expert). The report was reviewed by Erik Blommé (Sweden), Iqtidar Hasanan (Malaysia), and Wonder Kapofu (Zimbabwe) as well as by the FATF and ESAAMLG Secretariats and IMF staff.

South Africa previously underwent a FATF Mutual Evaluation (ME) in 2009, conducted according to the 2004 FATF Methodology. That Evaluation concluded that the country was compliant with 9 Recommendations; largely compliant with 13; partially compliant with 19; and non-compliant with 7. South Africa was rated compliant or largely compliant with 12 of the 16 Core and Key Recommendations and was placed under the regular follow-up process. In June 2014, South Africa was placed in a targeted follow-up process for the former R.5 (CDD) and R.10 (record-keeping). It was removed from that process in November 2017. The 2009 MER has been published and is available at www.fatf-gafi.org/countries/#South%20Africa.

ML/TF RISKS AND CONTEXT

43. The Republic of South Africa (South Africa) was established in 1961. The country covers an area of approximately 1,219 million kilometers in the southernmost part of the African continent, and comprises nine provinces: Eastern Cape, Free State, Gauteng, KwaZulu-Natal, Limpopo, Mpumalanga, Northern Cape, North West, and Western Cape. Pretoria is the administrative capital, Cape Town the legislative capital, and Bloemfontein the judicial capital. Johannesburg is the largest city and main center for business; other major cities by population size

[5] In addition, Richard Walker (Guernsey) helped to internally review draft outputs of the assessors.

include Durban and Port Elizabeth. South Africa shares land borders which total 5,244 km with Botswana (1,840 km), the Kingdom of Eswatini[6] (430 km), Lesotho (909 km), Mozambique (491 km), Namibia (967 km), and Zimbabwe (225 km). It also has a coastline of 2,798 km. At the end of 2018, the population was approximately 58 million.

44. South Africa is an upper middle-income and G20 country. The currency is the South African Rand (ZAR or R).[7] In 2018, GDP grew by 0.8 percent and nominal GDP was approximately R4.9 trillion ($333 billion). South Africa is an extremely unequal society, average income is $6,354 and there is high poverty and unemployment. The country experienced strong growth between 2002 and 2011, but growth has been lackluster since. Over the five-year period from 2014 to 2018 real growth averaged 1.1 percent and unemployment averaged 26 percent.

45. South Africa is part of a Common Monetary Area (CMA), that recognizes the Rand as legal tender, along with Namibia, Lesotho, and the Kingdom of Eswatini.

46. The powers of the lawmakers (legislative authorities), governments (executive authorities) and courts (judicial authorities) are separate from one another. Parliament consists of the National Assembly and the National Council of Provinces and is the legislative authority of South Africa making laws for the country in accordance with its Constitution. The National Council of Provinces represents provincial interests and must have a mandate from the provinces before it can make certain decisions. The President is the Head of State and leads the Cabinet. He/she is elected by the National Assembly from among its members and leads the country. The Constitution determines the matters over which the provinces have concurrent or exclusive legislative authority. The national government is advised by, amongst others, Traditional Councils — traditional leaders whose status and roles of traditional leadership according to customary law are recognized, subject to the Constitution.

47. South Africa has an uncodified legal system, meaning that there is no single primary source where the law originates. The sources are the Constitution; legislation; case law (court decisions); common law; customary law; customary international law (unless it conflicts with the Constitution or acts of Parliament), old writers or authors; and indigenous law.

48. Previous judicial decisions are authoritative and therefore constitute legal precedent (case law) because the courts are bound to follow the approach taken in previous cases. When a specific matter is not governed by legislation, common law usually applies comparative foreign case law where there is no local jurisprudence on point. Common law forms the basis of modern South African law and has binding authority (e.g. the general principles of criminal law, law of contract and the law of damages, and the elements of specific offenses such as murder, fraud, robbery, and theft). Comparative foreign case law applies where there is no local jurisprudence on point.

[6] Known as Swaziland previously.

[7] As of the onsite, 1 R= 0.068 USD and 1 USD = R14.71. USD values in this report have been converted at these rates.

49. The Constitutional Court is the highest court in all constitutional matters and deals with constitutional issues (e.g. deciding whether Acts of Parliament and the conduct of the President and executive are consistent with the Constitution, including the Bill of Rights) and other matters of general public importance. The court's decisions are binding on all persons including organs of state, and on all other courts. The Supreme Court of Appeal is the highest court in respect of all other matters. Decisions of the Supreme Court of Appeal are binding on all courts of a lower order.

A. ML/TF Risks and Scoping of Higher Risk Issues

Overview of ML/TF Risks

ML/TF Threats

50. The main domestic proceeds-generating predicate crimes in South Africa are tax crimes, corruption and bribery, fraud, then trafficking in illicit drugs, and environmental and resource type crimes.[8] Tax crimes encompass evasion of a broad range of taxes and fees, including corporate and personal income and customs and excise taxes as well as tax fraud (e.g., VAT fraud). Incidents of corruption and bribery are widespread, across state-owned, provincial, and municipal entities, particularly irregularities in procurement involving the private sector.[9] Governance weaknesses, including in supply chain management, performance reporting and inadequate oversight coupled with a lack of consequences for transgressors increase the scope for bribery and corruption. Fraud includes ponzi, other investment, cyber-, and digital banking frauds as well as those involving virtual assets. South Africa serves as a market and a transit point for trafficking in illicit drugs[10] and the authorities report that clandestine drug production was increasing in 2017-2018 but declined during 2019.

51. South Africa's geographic and economic position potentially exposes it to the threat of foreign proceeds of crime from the region being laundered in or through South Africa, and of being used as a transit route for illicit goods and people smuggling. Foreign proceeds come predominantly from fraud, corruption and bribery, illicit drugs, and tax crimes. Many cases presented to the assessors suggest that the proceeds are often in the form of cash and are being laundered using cash, banks, and legal persons, as well as virtual assets (VAs) and MVTS to a lesser extent.

[8] Including: mainly illegal mining, then illegal abalone fishing, and to a lesser extent wildlife trafficking (although proceeds generated in South Africa from wildlife trafficking are modest compared to other crimes).

[9] South Africa scores 56.7 in the World Bank Control of Corruption Index; below the FATF average (76.7) albeit better than other ESAAMLG members (39.5). Auditor General and other reports show that millions of dollars are lost in procurement irregularities yearly. There are also widely quoted claims that around 20 percent of GDP is lost to corruption, but these are unsubstantiated. The NRA focuses on 20-25 percent of government procurement being lost annually; equivalent to about $6 billion.

[10] See "Hiding in plain sight" by Enhancing Africa's Response to Transnational Organized Crimes.

52. South Africa is potentially exposed to TF including, financing to facilitate foreign terrorism for groups such as ISIL, and the presence of facilitation networks and cells. South Africa has had known exposure to intending and returning FTFs. Most TF cases shared with the team have a transnational element. Funds for some attacks in Africa are suspected of originating from or transiting through South Africa.

ML/TF Vulnerabilities

53. South Africa has a relatively high volume of and intensity of crime and more than half of reported crimes fall into categories that generate proceeds. It is a large economy and a regional transport and financial hub for sub-Saharan Africa.

54. There is widespread use of cash and a large informal economy. Cash use is assessed as high risk in the NRA, and a large proportion (up to 70 percent) of cross-border remittances between South Africa and the SADC remittance market are informal.[11]

55. Public sector corruption,[12] represents a significant weakness in the AML/CFT framework. Insufficient resources dedicated to AML/CFT in some competent authorities relative to South Africa's size and risk profile also represent an AML/CFT vulnerability.

56. South Africa's location and the reach of its banking networks potentially exposes it to proceeds and TF funds flowing in and transiting through the country. There are long porous borders with relatively poor controls at the numerous land and sea entry points. In addition, South Africa's large migrant population from higher risk jurisdictions in Africa and South Asia, and resulting remittance flows, are potential vulnerabilities that likely elevate South Africa's TF risk.

[11] Preliminary findings of ML NRA, pp. 11

[12] Often referred to as "*State capture*" in South Africa. The term was first coined by the World Bank near the beginning of this century. The Bank writings focus on the actions of the private sector to purchase favorable policy, legislation and influence, as well as through corruption in public procurement.

In this DAR, "*State capture*" as a phenomenon and how it manifested in South Africa refers to a process through which public and private actors colluded to redirect rents away from their intended, rightful, recipients into private hands operating outside of the realm of public accountability. It is not simply equated to corruption, but corruption is an aspect. The impact and extent of *"State capture"*, whilst widely reported on in the media, are still being examined and probed. The cost to the South African economy is believed to be substantial. In 2018, the President created *the Judicial Commission of Inquiry to Inquire into the Allegation of State Capture, Corruption and Fraud in the Public Sector Including Organs of State*. It is chaired by Deputy Chief Justice, Raymond Zondo and commonly known as the Zondo Commission. The Commission was mandated to make findings and recommendations concerning attempts through any form of inducement to influence members of the government, including representatives of state-owned enterprises (SOEs). This influence included the appointment of cabinet members and political advisors, the awarding of government contracts and procurement tenders, and intervening in the matter of closing banking facilities for private sector entities with whom they had a relationship.

The economic impact of *"State capture"* in South Africa is discussed in the 2020 IMF Article IV consultation report, particularly, Annex VIII, see: www.imf.org/~/media/Files/Publications/CR/2020/English/1ZAFEA2020001.ashx

The word "corruption" in this report should be read to include *"State capture"* unless the context suggests otherwise.

57. DNFBPs such as attorneys, other TCSPs, estate agents, and DPMS, are inherently vulnerable to misuse. Insufficient corporate ownership transparency also represents an acute vulnerability in South Africa; companies and trusts are misused often for ML or to carry out predicate crimes and there is no comprehensive framework for accessing accurate and up-to-date BO information. The RBA has only recently been incorporated in AML/CFT legal framework, and many key preventive measures obligations are also relatively new.

Country's Risk Assessment & Scoping of Higher Risk Issues

Country's Risk Assessment

58. South Africa is in the process of concluding its first national assessment of ML risks (ML NRA). The approach taken is mainly qualitative rather than quantitative, relying primarily on experts' judgement to consider threats, vulnerabilities, and consequences. The information considered includes internal information from competent authorities (including basic AML/CFT statistics such as STRs, ML investigations, prosecutions, and convictions) and open source information such as reports of international and regional bodies, researches of think tanks, etc. Several SRAs were conducted prior to the onsite with inputs from the private sector fed into the ML NRA with respect to sector vulnerabilities.

59. The ML threats identified in the preliminary findings of the ML NRA as high-risk are corruption and bribery, tax related offenses, cybercrimes, fraud and drug trafficking, followed by human trafficking, smuggling of illicit goods, and wildlife trafficking, which are rated as medium-high. Corruption and bribery are seen as high severe risks due to their role as "enablers" of other predicate offenses and ML. "*State capture*" has undermined some key AML/CFT agencies over the past few years, in particular the SAPS:DPCI, the NPA and the SARS, which has had significant negative impacts on the country's economy and national security. Use of cash is also identified as a high risk.

60. The preliminary findings of the ML NRA acknowledge South Africa's role as a financial hub, and as a gateway for funds flowing from sub-Saharan countries to the rest of the world, including for potential foreign proceeds of crime. The NRA also identified challenges in implementing the legal and institutional framework, including coordination between the private sector and the public sector, provision of resources in some instances, obtaining and accessing ultimate beneficial ownership information and introduction of products and services offered through new technologies.

61. SRAs of the following sectors fed into the preliminary findings of ML NRA: banking, insurance, securities firms, FSPs and CIS managers, casinos, estate agents, MVDs, KRDs, TSPs and attorneys. An SRA of ADLAs - (or MVTSs, dealing with foreign exchange) and the insurance sector were completed around the time of the onsite and were yet to be incorporated into the ML NRA. No SRAs were conducted for DNFBP sectors not currently covered by the South African AML/CFT regime DPMS that are not KRDs and CSPs), nor were they assessed as part of the NRA. The sectors are rated in the preliminary findings as follows:

Table 1.1. South Africa: Sector Risk Ratings

Sector	Risk Rating
Gambling Institutions	High
Motor Vehicle Dealers (MVDs)	High
Krugerrand Dealers (KRDs)	High
Banks	Medium to High
Lenders of money against the security of securities	Medium
Authorized Users of a Securities Exchange	Medium
Investment Managers	Medium
Linked Investment Service Providers (LISP)	Medium
Estate Agents	Medium
TSPs	Medium
Attorneys	Medium
CIS managers	Low
Financial Advisers and Intermediaries	Low

Source: South African authorities

Note: SRAs of ADLAs and life insurers were completed shortly before the onsite and was yet to be incorporated. It concluded that ADLAs are of a very low to low risk while life insurers are of a medium risk.

62. South Africa was also in the process of assessing its TF risk exposure at the national level (TF NRA). The TF NRA also considers potential threats, vulnerabilities, and consequences primarily based on experts' views and information similar to that of ML NRA. The TF NRA preliminary findings note that, while South Africa has not been the target of domestic terrorism, there is a degree of risk from the threat of international terrorism. The authorities have identified limited activities of the Islamic State involving South African citizens and acknowledge potential sources of TF risks stemming from the country being used by terrorist groups including Al-Qaeda in the Islamic Maghreb to the north, Boko Haram to the north west and Al Shabaab to the north east, as a transit point and a base for planning and logistics. The preliminary findings also recognize the potential threat of returning FTFs from ISIS held areas in Syria, not just from South Africans but also people from other areas of the continent seeking to relocate to South Africa. Several vulnerabilities were identified in the national and regional control frameworks including lax border controls of travelers and cash and informal remittance systems including at the regional level. The preliminary findings of the TF NRA do not show any consideration of sector vulnerabilities, except noting that known cases suggest VAs being susceptible to TF abuse.

63. Assessors share many preliminary conclusions coming out of the ML and TF NRAs but have the following specific concerns: (i) the significance of proceeds from corruption may not be fully recognized; (ii) there is no reference to high end sophisticated ML in the preliminary findings of ML NRA; (iii); the preliminary ML risk ratings for some FIs and DNFBPs seem incomparable or

unreasonable across institutions (e.g., casinos are rated higher-risk than banks) or inconsistent with known ML cases (e.g., attorneys and estate agents considered as medium-risk despite being regularly associated with known ML cases); (iv) potentially high-risk sectors outside of the current AML/CFT regime (e.g., DPMS, CSPs) were not assessed; (v) the threats stemming from foreign predicates and associated vulnerabilities are not well reflected; (vi) the TF NRA likely under estimates TF risks associated with funding domestic terrorist activities, and (vii) the preliminary findings of the TF NRA lack specific conclusions on sector vulnerabilities. See section on National AML/CFT Policies and Coordination discussions.

Scoping of Higher-Risk Issues

64. Assessors explored whether the authorities have focused enough on risks beyond the financial sector, including for informality (for ML/TF), and abuse of real estate, companies, and gate-keepers such as attorneys (for ML) and the implications of South Africa's AML/CFT regime not covering dealers in the diamond and gold mining industries. The team also focused on the authorities understanding of TF risks as TF-related risk information could only be shared with the team during the onsite. The banking and MVTS sectors' understanding of their ML/TF risks, particularly for cash, cross-border, and PEP transactions was also a focus.

65. Assessors explored efforts to combat ML/TF in the informal sector and how ML/TF risks are managed in the context of financial inclusion initiatives. There was also an increased focus on customs and border controls due to cash smuggling being frequently linked to ML and TF.

66. Corruption (including *"State capture"*) was also examined. In this context, the assessors focused on how well the authorities combat the laundering of proceeds of corruption and the effectiveness of measures targeted at foreign and domestic PEPs.

67. The team focused on South Africa's role as a regional financial and economic hub and the ML/TF risks emanating from cross-border financial flows and smuggling and how well South Africa cooperates with foreign counterparts.

Areas of Lesser Risk and Attention

68. The assessment team devoted lesser attention to life insurance and financial advisors and intermediaries due to their relatively lower level of ML/TF risk.

B. Materiality

69. South Africa has a large and complex financial sector, and acts as a regional financial hub for sub-Saharan Africa. Non-bank financial institutions in the securities sector hold about sixty percent of financial assets (R11,400 billion or $775.2 billion). The banking sector, comprising 34 banks had around $385 billion in assets in the end of 2018. 2018 cross-border banking transactions equated to around $1 trillion (being $475 billion of outflows, $350 billion of inflows and $180 billion of correspondent flows). As of 2016, cross-border annual remittances amounted to around $1 billion

in each direction. South Africa is rich in precious metals and stones in particular gold and diamonds.[13] South Africa has the largest real estate market in sub-Saharan Africa, amounting to $50.2 billion in 2019.[14]

C. Structural Elements

70. South Africa has a stable political system and has demonstrated commitment to implementing AML/CFT systems, which has involved close cooperation and coordination between a variety of government departments and agencies. This framework has recently been strengthened by the creation of the IDC in November 2018 to coordinate on AML/CFT matters at the national level.[15]

D. Background and Other Contextual Factors

71. South Africa has recently enacted amendments to its AML/CFT coordination and institutional structures, and the system is a work in progress.

72. Since the last ME, South Africa has been exposed to a prolonged period of corruption (including *"State capture"*) which generated large amounts of corruption related proceeds as well as resulting in undermining of the integrity and capacity of some key AML/CFT agencies. Anti-corruption efforts remain extremely high on government's agenda.

73. Financial exclusion is also a key contextual factor that impacts the effectiveness of the regime, with a large portion of the population unbanked or with limited banking access, and a sizeable informal economy that uses cash as a payment medium.[16] The NRA indicates that, even when individuals are fully banked, they often withdraw all cash immediately after being paid in order to purchase goods and services in the informal marketplace. As a result, cash use remains prevalent. In 2016, 52 percent of the total value of all consumer transactions in South Africa were conducted in cash.[17]

AML/CFT strategy

[13] According to South Africa Minerals Council, the total diamond sales in 2018 was R17 billion ($1.2 billion). See: www.mineralscouncil.org.za/sa-mining/diamonds. Precious metals are of a similar size.

[14] See Real Estate Market Size 2019 by MSCI.

[15] Members are: the NT, (Chair and secretariat), the Department of Home Affairs (DHA), the DIRCO, the DoJ&CD, the Department of Social Development (DSD), the Department of Trade and Industry and Competition, the FIC, the FSCA, the National Intelligence Coordinating Committee (NICOC), the National Prosecuting Authority (NPA), the SAPS, the SARS, the SARB, and the State Security Agency (SSA).

[16] The World Bank Global Findex database suggests 67 percent of South Africans have an account at an FI, compared to 73 percent for upper middle-income countries. The "FinScope" survey, conducted by an independent NGO called Finmark Trust, uses a figure at 90 percent and estimates that up to 45 percent of South Africans use informal financial services.

[17] Consumer cost of cash in South Africa, Genesis, 2016.

74. South Africa does not have a formal AML/CFT strategy. In 2017 NT and the FIC jointly issued a consultation paper[18] that set some policy priorities. These included: a) strengthening AML/CFT through a more consultative approach based on partnerships between key stakeholders in the public and private sectors; b) improving co-ordination and collaboration to ensure more effective preventive measures and better enforcement measures; and c) a more customer-friendly and less-costly approach to implementation of AML/CFT. These high-level principles were to be supported by increased CDD obligations (including for domestic PEPs), increased BO transparency, introducing UNSCR asset freezing, and improved information sharing and enforcement by supervisory bodies.

Legal & Institutional Framework

Policy Co-ordination Bodies

75. The *Inter-Departmental Committee (IDC)* is the highest AML/CFT coordination body in South Africa. The National Treasury (NT) is the Chair and Secretariat, and membership includes most of the main AML/CFT government agencies.

Ministries

76. South Africa has a cluster system of government in which various ministries meet to coordinate issues under the leadership of the Presidency.

77. The Ministry of Finance and National Treasury (NT): The Finance Minister is responsible for AML policy measures and issues and CFT policy issues to the extent that CFT is covered in the FIC Act, supported by the financial intelligence unit (FIU), the FIC, which reports directly to the Minister, and the NT which is responsible for broader financial sector regulatory policy. The NT receives the FIC's annual performance plans and recommends the FIC's budget allocations. The Minister is also responsible for approving companies to act as ADLAs but has delegated this power to the SARB:FinSurv (see below).

78. The Minister of Police, who is responsible for the POCDATARA is responsible for CFT policy matters to the extent that they are covered in that Act.

79. The Department of Justice and Constitutional Development (DoJ&CD): is responsible for the NPA and is the central authority for administering all MLA and extradition matters.

80. The Department of International Relations and Cooperation (DIRCO): participates in the United Nations (UN) and other global fora, facilitates MLA, and international technical assistance. An Inter-Departmental Working Group on Counter Terrorism (IDWG-CT), under DIRCO's auspices, assists with South Africa's obligations regarding UN commitments.

[18] A New Approach to Combatting ML and TF

Criminal Justice and Operational Agencies

81. The Financial Intelligence Centre (FIC) is South Africa's FIU. It also supports and guides the activities of supervisors concerning compliance with AML/CFT measures, supervises some AIs and reporting institutions (RIs),[19] and assists the Minister of Finance with advice on AML/CFT policy matters.

82. The South African Police Service (SAPS) is responsible for investigating ML cases and offenses pertaining to terrorism. It houses the **Directorate for Priority Crimes Investigations (SAPS:DPCI)**, also known as the Hawks,[20] which has overall responsibility for the combating, investigation, and prevention of national priority crimes such as serious organized crime, serious commercial crime, serious corruption, and related ML. The DPCI has three specialized units focused on investigating different predicate crimes.[21] The **Priority Crime Management Centre (SAPS:DPCI – PCMC)** collects, monitors and analyzes information and intelligence on identified National Priority threats for the production of tactical and strategic analysis products, and research for threat assessments and forecasting. The **Priority Crime Specialized Investigation (SAPS:DPCI – PCSI)** unit provides professional and specialized support capability to three units that investigate predicate crime through specialized technology and assistance with cybercrime, ML, asset forfeiture, financial investigations as well as forensic investigation services. There is also a **Crimes Against the State (SAPS:DPCI – CATS)** unit in DPCI that focuses on terrorism and TF. SAPS:DPCI has a staff complement of approximately 2,500 members, although recent budget allocations by the NT have provided for a significant increase in staffing and resources going forward.

83. Special Investigating Unit (SIU) deals with fraud, corruption, and serious maladministration in state institutions. It conducts forensic investigations and institutes civil litigation to recover state assets or public money. It refers some cases to the SAPS for criminal investigation.

84. The National Prosecuting Authority (*NPA*) includes the **National Prosecuting Services (*NPA:NPS*)** which institutes criminal proceedings on behalf of the State. Other parts include:

- ***Specialized Commercial Crime Unit (NPA:SCCU)*** guides investigations into and prosecutes serious commercial and corruption cases, including ML,
- ***Organized Crime Component, Head Office, NPS*** manages, assists, and supports ML prosecutions in the regions on an ongoing basis. Staff in the regional Directors of Public Prosecutions (DPP) offices prosecutes ML cases arising from organized crime

[19] AIs are subject to a broad range of AML/CFT obligations; RIs are KRDs and MVDs which have an obligation to report suspicious or unusual activity under the FIC Act, s.29.

[20] Previously known as the Scorpions.

[21] The SAPS:DPCI has three specialized units: Organized Crime Investigations (narcotics, illicit mining, precious metals and diamonds, ferrous and non-ferrous metals, environmental crimes, firearms and specific violent crimes, human trafficking, crimes against the State, and transnational vehicle crime); Serious Commercial Office (banking crime, serious economic offenses, and serious fraud); and Serious Corruption Investigations (corruption in the public sector, private sector, and foreign bribery)

investigations.

- The ***Priority Crimes Litigation Unit (NPA:PCLU)*** manages and directs investigations into and prosecutes all offenses under the POCDATARA (including TF), non-proliferation offenses, as well as other serious crimes impacting on State security.

- ***Specialized Tax Unit*** guides investigations into and prosecutes tax cases, including ML.

- ***Asset Forfeiture Unit (NPA:AFU)*** implements the freezing and forfeiture provisions in respect of the proceeds and instrumentalities of crime, as well as freezing obligations created under UNSCRs 1267 and 1373.

- ***The Investigative Directorate (NPA:ID),*** was proclaimed by the President on April 4, 2019. It has special investigative powers to address serious and complex economic crimes with a focus on the crimes detected by the *Commissions of Inquiry into State Capture* (Zondo Commission), the Public Investment Corporation (PIC), and the SARS. The NPA:ID is also mandated to investigate and prosecute statutory offenses including contraventions of, inter alia, the POCA and the FIC Act.

85. **The *South African Revenue Service (SARS)*** is the tax and customs authority. Along with the SAPS and the **National Immigration Branch (NIB)** of the **Department of Home Affairs (DHA)**, the SARS is involved in controlling the movement of people and goods across the border. The SARS investigates tax offenses of which tax evasion is a predicate offense to ML, but not the related ML investigation which must be investigated by the SAPS.

86. ***State Security Agency (SSA)*** is responsible for the domestic and foreign intelligence and counter-intelligence security. It coordinates all counterterrorism and TF investigations in its capacity as the chair of the CTFC.

Financial Sector Competent Authorities

87. ***South African Reserve Bank (SARB)*** and the MoF form the monetary authority of South Africa. The SARB also formulates and implements monetary policy. The following units of SARB are relevant to AML/CFT:

- The ***Prudential Authority (SARB:PA)*** licenses and supervises banks and life insurers for compliance with the FIC Act.

- The ***Financial Surveillance Department (SARB:FinSurv)*** licenses and supervises ADLAs (including their branches) for compliance with the FIC Act.

- The ***National Payment System Department (SARB:NPSD)*** is responsible for supervising banks for compliance with rules for wire transfers. In practice, such

responsibilities have been delegated to the SARB:PA.

88. ***Financial Sector Conduct Authority (FSCA)*** is an independent regulator responsible for supervising the following for compliance with the FIC Act: financial advisors and intermediaries, securities investment managers, CISs, and the various exchanges.

DNFBP Competent Authorities and Self-Regulatory Bodies (SRBs)

89. **The *National Gambling Board (NGB)***, is responsible for the regulation of the gambling industry. It is the umbrella institution for nine Provincial Licensing Authorities (PLAs).

90. **The *PLAs*** in each of the nine provinces are responsible for issuing gambling licenses and regulating their casinos for compliance with licensing conditions as well as ensuring compliance with the FIC Act in their own provinces.

91. **The *Estate Agency Affairs Board (EAAB)*** (part of the Department of Trade and Industry and Competition) is the statutory regulator for estate agents and is responsible for monitoring their compliance with the FIC Act.

92. **The *Legal Practice Council (LPC)*** is a statutory body that regulates the affairs of and has jurisdiction over attorneys. It is the SRB that oversees compliance with the FIC Act.

93. **The *Independent Regulatory Board for Auditors*** is responsible for registering auditors in public practice and is the SRB that monitors their compliance with the FIC Act.

Legal Persons and Arrangements and Non-Profit Organizations Competent Authorities

94. **The *Companies and Intellectual Property Commission (CIPC)*** registers companies, close corporations, and co-operatives.

95. **The *Master of the High Court (Master)*** receives trust instruments before trustees assume control of the trust property, registers inter-vivos trust instruments, and approves the appointment of trustee(s) pursuant to the Trust Property Control Act (1988) (TPC Act).

96. **The *Department of Social Development (DSD)* administers** the Non-profit Organisations Act (1997) (NPO Act), which creates an administrative and regulatory framework for NPOs, including a voluntary registration facility for civil society organizations. The NPO Directorate is the dedicated unit within the DSD responsible for monitoring compliance.

Financial Sector, DNFBPs and VASPs

Financial Institutions

97. **Table 1.2 provides details of financial institutions operating in South Africa in March 2019.** The five financial groups shaped around ABSA Bank, FirstRand Bank, Nedbank, Standard Bank, and Investec Ltd dominate the banking sector and play an important part in non-banking sectors

through financial services, wealth management and insurance operations.[22] As at March 31, 2019, they held around 90 percent of total banking assets. Some template other medium large South African banks have a large reach across the population, one of them catering to in excess of 10 million retail customers in the nation.[23] The larger banks' FSPs and CIS managers arms control around 23 percent and 27 percent of the assets under management (AuM) held by the two sectors respectively. The large banks are complemented by medium-sized South African banks, branches of foreign banks and small banks. The banking sector offers a diverse suite of products and services and acts as a financial hub which provides access to the continent and further afield. In particular, the larger banks have a broad regional network in sub-Saharan Africa as well as in global financial centers. They also have CBRs worldwide. While banks (especially the large ones that are part of a financial group) act as the main entry point to the financial system including from abroad, FSPs and CIS managers outside the groups also provide customers with access to the securities market through authorized users (AU, i.e., securities companies). The securities sector is significant in terms of market capitalization (around 3.4 times of the banking assets) and AuM by FSPs, CIS managers and AUs amount to R9,100 billion ($618.8 million), R2,300 billion ($156.4 million), and R1,376 billion ($93.6 million) respectively. Assets held by life insurers represent seven percent (R2.8 trillion or $190.4 billion) of South Africa's financial assets.

98. Public FIs operating in South Africa, though not material in terms of size, are relevant due to their customer numbers and the access to financial infrastructure they provide. These include: Postbank, the banking division of the South African Post Office (SAPO), a state-owned enterprise (SOE) that serves people who previously had very limited access to the financial services; and the Ithala SOC Limited (ISOC), the banking and insurance subsidiary of Ithala Development Finance Corporation Limited (Ithala), owned by the province of KwaZulu-Natal, whose customers are mostly government employees of the province. Both entities operate under an exemption to provide banking services without a license. There are more than 200 entities known as "Financial Technology (FinTech) companies" that engage in a range of financial activities, but not all fall within the FATF definition of FIs. Some of them are licensed as FSPs and subject to AML/CFT obligations but many are not, including the VASPs, since how the legal and regulatory framework applies to them remains to be clarified.

[22] These are not designated as financial groups yet by South African regulators as a framework is still being developed.

[23] Local branches of international banks accounted for 5.6 percent of banking sector assets at the end of March 2019, while other banks represented 3.8 percent at the end of March 2019.

Table 1.2. South Africa: Financial Institutions and VASPs (March 2019 unless stated otherwise)

Type	No.[1]	No. licensed/ registered	Total Assets (R billion, end 2018)	Total Assets ($ billion, end 2018)	FATF Glossary Activities	Subject to AML/ CFT	AML/CFT supervisor
Banks	34	34	5,517.00	385.55	1-8, 10, 13	Y	SARB:PA
Mutual banks	4	4	3.13	0.22	1-6, 10, 13	Y	SARB:PA
Cooperative banks	4	4	0.19	0.01	1, 2, 5	N	NA
Credit Unions	26	26	0.23	0.02	1,2,5	N	NA
Stokvels (saving clubs)	810,000	NA	49.00	3.7	1, 2, 9, 10, 11	N	NA
ISOC	1	1	0.70	0.05	1-8, 10, 13	Y	FIC
Postbank	1	1	3.50	0.26	1, 3, 4, 5	Y	FIC
SAPO	1		6.12		4, 5	Y	SARB:FinSurv /FIC
Development Bank of South Africa	1	1	89.21	5.85	2, 6, 7(a), 7 (d)	Y	FSCA[2]/FIC
Land Bank South Africa	1	1	50.42	3.30	2, 6, 7(a), 7 (d)	Y	FSCA/FIC
ADLA	19	19	0.67	0.04	4, 5, 7 (b), 13	Y	SARB:FinSurv
Domestic MVTS	Unknown	NA	Unknown	Unknown	4	Y	FIC
AUs (securities companies)	151	151	NA	NA	7, 8	Y	FSCA
CIS managers (Mutual Funds, Unit Trusts)[3]	55	55	2,300.00	159.00	9, 10, 11	Y	FSCA
FSP Cat. I (Financial Advisors)	10,250	10,250	NA	NA	8, 11	Y	FSCA
Among which, Insurance Agents and Brokers	Unknown	Unknown	Unknown	Unknown	8	Y	FSCA

Table 1.2. South Africa: Financial Institutions and VASPs (March 2019 unless stated otherwise) (concluded)

FSP Cat. II (Discretionary Investment Managers)[3]	670	670	9,100.00	631.00	8, 9, 11	Y	FSCA
FSP Cat. IIA (Hedge Fund)[3]	127	127			8, 9, 11	Y	FSCA
FSP Cat. III (Administrative)	28	28	NA	NA	8, 11	Y	FSCA
FSP Cat. IV (assistance business)	111	111	NA	NA	8, 11	Y	FSCA
Ithala	1	1	0.71		2	Y	FIC
Life insurance companies	78	78	2 789.00	193.84	12	Y	SARB:PA
Credit providers[4]	6,895	6,895	Unknown	Unknown	2	N	NA
Among which, money lender against securities	Unknown[5]	NA	Unknown	Unknown	2	Y	FIC
FinTech companies[6]	Unknown	NA	Unknown	Unknown	1, 2, 4, 7(c), 11, 13	Partially	FSCA
VASPs	Unknown	NA	Unknown	Unknown	i, ii, iii	N	NA

Source: South African authorities
1: Does not include one bank that exited July 2019, three banks in the process of exiting the market and includes one mutual bank that had been granted license but was yet to commence business.
2: Only for its businesses as an FSP
3: The total assets represent assets under management (AuM).
4: Includes microfinance institutions, finance companies, and money lender against securities.
5: There are 76 registered with the FIC.
6: Advanced technology firms with potential to transform financial services. There are 217, but not all fall within the FATF definitions of FI or VASP. Some are licensed FSPs subject to AML/CFT obligations, but many are not since how the existing legal and regulatory framework applies to them remains to be clarified.

DNFBPs

99. All DNFBP sectors operate in South Africa. More than 40,000 estate agents provide domestic and overseas customers access to South Africa's real estate market. The legal practitioners include lawyers and notaries; referred to as attorneys in South Africa. They offer a wide range of services including financial services, conveyancing, and setting up and administration of trusts and corporates. TSPs can also help set up trusts. Other professions, including accountants and CSPs are also involved in provision of corporate services and not yet captured by the AML/CFT regime. DPMS

are not regulated or covered by the AML/CFT regime (except that KRDs) must register with the FIC and file suspicious reports) – but the number of active dealers is unknown. Eight casino groups are active in South Africa, operating 39 casinos nation-wide with a gross gambling revenue (GGR) of around R18.6 billion. ($1.3 billion) to a large extent earned through casino plays (60 percent versus other gambling modes) in the Gauteng (41 percent versus the share other provinces have in GGR per province), KwaZulu-Natal (18 percent) and Western Cape (17 percent). Additionally, South Africa also partially covers MVDs, which is beyond the requirements of the FATF Standards. The details of the DNFBPs that operate are set out in Table 1.3

Table 1.3. South Africa: Designated Non-Financial Businesses and Professions (March 2019)

Type	No.	No. licensed/ registered	FATF Glossary Activities	Subject to AML/CFT?	AML/CFT supervisor or SRO
Casinos	39	39	a)	Y	NGB/PLA
Estate Agents	44,874	44,874	b)	Y	EAAB
DPMS	Unknown	NA	c), d)	N	NA
Among which, KRDs	Unknown [1]	NA	c)	Partially	FIC
Attorneys (practicing only, including notaries)	19,119	19,119	e)	Y	LPC
Accountants	9,928	9,928	e)	Partially	FSCA
Auditors	4,152	4,152	e)	Partially	FSCA
TSPs	300[2]	NA	f)	Y	FIC
CSPs	Unknown	Unknown	f)	N	NA

Source: South African Authorities
1: 223 are registered with the FIC.
2: This is an estimate, there are 74 registered with the FIC.

Virtual Asset Service Providers (VASPs)[24]

100. The scale of VASP operations is not material. There are 12 crypto-asset trading platforms identified as at 2019. Crypto-asset trading volumes are about 1.4 percent of all trading on the Johannesburg Stock Exchange (JSE), while the trading volume of alternative exchanges was about 0.002 percent in 2018. The largest three platforms control around 80-90 percent of the market in South Africa, holding AuM of around R6.5 billion ($442 million, or around 0.05 percent of all AuM) and the largest platform (controlling around 65 percent of the market) trading for around R125 million ($8.5 million) per day. Most traders on domestic crypto-asset trading platforms are local citizens (about 86 percent in 2017). There are about approximately 800,000 South African citizens registered with the three largest exchanges. The number of foreign investors trading on domestic

[24] Known as Crypto Asset Service Providers (CASPs) in South Africa

platforms has increased from two percent of trades in 2017 to 14 percent in 2018. Four crypto-ATMs are present in South Africa but are rarely used. Bitcoin is the dominant (80 percent of the market) crypto-asset traded and stored on the three largest exchanges. There are also providers of payment services in VA.

101. When assessing the effectiveness of preventive measures and AML/CFT supervision, the assessment team assigned the highest importance to banks, followed by attorneys[25] and estate agents. ADLAs, FSPs category II (asset managers), CIS managers, casinos, TSPs, and VASPs were considered to be of a medium level of importance. Less importance was given to life insurers and FSP category I (financial advisors). Little to no weighting was given to sectors outside the scope of the FATF Standards, including MVDs.

Preventive Measures

102. South Africa's preventive measures regime flows from the FIC Act, which provides the legal basis for financial sector regulation and supervision and sets out the basic AML/CFT obligations of AIs and RIs. The FIC Act was significantly amended in 2017 which came into force in April 2019. The amended Act provides for, a RBA to CDD and a requirement for business risk assessments within the private sector. The amendments also put in place a full range of CDD measures including understanding and obtaining information about the client, ongoing due diligence, PEPs, beneficial ownership, and record keeping. Several previous exemptions from the preventive measures regime were removed, though, as discussed in para. 133. some FIs and DNFBPs are still outside the scope of the regime. These exemptions are not justified by risk assessments. Based on identified risk, South Africa has applied reporting obligations on MVDs.

103. Furthermore, FIC Guidance Note (GN) 7 provides for guidance to AIs on implementation of the FIC Act. This GN is enforceable means under the FATF Recommendations as it requires each AI to follow the guidance, or otherwise to be able to demonstrate that the AI nonetheless achieves an equal level of compliance with the relevant provisions in the FIC Act. Furthermore, enforcement action may emanate as a result of non-compliance with the FIC Act where it is found that an AI has not followed the GN7. The guidance has been issued by the FIC, in collaboration with the NT, the SARB and FSB, the predecessor to the FSCA.

104. The Regulations relating to banks were issued by the Minister of Finance in 2012 and are enforceable (Banks Act, s.90). Particularly Regulation 36(17) (page 776) is of importance regarding CBRs, covering all 'banks and controlling companies in respect of a bank', as defined by the Banks Act (s.1).

105. To implement a recommended action from the previous MER on R.16, the SARB issued in 2015 a directive for conduct within the National Payment System (NPS) in respect of the FATF Recommendations for Electronic Funds Transfers (FATF EFTs (EFT Directive) 1 of 2015). In 2017 the

[25] Particularly their transactional business (as far as related to the activities included under R.22(d)), their conveyance role, trust administration, and setting up of trusts and companies.

SARB published an Interpretation Note (IN) for EFT Directive 1 of 2015 to assist the participants in implementing the EFT Directive 1 of 2015. This Directive and its IN are enforceable means under the FATF Methodology as they set out clearly stated requirements for R.16, which are sanctionable for non-compliance under the NPS Act.

Legal Persons and Arrangements

106. The Companies Act of 2008, provides for the incorporation, registration, organization and management of companies and the capitalization of profit companies. It repealed the Companies Act of 1973, which was in place during the previous ME. The CIPC registers, monitors, supervises, and enforces compliance by legal persons with this Act.

107. Legal persons can be registered as profit or non-profit companies. Five main types of for-profit companies can be formed: (i) private companies; (ii) personal liability companies (also known as incorporated companies); (iii) State-owned companies; (iv) public companies; and (v) external for-profit companies. For-profit companies have share capital, and these can be a public company (i.e. shares offered to the public) or a private company (i.e. shares allotted to a limited number of shareholders). Not for profit companies can be: (i) not for profit without members' companies; (ii) not for profit with members' companies, and (iii) external not for profit companies. Not for profit companies do not have share capital but may be without members (default provision of the Act) or with members. Close corporations also exist under the previous Companies Act but no new one may be formed. They do not have share capital; instead members have a percentage interest which represents their contribution. Members can only be natural persons, although a trustee of a trust may be a member in some circumstances. Close corporations do not have directors; all members are responsible for the control.

108. Co-operatives are autonomous associations of persons (a minimum of five) united voluntarily to meet their mutual economic, social, and cultural needs through a jointly owned and controlled enterprise that is organized and operated on co-operative principles.

109. Foreign companies on the register are not companies created in South Africa, but companies created in other jurisdictions that choose to also register in South Africa.

110. There are around 2.1 million legal persons in South Africa, the vast majority being private companies (see Table 1.4). Around 400 thousand new companies are formed and roughly the same amount struck off the register each year. There are approximately 10 million directors with around 2.5 million of those being foreign directors.

Table 1.4. South Africa: Company Statistics Report (as at June 14, 2019)

Type of Legal Persons	Number
Private companies	1,509,814
Public companies	1,986
Close Corporations	355,073
Non-Profit organizations	48,068
Personal liability companies	14 660
Foreign companies with South African presence	1,748
Primary co-operatives	158,867
Secondary co-operatives	1,188
Tertiary co-operatives	84
Total	2,091,488

Source: CIPC, June 14, 2019

Legal Arrangements

111. The only legal arrangements recognized under South African law are trusts. They are regulated under the Trust Property Control Act, 1988. Three types exist in South Africa: inter-vivos trusts (created during the lifetime of the founder (settlor) through agreement between the founder and trustee and involve property being transferred to the trustee to hold on behalf of beneficiaries; testamentary trusts (mostly created through a will by a deceased person leaving their estate to a trustee to administer for a beneficiary); and community trusts (dealing with land restitution claims on behalf of the community).

112. Trusts are registered with, and trustees appointed by, the Master. There were 180,159 trusts on the electronic register at the end of 2018, representing those registered since 2008. Records of trusts established before 2008 exist in paper form only**.** Trust registrations are declining due to limiting tax legislation with around 15 thousand registered per year over 2012 to 2019 as shown in Table 1.5.

Table 1.5. South Africa: Trusts Registered Annually with Master of High Court, 2012 – 2019

2012	2013	2014	2015	2016	2017	2018	2019	Average
18,549	16,374	17,523	17,442	15,814	12,850	12,316	11,558	**15,303**

Source: Master of High Court

113. A trust established by a person outside South Africa in respect of property located in South Africa will be subject to the requirements of South African trust law. A person outside South Africa appointed as a trustee in respect of trust property in South Africa may be authorized as a trustee by the Master only in respect of that property. The Master has no powers over trusts created outside South Africa nor may foreign trusts be registered. Trusts created outside South

Africa by South African citizens or residents with property in such countries are outside the scope of the Master. The Master's Office shares all information in its data base with the SARS for tax assessment and investigation of tax crime purposes.

Supervisory Arrangements

114. AML/CFT supervision is the responsibility of various sector supervisory bodies, including SRBs in the DNFBP sectors, and, where there is no supervisor or SRB, the FIC. The FIC is responsible for national supervisory coordination.

115. The implementation of a twin peaks supervisory model in 2018 created the SARB:PA, which supervises deposit-taking institutions licensed under the Bank Act, and the FSCA, which supervises other financial sector institutions. The supervision of the life insurance sector, including for AML/CFT, was delegated by the FSCA to the SARB:PA via an MOU in 2018. Based on an MOU between the two, supervision of banks' compliance with wire transfer rules is conducted by the SARB:PA in consultation with the SARB:NPSD, which is responsible for overseeing the NPS including with respect to rules for wire transfers. Cross-border MVTS activities are supervised by the SARB:FinSurv, which is also responsible for ensuring compliance with foreign exchange control regulations. Postbank and ISOC engage in deposit-taking activities under an exemption from being licensed as a bank[26] and thus, are not supervised for AML/CFT by the SARB:PA, but by the FIC. The FIC and the SARB:NPSD jointly supervise SAPO's compliance with wire transfer rules.

116. Covered DNFBP sectors are supervised or monitored by their respective supervisors, except for TSPs and KRDs which are under the supervision of the FIC for their obligations as AIs and RIs respectively. Accountants and auditors that are licensed as FSPs are supervised by the FSCA. Additionally, FIC supervises MVDs for their obligations as RIs.

117. VASPs are not subject to AML/CFT obligations other than the reporting obligations that apply to all businesses and are not subject to AML/CFT supervision. Some VASPs have voluntarily registered with the FIC.

International Cooperation

118. South Africa is a regional and continental hub, with large financial flows from other African jurisdictions as well as Europe and North America. Recent cases of *"State capture"* have highlighted the risks faced by South Africa with regards to proceeds of corruption and other financial crimes being laundered abroad. Most information exchange occurs with countries in Europe and Africa; major international cooperation countries include the United States, Botswana, and Germany.[27]

[26] As of the onsite, Postbank was in the process of applying for a banking license.

[27] Based on analysis of the latest available detailed data on MLA requests.

119. Feedback on international cooperation, received from 15 countries, was generally positive but noted that provision of assistance can be slow on the part of the South African authorities.

120. Formal MLA requests may be directed via the DIRCO or the MoJ and NPA, and informal cooperation achieved through these central channels as well as on an agency-to-agency basis.

NATIONAL AML/CFT POLICIES AND COORDINATION

A. Key Findings and Recommended Actions

Key Findings

- Corruption, tax related crimes and fraud, are understood as the main domestic ML threats consistently by the key AML/CFT authorities but the understanding of the relative scale of such threats as well as the vulnerabilities or channels exploited to launder the proceeds is limited. The threats arising from proceeds of foreign predicates is understood only to a very limited extent. The authorities' understanding of TF risks is underdeveloped and uneven.

- South Africa is yet to develop coordinated and holistic national AML/CFT policies informed by ML/TF risks. Some ML risks are mitigated by existing policies or measures but significant risks remain largely unaddressed for beneficial owners of legal persons and trusts, cross-border movement of cash, and criminal justice efforts are not yet directed towards effectively combating higher risks such as ML related to corruption, narcotics, and tax offenses. Efforts at the policy level have been focused mainly on terrorism and are yet to target TF risks.

- Some sectors (including VASPs and potential high-risk DNFBPs) are not yet captured by the AML/CFT regime and their risks are not yet assessed. Simplified measures are often not justified by proven low risks.

- The extent to which the competent authorities' priorities and objectives are aligned with national ML risks and policies is uneven, with the LEAs and the NPA focusing more on predicate crimes than on ML and supervisors at varying stages in applying an RBA to AML/CFT supervision. The authorities' objectives and activities are aligned with the TF risks only to the extent that such risks are recognized.

- The IDC on AML/CFT, the policy coordinating body, plays a central role in coordinating the ML NRA and TF NRA but excludes some stakeholders and is yet to generate any AML/CFT policy initiatives at the strategic level. Coordination and cooperation at the operational level works well in general but the often-formal nature sometimes prolongs the process.

Recommended Actions

- The authorities should improve their understanding of the major proceeds generating crimes, including those committed in a foreign country and channels and vulnerabilities exploited to launder these proceeds.
- The authorities should improve and harmonize among themselves, their understanding of TF risks including by completing the TF NRA to inform policies to prevent and combat TF.
- South Africa should develop national AML/CFT policies to address higher risks for: (i) BO; (ii) use of cash and its cross-border movement physically and through illegal MVTS; (iii) third-party ML; (iv) foreign predicate crimes; and (v) TF, including by fully integrating it into the NCTS. South Africa should also ensure all FIs, DNFBPs and VASPs (unless they are assessed as posing a proven low risk), in particular those with potentially higher risk such as DPMS and CSPs, are subject to AML/CFT obligations and supervision or monitoring.
- South Africa should ensure the key AML/CFT agencies' priorities, objectives, and performance targets are aligned with ML/TF risks identified and national AML/CFT policies, particular to ensure that LEAs focus on significant ML.
- The authorities should review the composition and structure of the IDC on AML/CFT to ensure it is (i) inclusive of all stakeholders including DNFBP supervisors; and (ii) able to drive policy making in both the Financial Cluster and the JCPS cluster.
- The authorities should put in place mechanisms for cooperating and coordinating to combat the PF of weapons of mass destruction.
- The authorities should share the findings of the ML NRA and TF NRA, upon their conclusion, to all private sectors subject to AML/CFT obligations.

The relevant Immediate Outcome considered and assessed in this chapter is IO.1. The Recommendations relevant for the assessment of effectiveness under this section are R.1, 2, 33 and 34, and elements of R.15.

B. Immediate Outcome 1 (Risk, Policy and Coordination)

Country's Understanding of its ML/TF risks

121. South Africa is in the process of concluding its first coordinated assessment of ML/TF risks at the national level. The ML NRA exercise was coordinated by an AML/CFT NRA Inter-Departmental Working Group (NRA IWG) and involves major stakeholders in the public sector (see page 16 for more details). The NRA IWG, however, excludes some stakeholders, notably regulators of DNFBPs – some of them were only invited to comment on a draft report late in the process. Financial sectors' inputs were sought through supervisors and reflected in various SRAs, which fed into the NRA. Some casinos, attorneys, and TSPs participated in sector risk assessments (SRAs) conducted by the FIC by responding to surveys. Although key statistics such as STRs, ML

investigations, prosecutions and convictions were considered, the NRA takes a primarily qualitative approach and relies on experts' judgement and SRAs, complemented by open source information. Preliminary finding documents on ML and TF were completed in July and August 2019 respectively.[28]

122. The main domestic ML threats including, inter alia, corruption, tax related crimes, and fraud, are understood consistently by the main AML/CFT authorities, but the authorities' understanding of the relative scale of such threats is questionable. The basis for considering these threats high-risk is more how significant the impacts are, the analysis of which sometimes is rather narrowly focused (for instance, the impacts of fraud on the banking sector), rather than the scale of the proceeds generated. Corruption is identified as a main concern for its role as an "enabler" of other predicate offenses and ML, including by undermining some key AML/CFT agencies, less so for the scale of proceeds generated, which the authorities indicated was not as high as that of tax crimes or drug trafficking. The basis of this assertion about the relative scale of proceeds is unclear. The authorities highlighted VAT fraud as a main tax-related offense and also recognized evasion of income taxes as a concern.

123. Authorities noted some vulnerabilities or channels exploited to launder proceeds of domestic predicates, in particular for the use of cash, while their understanding of more sophisticated ML schemes is limited. During the onsite, the authorities indicated that they believe the proceeds that stay within South Africa are mainly used to support luxurious lifestyles including by purchasing real estate, motor vehicles etc., in many cases through corporate structures or trusts. The authorities also noted that some proceeds are laundered cross-border through cash smuggling, trade-based schemes (e.g., mis-invoicing), wire transfers, and overseas cash withdrawal using bank cards. Such knowledge is however not fully translated into appreciation of sector vulnerabilities (see more discussion below). The authorities also did not show an in-depth understanding of the specific vulnerabilities or channels exploited, such as types of corporate structures most misused or vulnerable, the role of enablers, the geographic regions or corridors most exposed to cash smuggling or trade-based schemes, or the foreign jurisdictions where the most proceeds ended up (though Dubai and China were mentioned in a few recent cases). Moreover, their understanding of more sophisticated schemes appears limited. The authorities well recognize the need for an improved understanding of the vulnerabilities and channels but the relative low number of cases for significant or sophisticated ML or main proceeds generating predicate offenses (such as corruption) hampers such efforts.

124. While banks are consistently considered to be most exposed, there is a degree of disconnect between the authorities' understanding of sector ML vulnerabilities in other sectors and known ML typologies. The onsite discussions suggest that there is a general consensus among the authorities that banking is the most exposed to ML risks, which is consistent with known ML typologies, but banks are rated as medium- to high-risk in the SRA. The authorities' understanding of sector ML vulnerabilities of other sectors is primarily informed by the SRAs, which concluded with risk ratings that do not appear aligned with known typologies (see **Error! Reference source not f**

[28] They also intend to extend the NRA exercises to cover PF.

ound.. for SRA ratings). For instance, gambling entities are rated as high-risk though only one known ML case involves a casino. Similarly, the authorities noted that real estate, motor vehicles, and corporate structures were often involved in known ML cases, but such knowledge does not seem to feed into the SRAs or inform understanding of sector vulnerabilities. Attorneys and estate agents are both rated medium risk. Furthermore, some DNFBP supervisors were not involved in the analysis and do not agree with the SRA ratings of the sectors under their purview. Finally, the potential ML/TF risk exposure of unregulated sectors not yet covered under the AML/CFT regime is largely unknown. These include DPMS, CSPs that are not attorneys, accountants (for activities other than providing financial services) and VASPs (see more below).

125. The authorities could not demonstrate an understanding of threats from foreign predicates or vulnerabilities exploited to launder the proceeds. The preliminary findings of the ML NRA noted that South Africa's financial system (particularly banks) is a gateway for funds flowing from the rest of sub-Saharan Africa to the rest of the world, including potential foreign proceeds of crimes such as corruption. Despite ML cases with sizeable foreign proceeds in cases South Africa presented to assessors, none of the main AML/CFT agencies appear to recognize or prioritize foreign proceeds of crime. The NRA IWG acknowledges that the understanding of such risks needs to be improved at the national level.

126. The authorities identified some potential TF threats, but their understanding of such threats is constrained by the narrow approach taken to assessing risks. Prior to the TF NRA exercise, TF issues were viewed primarily through the lens of terrorism that potentially targets South Africa, perceived by authorities to be low risk. Although the TF NRA preliminary findings identify a number of potential threats associated with FTFs and foreign terrorist groups on the continent and beyond using South Africa as a transit point and planning base, authorities considered the TF threats to be low, based on the lack of established evidence from law enforcement or intelligence agencies to demonstrate that such potential threats have materialized. Using this narrow approach, the authorities' low-risk conclusion is based on known intelligence that is incomplete due to their lack of an in-depth understanding of vulnerabilities that might have been exploited by potential threats (see below), hence does not seem well grounded. Moreover, they are reluctant to classify politically motivated violent acts as terrorism, which further narrows the evidence based on which they assess TF threats (see details in chapter 4).

127. Authorities have expressed concern about some high-level vulnerabilities that could be exploited for TF but are unable to determine if, or to what extent, such exploitation is occurring. These vulnerabilities include weak border controls for money and people, informal remittances from émigré communities to their home countries, NPOs, potential links between terrorist groups and organized crime, new financial technologies such as VAs and crowd funding. Many of these vulnerabilities are identified on the basis that there exists the potential for certain vulnerabilities in the AML/CFT system to be exploited by terrorist groups for support. Any insights from the authorities into how these vulnerabilities may be exploited to fund the agendas of international or domestic terrorists were not shared with the assessors.

128. Authorities' understanding of sector vulnerabilities related to TF is poor. None of the SRAs differentiate between ML and TF vulnerabilities or address TF risks specifically. Nor do they inform the TF NRA. Across all sectors, supervisors were not involved in the TF NRA and show a very limited understanding of TF risks, if any. They see TF issues almost only in the context of ensuring compliance with TFS obligations.

129. South Africa recognizes the potential ML/TF risks of VASPs[29] and has taken initial steps to identify them but is yet to develop a full-fledged understanding of such risks. The SARB issued a Position Paper on Virtual Currencies[30] in 2014, which draws from findings of the FATF and EU on potential ML/TF risks of VASPs. More recently, the ML and TF NRAs reflected some of these risks as well. VASPs are often considered as high-risk customers by banks because they are not regulated. The inherent ML risks of VASPs are yet to be assessed, though evidence suggests that VASPs and VAs are exposed to abuse through some predicate crimes, in particular fraud. The TF NRA considers VASPs to be increasingly susceptible to TF based on a few known cases while specific vulnerabilities have not been identified. More broadly, the authorities, through the Inter-Governmental FinTech Working Group (IFWG), have taken steps to take stock of the VA market in South Africa to inform the development of a regulatory framework and issued a consultation paper that recognizes the generic risks of VA being misused for ML or TF.[31]

130. Authorities noted some high-level weaknesses in the AML/CFT regime. There is a broad consensus that a relatively low number of ML prosecutions and convictions represents the weakest aspect of the regime, with the LEAs being significantly affected in the past decade by "*State capture*". The limited number of cases also adds to the challenges in understanding risks (see para. 123. above). Authorities also recognize gaps in sector coverage and lack of transparency of BO information as deficiencies. Generic challenges regarding domestic coordination, international cooperation, resources, and capacity constraints are also identified.

National Policies to Address Identified ML/TF Risks

131. South Africa is yet to develop coordinated and holistic national AML/CFT policies informed by ML/TF risks. A few existing policies or measures address some of the risks identified but as they are not fully informed by risks, these often are not designed using a holistic approach that involves all relevant aspects of the AML/CFT regime:

[29] The authorities have prepared a legislative proposal to subject VASPs to AML/CFT obligations.

[30] See: http://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf

[31] See: http://www.treasury.gov.za/comm_media/press/2019/CAR%20WG%20Consultation%20paper%20on%20crypto%20assets_final.pdf:

- South Africa amended the FIC Act in 2017 to close some gaps in the legal framework and provide for a RBA to preventive measures but some higher-risk activities are yet to be covered (see more details under para. 123).

- South Africa has developed and implemented measures to promote financial inclusion. These have aimed to enable greater access to formal financial services and to bring the activities into the formal system (see more details in chapter 1). There are, however, no specific policies on reducing the use of cash to help mitigate ML risks (e.g., limiting use of cash in large-value transactions such as purchasing real estate, etc.).

- CTRs were introduced in 2010 to improve FIC's sources of financial intelligence. AIs and RIs must report cash transactions over R24,999.99 ($1,700). Over 150,000 CTRs have been used over the past six years in FIC disclosures to LEAs to help with investigating potential ML and associated predicate offenses involving cash (see section on Legal Systems and Operational Issues).

- The authorities brought MVDs into the AML/CFT regime as RIs in 2001 because they considered the MVDs' cash-intensive business nature higher risk. The FIC has been overseeing them actively (see more in chapter 6).

132. However, some significant ML/TF risks remain largely unaddressed:

- **Measures taken to combat corruption and other serious crimes are yet to address the laundering of the proceeds.** The SAPS:DPCI unit was established in 2009 to prioritize the investigation of serious organized crime, serious commercial crime, and serious corruption. Moreover, an Anti-Corruption Task Team (ACTT) was established in 2010 to facilitate investigation and prosecution of priority corruption cases.[32] However, the efforts of the SAPS:DPCI and the ACTT are not yet directed towards effectively pursuing ML related to these serious crimes. Risks from proceeds of corruption are targeted by supervisors to a limited extent but these efforts are undermined by a deficient legal definition of domestic PEPs (see section on Preventative Measures).

- The authorities are yet to put in place policies to tackle the challenges in accessing accurate and up to date information on **beneficial owners** of legal persons and trusts. The supervisory efforts are not targeted towards sectors or entities involved in company and trust services, such as attorneys and TSPs.

- **Some potentially high-risk sectors,** notably CSPs (which are not attorneys) and DPMS, **remain out of the regime** (see details in para. 133. below).

- **Risks associated with the cross-border movement of cash remain largely unaddressed**, especially between South Africa and other members of the CMA, for which no controls are in

[32] Members are: the SAPS:DPCI, the NPA, the NPA:AFU, the SIU, the SARS, the NT (offices of the Accountant-General and the Chief Procurement Officer), the FIC, the NICOC, the SSA, the Presidency, the DoJ&CD, the Department of Public Service and Administration (DPSA) and the Government Communication and Information System (GCIS).

place over such movement. Controls over **cross-border movement of cash and bearable negotiable instruments (BNIs)** to or from other countries have been focused mainly on airports and outflows. The Customs and Excise Division of SARS (SARS:Customs) responsible for such controls does not have sufficient systems and staff to enforce them.

- Overall, identifying and sanctioning **illegal MVTS** is not being pursued as a policy objective of the AML/CFT regime in a collaborative manner and such efforts have been very limited and fragmented. A few high-profile cases have been picked up and being handled by the Illicit Financial Flows Task Team (IFFTT), the focus of which is large-size outflows in breach of foreign exchange controls, rather than activity linked to ML or TF. Thus, the remaining bulk of smaller illegal networks are not being addressed.

- The **proceeds of foreign predicate crimes** are not being targeted proactively by LEAs due to the lack of understanding of such risks**.** Supervisory activities for South African banks' operations in other countries in the Southern African Development Community[33] (SADC) are not risk driven**.** Other sectors potentially exposed to such risks, for instance, estate agents, are not receiving supervisory attention commensurate with their risk profiles. The criminal justice system is also not addressing these threats.

- The authorities were challenged to show how they are proactively addressing **TF risks**, Based on a synopsis shared with the team, the NCTS addresses TF only to the extent of generally recognizing the need for (i) regulating financial sector to mitigate risks from domestic extremism and international terrorism; and (ii) making financial investigation an integral part of all terrorism investigations.[34] In the Implementation Plan that follows the Strategy, one of the priorities identified is to strengthen capacity to conduct financial investigations into TF, which was however assigned to the FIC rather than LEAs. The team was not provided information on the progress made towards this priority. The authorities also indicated that the National Intelligence Estimate (NIE) compiled by National Intelligence Co-ordination Committee (NICOC) annually includes FIC's inputs on TF risks, but the assessors were not able to verify.

Exemptions, Enhanced, and Simplified Measures

133. Exemption or simplified measures are often not justified by risks:

- **Sector coverage**: Cooperative FIs (CFIs), credit providers other than money lenders against securities, FinTech companies (that offer financial services and are not VASPs or FSPs), VASPs, DPMS,[35] accountants (for activities other than providing financial services), and CSPs other than attorneys are not subject to AML/CFT obligations except the general requirements to file STRs

[33] SADC is an inter-governmental organization in the Southern African Region of 16 countries: Angola, Botswana, Comoros, Democratic Republic of Congo, Eswatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Tanzania, Zambia, and Zimbabwe. Its headquarters is in Gaborone Botswana.

[34] The authorities intend to integrate CFT into the NCTS and its action plan.

[35] Currently KRDs are subject to limited obligations as RIs.

that apply to any businesses (see R.20 in the TCA) and are not subject to supervision or monitoring. These exclusions are not based on risks.

- **Enhanced or simplified measures**: Since the NRAs and SRAs are yet to be concluded, risk assessment results are not yet used to inform the application of enhanced and simplified measures. GN7 suggests some non-binding indicators to help AIs' assess ML/TF risks, but these are fairly generic and only point to a few specific high-risk factors in South Africa's context (e.g., domestic PEPs and cash use). Thus, to a large extent, the private sector has discretion to define high- and low-risk scenarios and the enhanced or simplified measures applicable. In addition, AIs can take simplified measures when risks are assessed as lower, but such measures may be allowed even when there is a suspicion of ML/TF or when the AI does not adequately understand and assess its ML/TF risks. The deficiencies in AIs' risk assessments mean that the scenarios and measures defined often are not supported by proper risk assessments (see more details in chapter 5).

Objectives and Activities of Competent Authorities

134. National policies are yet to be developed to direct setting of AML/CFT objectives and allocation of resources. As of the onsite, the extent to which objectives and activities of key AML/CFT agencies are aligned with ML/TF risks and national policies varied.

135. Some ML cases have been identified, but overall, the NPA and LEAs have been focused mainly on predicate offenses rather than ML or TF. The NPA's Strategic Plan 2013-2018 recognized ML as an "emerging crime" in its performance environment but did not elaborate on its significance or indicate the level of priority given to tackle it. According to this Plan, the NPA:AFU's performance is measured by the "value of completed forfeiture cases". It uses a Case Intake and Allocation Committee to evaluate cases in terms of asset recovery potential, but the criteria used for such evaluation were not shared with the assessors. Although the SAPS:DPCI – Financial and Asset Forfeiture Investigation (SAPS:DPCI – FAFI) Component identifies *"[i]mprove successful financial and asset forfeiture investigations, resulting from ML investigations and asset seizure/forfeiture"* as one of its priorities during 2015 – 2019, at the SAPS:DPCI level emphasis is placed on the investigation of predicate offenses rather than identification and investigation of ML networks and professional enablers. Accordingly, the NPA's ML prosecutions are focused mainly on self-laundering cases with no prosecutions of third-party ML. Little attention has been paid to investigation and prosecution of ML arising from foreign predicate offenses. Furthermore, some key performance indicators might have unintendedly encouraged undue focus on small and simple cases hence diverting efforts away from combatting complex and higher risk ML/TF activities.[36] The objectives and activities of the SAPS and the NPA in investigating TF is coordinated through the CFTC chaired by the SSA and are

[36] For example, the NPA has a performance target of obtaining convictions for more than 90 percent of prosecutions it undertakes; the SAPS:DPCI is expected to deliver case ready files for 90 percent of the ML investigations it undertakes.

aligned with the TF risks only to the extent that such risks are recognized by the CFTC. Very few TF cases have been investigated.

136. While the FIC indicated that it pays special attention to certain predicate crimes deemed high-risk, these are only partially aligned with South Africa's risk profile. Although the FIC, in its analysis of transaction reports, gives priority to those that involve the state or SOEs, its disclosures related to corruption only constitute four percent of the total proactive disclosures. Disclosures related to fraud and tax evasion constitute 27 percent and 23 percent respectively. A share of proactive disclosures is labelled ML (24 percent) and TF (15 percent), but the underlying predicate crimes are not specified (see **Error! Reference source not found.** 3.1 in chapter 3).

137. While some supervisors have covered certain - in some cases isolated - aspects of ML risks, the extent to which they have targeted TF risks has been very limited reflecting their lack of understanding of such risks. The supervisors are at varying stages in applying an RBA to AML/CFT supervision, with the SARB:PA being the most advanced, followed by SARB:FinSurv. The risk matrixes used by the SARB:PA (for the banking sector) have incorporated some risk factors key in the South African context. However, the risk ratings inform selection of entities to be inspected and scope of inspections only to a limited extent. The FSCA is yet to apply an RBA to AML/CFT supervision specifically – its activities so far have not been informed by ML/TF risks. The FIC's supervisory activities have been primarily driven by promoting registration by AIs and RIs with the FIC and filing of CTRs, with little regard to other aspects of the risks. The only thematic inspections carried out by supervisors were done by the SARB:PA and SARB:FinSurv on TFS, which by nature is rules-based with limited regard to risks (see more details in chapter 6).

138. None of the authorities' objectives and activities seem orientated effectively towards targeting high ML risks posed by foreign proceeds entering or flowing through South Africa and cash and its cross-border movement physically, or risks associated with illegal MVTS. There is very little activity by all key AML/CFT agencies directed towards the risks from foreign proceeds of crime. The SARB:FinSurv makes some efforts to uncover illegal cross-border MVTS activity but not as a high priority. Its efforts were not followed up by the SAPS to sanction and shut down illegal operators. The SARS, responsible for border cash matters, seems to focus mainly on outwards cash movement at the main airports only.

National Coordination and Cooperation

139. The IDC on AML/CFT, an advisory committee, was established in November 2017 to understand and mitigate ML/TF risks but does not involve all stakeholders. The IDC brings together the NT, the FIC, financial regulators, LEAs, prosecutors, and the security agency but it notably excludes the supervisors of DNFBPs.[37] The NPO Directorate, which is part of the IDC structure, did not attend IDC meetings though there is a separate NPOTT established in 2018 to coordinate on risk assessment of NPOs (see more in chapter 4). The CIPC, the company registry, though being part of the IDC structure, was only invited to an IDC meeting in May 2019. The DNFBP

[37] For the real estate sector, for casinos, for attorneys, and for the accounting profession.

supervisors, the NPO Directorate, and the CIPC were therefore not involved in the ML NRA or TF NRA. Some DNFBP supervisors do not agree with the preliminary findings and expressed concerns about a proposal to shift their AML/CFT supervisory responsibilities to the FIC,[38] suggesting the need for better coordination to build consensus on such policy initiatives.

140. The IDC plays a central role in coordinating the NRAs but has yet to generate any AML/CFT policy initiatives at the strategic level. The IDC is mandated to identify measures that will assist in mitigating ML/TF risks more effectively. Chaired by the NT, which falls under the Financial Cluster, the IDC's agenda to date has been driven mainly by financial regulatory issues and preparation for the assessment. In particular, the IDC plays a central and critical role in coordinating the country's first ML and TF NRA exercises. Although the law enforcement and judicial aspects of the regime (main LEAs, NPA, SSA, etc.), which falls under the JCPS cluster, is represented in the IDC, no discussions have taken place on specific issues related to their AML/CFT work. In light of the ML NRA and TF NRA being still ongoing, the IDC is yet to produce any major AML/CFT policy initiatives. With the IDC's current structure and the records of its activities to date, its ability to enable or influence policy making within the JCPS cluster cannot be established.

141. AML/CFT issues are considered in policy development on some regulatory issues led by the NT but not on issues that fall under the JCPS cluster. In the Consultation Paper on Policy Proposals for Crypto Assets prepared by the IFWG, considerations have been given to harmonizing the regulatory framework and the envisaged introduction of AML/CFT obligations to VASPs. A consultation paper on financial inclusion recognizes the need to balance financial inclusion objectives and implementation of AML/CFT measures. As noted above, the existing policy initiatives against terrorism cover TF only to a limited extent.

142. AML/CFT Cooperation and coordination at the operational level works well in general, though some stakeholders are not involved in certain aspects of the operations. In addition, such cooperation is often very formal (i.e., has to be based on a Memorandum of Understanding - MOU) and may be less timely than could be achieved through more informal cooperation. Specifically:

- **With regard to ML investigations and prosecutions**, in addition to MOUs, various mechanisms such as the ACTT and the IFFTT, exist for the FIC, LEAs, and the NPA to cooperate in pursuing predicate crimes, but they are not being sufficiently used to pursue ML. The South African AML Integrated Task Force (SAMLIT) was established recently, which aims to enable more public-private collaboration between the FIC, the SARB:PA and banks to support investigations and to better understand financial crimes trends.

- **With regard to TF investigations, prosecutions, and prevention**, the CTFC, the main operational body that coordinates the handling of TF cases, works effectively. Under the CFTC, every terrorism related inquiry involves a component of TF worked on by the FIC, but TF is not

[38] The legal consultation process of the proposal commenced in July 2020.

being proactively identified and pursued. The IDWG-CT[39] oversees the reporting on, and implementation of, South Africa's international obligations associated with TF arising from the UNSCRs. It, however, does not include regulators responsible for overseeing implementation of TFS by FIs and DNFBPs.

- **With regard to supervision,** cooperation between FIC and the supervisors appears to be strong, particularly in that FIC provides inputs into and supports onsite inspections conducted by other supervisory bodies, with the exception of the LPC[40], which has not yet carried out any AML/CFT oversight. An FIC Act Enforcement Forum was established in 2011 to discuss issues pertaining to interpretation and enforcement of the FIC Act. The cooperation among the FIC and supervisors is weaker in developing sector specific guidance to help the private sector implement the risk-based preventive measures. The SARB:PA and the FSCA cooperate at the licensing stage but no evidence suggests they collaborate in AML/CFT supervision of banking, life insurance and securities institutions that belong to the same group.

143. Coordination on PF remains fragmented and takes place at different levels through IDCs which focus on proliferation rather than PF. The South Africa Council for the Non-Proliferation (NPC) of Weapons of Mass Destruction (WMD) is the main coordinating body focused on export controls of dual goods and nuclear items. Formal coordination among authorities on PF is still at its early stage and is lacking a more integrated and holistic approach.[41]

Private Sector's Awareness of Risks

144. The authorities intend to publish sanitized versions of the ML NRA and TF NRA upon their conclusion. A high-level summary of the preliminary findings of ML NRA has been shared with representatives of some private sectors in a few workshops while preliminary findings of TF NRA have not been shared with the private sector. The SARB:PA and the FSCA have shared the SRAs or their high-level summaries with some entities and intend to publish the SRAs. SRAs of DNFBPs have not been shared with the private sector. Preparation of some SRAs involved the private sector only to a limited extent. The sectors not yet covered have not been shared with any information of the NRAs.

C. Overall Conclusion on IO.1

145. Faced by a relatively high volume and intensity of crime, the authorities have demonstrated understanding of domestic ML threats, including those related to corruption, and associated vulnerabilities to some extent, while their understanding of TF risks has been limited. Their lack of understanding of ML risks arising from foreign proceeds is a concern as South Africa is

[39] Members: the DHA, the DoJ&CD, the Departments of Social Development, Defence, Correctional Services, and Transport, the NT, the SAPS, the SSA, the NICOC, the NPA, the FIC, and the SARS

[40] An MOU was signed by the LPC with the FIC in 2019 to delegate the functions of AML/CFT supervision of attorneys.

[41] The authorities intend to extend the IDC's mandate to PF.

a regional financial hub. Moreover, the country is yet to develop and implement national policies to address its ML/TF risks, which has prevented AML/CFT agencies from setting up objectives and aligning their activities with national priorities. Operational AML/CFT cooperation and coordination works relatively well but the IDC, the policy coordinating mechanism, excludes some stakeholders and is yet to generate any AML/CFT policy initiatives at the strategic level. A particular concern lies in the IDC's questionable ability to drive or influence policy making within the JCPS cluster.

146. South Africa is rated as having a moderate level of effectiveness for IO.1.

LEGAL SYSTEM AND OPERATIONAL ISSUES

A. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 6

- Authorities in South Africa, particularly SAPS, routinely use financial intelligence to help investigate predicate crimes and trace criminal assets, primarily related to fraud and corruption. The use of financial intelligence, however, by SAPS to proactively investigate ML or TF specifically, was demonstrated to a significantly lesser degree, driven in part by inadequate skills and resources.

- Each year the FIC receives around 300,000 STRs and Suspicious Activity Reports mainly from banks and ADLAs (cross-border money remitters and bureau de change). It also receives annually more than five million cash transaction reports (CTRs) and two million cash threshold aggregate reports (CTRAs). These reports are increasing in quality, particularly from banks, as a result of feedback from the FIC, which has good systems for analyzing them.

- While South Africa has benefited from some voluntary reporting (notably from a few VASPs), the data held by the FIC is incomplete in the sense that the FIC is not receiving reports from many higher-risk DNFBPs and does not routinely receive intelligence from cross-border cash declarations or related violations.

- FIC makes effective use of its powers to obtain additional information from reporting entities to follow the money and trace criminal proceeds. It also provides proactive and reactive disclosures to LEAs and has been able to provide 'live monitoring' during selected investigations. The vast majority of the FIC disclosures, however, are reactive and relate to the predicate offenses for ML, with ML or TF specific disclosures representing only eight percent of the total.

- FIC produces limited strategic products. It does contribute to the National Intelligence Estimates. However, the main strategic intelligence product, the GIS Quarterly Report, is not proactively disclosed to LEAs.

- The FIC, the SAPS and the SARS cooperate effectively and form 'Task Teams' (TTs) to address major predicate offense, ML & TF investigations.

Immediate Outcome 7

- The authorities identify and investigate ML cases to some extent. Emphasis is placed on the investigation of predicate offenses. PFIs are undertaken in all cases of organized crime, serious commercial crime, and serious corruption. SAPS:DPCI pursues ML offenses during the investigation of predicate offenses but the authorities have not sufficiently demonstrated the proactive identification and investigation of ML cases as a primary objective.

- Investigation and prosecution of ML activity is partly consistent with South Africa's risk profile. The bulk of ML cases investigated and prosecuted relate to fraud, which is somewhat consistent. There are fewer ML prosecutions relating to other high-risk areas such as serious corruption, narcotics, and tax offenses. ML cases relating to *"State capture"* have not been sufficiently pursued in the past, and corruption cases referred to the NPA by the SIU have not been dealt with expeditiously.

- The NPA has suffered from major resource and staffing constraints, which is now being addressed by the establishment of the NPA:ID, and an increased budget allocation for hiring of prosecutors.

- Prosecutions for ML are regularly undertaken, and a reasonable number of convictions is being achieved but only partly consistent with South Africa's risk profile. The cases largely concern self-laundering based on the predicate offending which is often prosecuted at the same time. Standalone ML cases are prosecuted, but few cases of third-party ML and foreign predicate offenses are prosecuted. This appears to be a consequence of the focus on the investigation of predicate offenses rather than the proactive identification and investigation of ML networks and professional enablers.

- Sanctions applied against natural persons convicted of ML offenses are to some extent effective, proportionate, and dissuasive. South Africa has a high head sentence of 30 years' imprisonment for the ML offense and sentences of up to 25 years imprisonment have been handed down in practice. However, the majority of sentences imposed by the courts involve non-custodial or suspended sentences for the ML offense. Sanctions have been applied against legal persons.

Immediate Outcome 8

- South Africa proactively pursues confiscation of criminal proceeds and instrumentalities as a policy objective and some good results have been achieved. The NPA:AFU places emphasis on its civil forfeiture powers under POCA which targets tainted property. Less emphasis is placed on criminal confiscation of property of equivalent value, which is dependent upon a conviction for the ML or predicate offense.

- Whilst the authorities have demonstrated positive results for recovery of proceeds of crime in the area of fraud and economic crime including ML, efforts for recovery of assets from *"State capture"* and proceeds which have been moved to other countries have been less successful to date due to the phenomenon of *"State capture"* itself and resource constraints. Recent efforts are beginning to show positive results in some major cases, but these efforts are still at the early stage. Recovered property is consistently returned to victims including state-owned enterprises (SOEs) or is paid to the Criminal Assets Recovery Account (CARA). Sharing of funds with foreign jurisdictions is sometimes pursued, and the authorities have demonstrated the recovery of proceeds arising from foreign predicate offenses in some cases.

- South Africa has not positively demonstrated that confiscation of falsely declared or undeclared cross-border movement of currency is being addressed and applied as an effective, proportionate, and dissuasive sanction. Use of cash is prevalent in South Africa and it has been assessed as high risk from a ML and TF perspective, including cross-border movement.

- Overall, confiscation of proceeds of crime partially reflects South Africa's ML/TF risk and national AML/CFT policies and priority. The bulk of tainted property recovered by the authorities stems from economic crime and fraud. Recovery of assets from serious corruption, including foreign corruption, has been less successful to date, but positive efforts are now underway to address the issue. The detection and recovery of cash proceeds of crime remains challenging.

Recommended Actions

Immediate Outcome 6

- The SAPS should increase its requests from the FIC for ML and TF specific financial intelligence.

- The SAPS and the SARS should increase their skills and resources so that they can much better use financial intelligence in their investigations.

- The FIC should receive information contained in the SARS cross border cash declaration system proactively. In addition, outreach should be made to those DNFBPs that are under-reporting to increase the volume and quality of STRs received from them.

- The FIC should be granted access to relevant SAPS databases to assist in the identification and prioritization of relevant STRs.

- FIC should proactively disclose its GIS Quarterly and Annual Reports to LEAs and develop in-depth strategic reports focused on analysis regarding typologies and trends relating to predicate crimes, ML and TF to support LEA's operational needs.

Immediate Outcome 7

- The SAPS:DPCI should place much more emphasis on the proactive identification and investigation of ML cases as a strategic priority, over and above the investigation of serious predicate offenses.
- The authorities should significantly enhance efforts to pursue ML cases from, serious corruption (including *"State capture"*) and other high-risk areas such as narcotics and tax evasion. This includes expeditious handling of cases referred to the NPA by the SIU in terms of the recent MOU entered into between the agencies.
- The LEAs and the NPA should place much greater emphasis on investigating and prosecuting third-party ML and cases of foreign predicate offenses.
- Efforts to pursue high level, complex and serious cases of ML and to tackle ML networks and professional enablers should be prioritized.
- Sufficient resources should be allocated to the authorities to achieve these actions, including attracting and retaining skilled staff and expertise.

Immediate Outcome 8

- Efforts for recovery of assets from *"State capture"* and proceeds which have been moved to other countries should continue to be prioritized.
- Recovery of crime proceeds from high risk areas such as serious corruption, narcotics and tax evasion should be enhanced by greater use of multidisciplinary or fusion teams from the FIC, the SAPS:DPCI, the SARS, the NPA, and the NPA:AFU at the operational case level.
- Additional focus should be placed on the recovery of proceeds from foreign predicate offenses, including seeking assistance from other jurisdictions to support such action and sharing or repatriation of funds in appropriate cases.
- Major efforts to enhance the effectiveness of measures to detect and seize illicit cross-border cash flows at air, sea, and land border points should be undertaken. The authorities should expedite a review of the cash declaration system and implement a revised system which is effective in countering cash smuggling activities and introduce enhanced monitoring systems.
- Sufficient resources should be allocated to the authorities to achieve these actions.

The relevant Immediate Outcomes considered and assessed in this chapter are IO.6-8. The Recommendations relevant for the assessment of effectiveness under this section are R.1, R.3, R.4 and R.29-32 and elements of R.2, 8, 9, 15, 30, 31, 34, 37, 38, 39 and 40.

B. Immediate Outcome 6 (Financial Intelligence ML/TF)

Use of financial intelligence and other information

147. South African competent authorities,[42] particularly SAPS use financial intelligence to help investigate predicate crimes, ML and TF, while the NPA:AFU uses financial intelligence to identify and trace criminal assets. The FIC produces both Reactive Disclosures (ones in response to a request for information) and Proactive Disclosures (unsolicited). The former are seen as more useful to LEAs than the latter. Over the five-year period from 2014 to 2018 South African competent authorities made 8,634 requests for information to FIC for financial intelligence relating to ongoing cases. However, the vast majority of these requests (92 percent) were for predicate crimes, with ML (five percent) and TF (three percent) representing only eight percent of the total requests indicating that while the use of financial intelligence is used to a large extent to support investigations of predicate offenses it is only being used to some extent to develop evidence and proactively identify ML and TF offenses. Table 3.1 identifies the major crimes that were the subject of the requests made by South African competent authorities to the FIC:

Table 3.1. South Africa: Requests Made to the FIC by South African LEAs 2014–2018

Crime Type	Number of Requests	Percentage of Total Requests
Fraud Related Crimes	2,338	33%
Corruption	1,200	17%
Drug Related Crimes	1,028	15%
Tax Evasion	985	14%
Robbery & Theft	588	8%
Environmental Crimes	198	3%
ML	469	7%
TF	221	3%
Total	7,027	100%

148. While South Africa has yet to complete a NRA (see section on ML/TF Risks and Context), the top four predicate offenses for which LEAs[43] are requesting financial intelligence from the FIC seems to be generally in line with the proceeds generating crimes that cause the most significant risk to the South African economy.

149. SAPS, as the agency responsible for investigations into ML and TF, is not appropriately requesting financial intelligence specific to ML or TF offenses. While ML charges are laid, and convictions obtained (see IO.7), ML charges are incidental to the investigation of the predicate offense, with stand-alone ML investigations a rarity.

150. As indicated in IO.7, the SAPS has suffered during the period of *"State capture"* from a loss of key experienced personnel and a hiring freeze on new resources. The SAPS:DCPI

[42] The competent authorities included in these numbers that are authorized to receive FIC disclosures are: the SAPS, the SARS, the NPA:AFU, the SSA, the SARB:FinSurv, the FSCA, the IPID, the NPA:SCCU and the SIU.

[43] The SAPS and the SARS are responsible for 75 percent of the requests made to FIC. It should be noted that SARS does not investigate ML stemming from criminal tax offenses but rather refers such cases to the SAPS.

indicated that, while it had approval for approximately 5,000 officers within its special investigative units, only about 2,000 of those positions were occupied as of the onsite.

151. In addition to responding to requests for information, the FIC also made 2,216 proactive disclosures to South African LEAs over the same time period (see Table 3.2). While fraud related crimes remain the dominant subject of the disclosures, the FIC's proactive disclosures of specifically ML and TF cases represent a significant higher percentage (39 percent) of the proactive disclosure than the requests (10 percent) from LEAs.[44]

152. The FIC receives feedback on disclosures from LEAs on a quarterly basis and proactively analyzes it to understand which products have resulted in investigations, prosecutions, administrative sanctions, or tax assessments. Statistics for FIC disclosures that have been closed by the LEAs without pursuing further investigation is also analyzed.

Table 3.2. South Africa: Proactive Disclosures made by the FIC to South African LEAs – Five Years to March 31, 2018

Crime Type	Number of Disclosures	Percentage of Total Disclosures
Fraud Related Crimes	607	27%
Tax Evasion	510	23%
Corruption	98	4%
Drug Related Crimes	92	4%
Environmental Crimes	43	2%
Robbery & Theft	16	1%
ML	521	24%
TF	329	15%
Total	2,216	100%

153. In addition to the interactions with the FIC, SAPS also make use of financial intelligence gleaned from evidence obtained through the execution of s.205 subpoenas (see Table 3.3). Such intelligence will often result in new leads being identified prompting additional grounds to obtain further s.205 subpoenas. In more complex cases, this process can be repeated multiple times. While less efficient than obtaining information from the FIC, the step of securing court ready evidence from the financial intelligence is done concurrently.

[44] Due to joint operations and collaboration between the FIC and the SAPS, the FIC is aware of ongoing investigations. As such, a portion of these proactive disclosures relate to ongoing cases.

Table 3.3. South Africa: Section 205 Subpoenas Obtained by SAPS (2014–2018)

2014	2015	2016	2017	2018	Average
331	313	390	361	470	373

STRs received and requested by competent authorities

154. Each year FIC receives on average approximately 300,000 STRs, Suspicious Activity Reports[45], TF Transaction Reports (TFTRs) and TF Activity Reports (TFARs[46]). These reports, referred to as s.29 reports are mandated by the FIC Act. More than 95 percent of the reports are filed by two types of AI – banks and ADLA. Please see the following table:

Table 3.4. South Africa: Section 29 Reports Received by FIC from AIs and RIs (Six Years to March 31, 2019)

Year Ending March 31	2014	2015	2016	2017	2018	2019	Total	Average
STR	355,369	267,398	180,363	161,435	169,203	144,730	**1,278,498**	**213,083**
STRB Reports				136,722	77,702	71,818	**286,242**	**95,414**
STRB Transactions				2,040,190	258,264	172,204	**2,470,658**	**823,553**
Suspicious Activity Reports				60,237	83,709	71,696	**215,642**	**71,881**
TFAR				11	15	30	**56**	**19**
TFTR				7	10	160	**177**	**59**
TOTAL Section.29	**355,369**	**267,398**	**180,363**	**358,412**	**330,639**	**288,434**	**1,780,615**	**296,769**

Source: The FIC
1: The average total value of STRs filed in each of the last three years is around R300 billion ($20.4 billion).
2: STRBs are batch reports.

155. FIC indicated that, while the volume of reports may be trending down, the quality of reports, particularly from banks, has increased during this period following feedback to reporting entities on the quality of the STRs and a reduction in defensive reporting. FIC has also noticed an increase in the quality of the rationales provided by reporting entities with respect to the grounds

[45] Suspicious Activity Reports are intended to be filed when there is suspicious activity conducted by the client, but which is not linked to an actual transaction, such as an attempted transaction. The FIC authorities indicated that there is ongoing feedback to AIs and RIs with respect to the reports as many of them still detail actual transactions.

[46] Like suspicious activity reports, TFARs are intended to be filed when there is suspicious activity conducted by the client related to TF, but which is not linked to an actual transaction.

for suspicion documented in the STRs following FIC's outreach efforts to improve this aspect of the reports. FIC created mandatory fields in the reports to address key fields of data that were sometimes blank and since 2017, engaged with AIs at the operational level through 22 individual roadshows to improve reporting. FIC indicated however, that incomplete STRs are returned to the RE and do not form part of FIC's financial intelligence holdings until and unless they are returned completed. In addition, following 19 training sessions by FIC and SAPS:DPCI – CATS with FIs, FIC noticed an improvement in reporting related to TFARs and TFTRs.

156. In addition, FIC receives more than five million CTRs and two million CTRAs annually. A CTR must be filed when a cash transaction exceeds R24,999 ($1,700) and a CTRA must be filed if the aggregate total of cash transactions in a 24-hour period exceeds R24,999 ($1,700). These reports have proven valuable to FIC analysts for two main reasons. Firstly, as represented in **Error! R eference source not found.**, these types of reports are often included in the cases disclosed to LEAs; and, secondly, as a prescribed report received by the FIC, FIC analysts are authorized to follow up with AIs and RIs on the subjects of any prescribed report in order to gather additional financial intelligence relating to them and their accounts.

Table 3.5. Section 28 Reports Received by the FIC from AIs and RIs (2014 to 2019)

Year Ending March 31	2014	2015	2016	2017	2018	2019	Total	Average
CTR (million)	6.1	6.7	9.3	2.6	2.7	2.6	**30**	**5.0**
CTRA (million)				2.1	2.1	2.6	**6.8**	**2.3**
Total Section 28 (million)	6.1	6.7	9.3	4.7	4.8	5.2	**36.8**	**6.1**
Reports Disclosed	5,873	6,188	27,310	4,577	83,709	21,707	**149, 364**	**24, 894**

157. While the FIC has a rich source of obligatory reports to draw from for its analysis, there are some notable and important gaps. A few sectors including risky DNFBPs (such as most DPMS) still fall outside the AML/CFT regulatory framework (see section on ML/TF Risks and Context) and thus have not been filing STRs with the FIC. For more information of STR reporting of DNFBPs see section on Preventative Measures. In addition, the FIC does not receive, on a proactive basis, reports from the SARS regarding the cash declaration system at South Africa's various border control points.

158. While VASPs currently fall outside the AML/CFT framework, South African authorities indicate that the larger VA exchanges have provided STRs, TFARs, and TFTRs, as well as voluntarily provided CTRs and CTRAs. Some of the reports have already been included in the FIC's analysis and currently form intelligence in ongoing cases.

159. The FIC makes extensive use of its authority to request additional information from AIs and RIs regarding the reports that have been submitted including prescribed information relating to transactional activity and supporting documentation. Such use enhances its analysis and in so doing provides additional intelligence to South Africa's competent authorities. In the last three years the FIC compelled AIs or RIs 96,995 times to advise it if certain subjects of its analysis have

accounts with the AI or RI.[47] In addition, the FIC gathered additional information from AIs or RIs 9,563 times on subjects which had been the subject of an obligatory report filed by the AI.

160. The FIC accesses a variety of non-transactional information from government and commercial databases when developing financial analysis. While the FIC can, by way of written request, obtain information related to a subject's criminal record or related firearms registry information, it does not have direct access to basic police databases that would assist them in identifying the relevance of, and to prioritize, the STRs that they receive.

Operational needs supported by FIU analysis and dissemination

161. The FIC responds to requests for information from LEAs as well as making proactive disclosures to LEAs based on their own analysis of reports from AIs and RIs. While the statistics over the past five years indicate that disclosures from the FIC are 77 percent reactive (responding to requests from LEAs) versus 23 percent proactive (self-generated by the FIC), the FIC is working with LEAs, and on its own detection systems and models, to increase the number of proactive financial intelligence products it provides to LEAs to identify ML/TF specific cases.

162. The SAPS, the largest recipient of the FIC's proactive disclosures (46 percent), indicated that these disclosures were less useful than the responses they received from their own requests as it was often difficult to know what crime the transactions, contained in the proactive disclosure, related to. Approximately five percent of these disclosures lead to new investigations while others related to ongoing investigations that FIC was already aware of.

163. The FIC's average response time for requests for information from LEAs in around seven weeks (see Table 3.6). In complex matters the FIC often provides a preliminary report to ensure usefulness and timeliness of the provision of financial intelligence. The FIC will then continue with its analysis before disclosing a more comprehensive report. In addition, the FIC conducts in-person briefing sessions with LEAs on sensitive and complex matters to explain the disclosure provided to LEAs. This process helps to clarify any possible misunderstandings on the value and usefulness of the information disseminated.

[47] Enquiries in terms of S.27 of the FIC Act are sent to AIs for all ML/TF cases the FIC processes to determine: i) whether a specified person is or has been a; ii) whether a specified person is acting or has acted on behalf of any client; iii) whether a client is acting or has acted for a specified person; iv) whether a number specified by the FIC (for example, a bank account number) was allocated to a person with whom that institution has or has had a business relationship; or v) on the type and status of a business relationship with a client.

This information often assists the SAPS in drafting of subpoenas for bank statements or other financial information from institutions, to identify additional persons or entities linked to a subject, or account number, or in the understanding of a subject's financial landscape when tracing funds.

Table 3.6. Intelligence Requests Made to the FIC by South African LEAs – Five Years to March 31, 2018

Year	2014	2015	2016	2017	2018	Average
Number of domestic requests received	1,695	1,626	1,776	1,904	1,876	1,775
Number granted	1,695	1,626	1,776	1,878	1,840	1,763
Average working days to respond	40	21	35	35	47	36

164. The FIC has a strong working relationship with South African LEAs. Major investigations often involve a task team, where a FIC analyst will be assigned to assist with the investigation by providing ongoing financial intelligence. The involvement of FIC analysts on investigative teams is a strong indicator of how the FIC analysis and dissemination (real-time) supports the operational needs of competent authorities (e.g. see Box 1.1).

Box 1.1. Krejcir Case Study – Predicate Crime and Asset Recovery

The FIC received requests for financial intelligence relating to three projects concerning criminal syndicates involved in offenses including gold smuggling, murder, drug smuggling, assault, fraud, vehicle cloning, tax evasion, and customs related offenses.

The FIC conducted analysis on different accounts using transactional data, regulatory reports, person profiles, property and vehicle databases, company, and intellectual property searches along with various other databases that it has access to. Upon completion of the initial base line analysis, FIC discovered that certain suspects of the different projects overlapped and were involved in different stages of the financial flows and the evidentiary transactions identified.

The FIC disclosed its analysis to a multi-agency task force with members from the SARS, the DPCI, the SSA, and the NPA. The task force used the financial intelligence in the course of its investigation to identify evidence of predicate offenses and to trace proceeds of crime. The investigation led to the successful prosecutions of numerous members of the criminal syndicates and the recovery of proceeds of crime and offense related property (i.e., cash, vehicles, boats, firearms, custom seizures, & stolen property) valued around R 288 million ($19.6 million).

165. The FIC has exercised its power to live monitor suspect accounts related to terrorism on numerous occasions, including during active investigations (see Table 3.7).

Table 3.7. South Africa: Section 35 Monitoring Orders: Terrorism & TF Investigative Inquiries—Six Years to March 31, 2019

Year Ending March 31	2014	2015	2016	2017	2018	2019	Total	Average
Number of Orders Issued	4	63	16	16	10	1	110	18
Number of Accounts Linked	27	105	46	67	20	3	268	45
Number of Cases Linked	2	8	4	5	3	1	23	4

Note: These figures are inclusive of extensions and amendments to existing orders. The spike in orders in 2015 is due to an initiative that focused on the FTF phenomenon and lasted a few years.

166. Financial intelligence obtained from the FIC has led to the freezing and eventual forfeiture of the amounts of proceeds of crime set out in Table 3.8. See also section 3.4.

Table 3.8. South Africa: Feedback on Requests: NPA:AFU Five Years – April 1, 2014 to March 31, 2019

Year Ending March 31	2015	2016	2017	2018	2019	Total
Cases	39	48	34	16	13	150
Amount Restrained or Frozen (R million)	R 1,927	R 49.2	R 205	R 2,290	R 2,001	R 6,472
Amount Restrained or Frozen ($ million)	$ 131	$ 3.3	$ 13.9	$ 155.7	$ 136.1	$ 440.1

167. The FIC produces a variety of reports for both internal and external consumption, with the majority designed to contribute to raising awareness of ML/TF issues among the general public,[48] reporting entities and to support internal operations. There are two reports produced by the FIC that do have a more operational focus as follows:

- **NICOC Estimates:** The FIC provides strategic inputs on ML and TF related topics to NICOC's National Intelligence Estimate.
- **Geographical Information System (GIS) Reports:** The FIC produces quarterly and annual GIS reports which provide a breakdown of all reactive reports (i.e. domestic and international requests for information) and proactive reports (i.e. referrals submitted to local LEAs). The reports provide information on the location of requesting and receiving agencies for FIC's products. The reports are used by the FIC when engaging with local LEAs to highlight geographical areas where better utilization of financial intelligence might be possible, but they are not proactively and routinely shared with LEAs.

[48] FIC's website contains high level typologies reports on different topics aimed at REs and the general public. FIC claims that these reports also benefit LEAs, however they are generally one page in length and lack any in-depth analysis. The assessment team does not consider these public reports as effective tools in supporting the operational needs of LEAs.

168. While most of the reports have obvious value to the FIC executives the utility of such reports in supporting the operational needs of competent authorities is less clear. The GIS Quarterly and Annual Reports, which are the only strategic intelligence produced, do contain operational information but are not proactively shared with LEAs.

Cooperation and exchange of information/financial intelligence

169. The FIC and the LEAs cooperate and exchange financial intelligence and other relevant information effectively to identify investigative leads, develop evidence in support of investigations, and trace criminal proceeds related to ML/TF and associated predicate offenses. Joint task teams, inclusive of the FIC are created to address specific types of cases. These committees or teams are operational in nature where financial intelligence is exchanged. Some of the teams currently in operation are as follows: the National Project Committee and Provincial Project Committees, which meet regularly to monitor and coordinate LEAs joint efforts in project driven investigations; the ACTT; the National Coordinating Strategic Management Team (on illegal mining); the Intelligence Working Group: Rhino Horn Smuggling; the CTFC; and the IFFTT.

170. Cooperation between FIC and LEAs along with the secure exchange of financial intelligence is effective. Operational intelligence is shared securely between the FIC and LEAs through the goAML encrypted email application, a secure file transfer protocol (SFTP) solution as well as through a dedicated encrypted email mailbox, using PKI.[49] The three mechanisms or applications are accessed through authentication protocols. There are MOUs in place to govern information sharing and each competent authority has an Authorized Officer to receive information from the FIC. All information is approved before dissemination and dedicated resources utilize a secure mechanism to disseminate information to competent authorities upon request and spontaneously.

171. The FIC utilizes the Egmont Group secure web (ESW) to securely disseminate information to other jurisdictions (FIUs) who are Egmont members. For non-Egmont members, security is achieved through the use of the same three mechanisms described earlier (goAML, SFTP and encrypted email using PKI).

C. Overall Conclusion on IO.6

172. The use of financial intelligence plays an important part in addressing predicate crimes, ML, TF, and the identification of criminal assets. The FIC obtains a large number of obligatory reports and possesses the tools and has access to additional information that allows it to analyze such reports and effectively produce operational financial intelligence. Given however, the identified risk pertaining to cash, particularly cross border transactions, the fact that the FIC not

[49] PKI stands for Public Key Infrastructure - a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.

routinely receiving reports on cash courier activity, and the low volume of reporting from high risk DNFBPs, significant gaps in financial intelligence exist.

173. The SAPS, the SARS and other competent authorities routinely use financial intelligence to mainly support their investigations and activities related to predicate crimes, and not on proactively identifying and supporting ML and TF cases. LEAs require additional skills and resources to more effectively use the information that is generated to conduct their financial investigations (see IO.7).

174. South Africa is rated as having a moderate level of effectiveness for IO.6.

D. Immediate Outcome 7 (ML investigation and Prosecution)

ML identification and Investigation

175. The authorities identify and investigate ML cases to some extent. Emphasis is placed on the investigation of predicate offenses. SAPS:DPCI is the main agency responsible for the investigation of ML offenses. PFIs are undertaken in all cases of serious organized crime, serious commercial crime, and serious corruption investigated by SAPS:DPCI. SAPS:DPCI pursues ML offenses disclosed during the investigation of predicate offenses. All matters are evaluated by the SAPS:DPCI – PCSI for ML potential and a basic financial investigation is conducted. It is the role of the financial investigator within SAPS:DPCI – PCSI to uncover ML from predicate offenses referred to it by other components of SAPS:DPCI. However, the authorities have not sufficiently demonstrated the proactive identification and investigation of ML in all cases. ML cases are largely identified and investigated based on evidence arising from the specific predicate offense, rather than a broader identification of ML activities and, in particular, major proceeds-generating offenses. Boxes 2 through 9 contain examples of some cases pursued.

176. SAPS:DPCI – PCSI became fully operational in 2012 and is responsible for ML investigation, asset investigation, cybercrime investigation, and a newly formed forensic accounting investigation section. The three SAPS:DPCI units investigating predicate crimes refer the investigation of those predicate offenses to SAPS:DPCI – PCSI to conduct a PFI. Both the criminal investigator and the SAPS:DPCI – PCSI members work together until the case is completed. South Africa adopts the principle of Prosecutor Guided Investigations (PGI) and prosecutors from the NPA are also engaged at an early stage to help guide the investigation. “Project teams” with other agencies, such as the FIC or the SARS, are formed to coordinate action on a regular basis.

177. Data provided by the authorities indicates the largest category of predicate offenses investigated by SAPS:DPCI by far is fraud, followed by participation in an organized criminal group and corruption or bribery, and to a lesser extent theft, counterfeiting and piracy of products, and tax crimes (see Table 3.9). This is somewhat consistent with risk exposure. A number of these investigations lead to prosecutions where the offense of ML is charged in addition to the predicate offense.

Table 3.9. South Africa: SAPS:DPCI Predicate Offense Investigation Activity Resulting in ML Charge – Jan 1, 2014 to Dec 31, 2017

Predicate Crime Type	Reported to SAPS:DPCI	Investigated by SAPS:DPCI	Percent of total	Referred for Prosecution	Prosecuted for ML	Percent of total	% of referred prosecuted for ML
Fraud	8,404	5,350	60%	740	240	23%	32%
Corruption & bribery	1,663	1,334	15%	722	18	22%	2%
Theft	836	589	7%	159	39	5%	25%
Counterfeiting & product piracy	612	468	5%	280	0	9%	0%
Tax crimes	607	229	3%	33	8	1%	24%
Drug Trafficking	259	220	2%	182	5	6%	3%
Piracy (movies and music)	362	184	2%	114	0	4%	0%
Forgery	97	81	1%	47	4	1%	9%
Environmental crime	61	61	1%	74	8	2%	11%
Human Trafficking	52	52	1%	30	2	1%	7%
All Others	363	324	4%	173	14	7%	8%
Less Multiple Charges Laid					16		
Total	**13,283**	**8,892**	**100%**	**2,554**	**322**	**100%**	**13%**

Source: The SAPS:DPCI and the NPA
Note: All but two prosecuted cases resulted in convictions

178. In practice, the FIC plays a significant role in identifying and tracing the flow of funds during the PFI of the predicate offenses which are investigated by SAPS:DPCI. FIC obtains information from financial institutions to "follow the money" under powers to request whether accounts of persons or entities are held by financial institutions (FIC Act, s.27), to request provision of specific account information (FIC Act, s.32) and to freeze accounts for up to 10 working days (FIC Act, s.34). FIC shares the information it obtains from the financial institutions and analyzes it to trace the fund flows for use both by LEAs and the NPA:AFU. The information is provided to SAPS:DPCI which collects the evidence under its subpoena powers (CPA s.205) for use in court to support criminal charges.

179. SAPS:DPCI – PCSI identifies and investigates fund flows to some extent based upon its own analysis of transactions and other sources of information including from SAPS:CI. SAPS:DPCI –

PCSI has recently formed a forensic accounting investigation section to strengthen its in-house capacity to conduct financial investigations, particularly in more complex cases, but the section is not yet operational. To date SAPS:DPCI – PCSI has relied upon engagement of outside forensic accounting firms when necessary to assist in complex financial investigations. The lack of in-house forensic accounting expertise means SAPS:DPCI – PCSI to a large extent focuses on collection of evidence to prove fund flows identified by FIC or by other means to prove the predicate offense.

Box 2.1. Case Example – Procurement Fraud

A whistle blower exposed procurement fraud irregularities at the Western Cape offices of an SOE, Eskom (the national electricity supplier). The accused, an Eskom employee and a managing director of one of its subsidiaries, sought to procure an unfair advantage for himself and a company he set up to take over the operational contracts from the subsidiary and Eskom at a stage when the subsidiary's operations were being absorbed by Eskom. The accused set up a scheme to move the proceeds between company accounts and a trust ostensibly to pay dividends to employees. The ML was uncovered by the PFI and use of FIC profiling of the employee. The financial analysis by SAPS:DPCI – PCSI showed the inter-account movement of monies especially in respect of interest- bearing accounts did not accord with business practice and that the dividends paid out did not reflect shareholding as claimed. The legal entity charged was sentenced to a fine whereas the accused received a sentence of 15 years for fraud and 10 years for ML. The sentences were ordered to run concurrently. The NPA:AFU obtained a restraint of R10.5 million ($714,000) in the matter (the case is pending appeal).

Box 3.1. Case Example – Abalone

Abalone was seized during search and seizure operations and the accused arrested. Documents seized at another location indicated raw plastic had been purchased and was being exported to China. Further investigation revealed that more plastic had been purchased than was being exported. After consultations with the SARS:Customs and the shipping line concerned, a stop order was placed on two containers still en route to China and the containers were re-routed back to Cape Town. Dried abalone was found hidden inside the plastic bales. As a result of investigations into the predicate offending, ML charges were developed and pursued. Five accused were convicted of ML including a legal entity. Three accused were sentenced to one year's imprisonment, another accused was sentenced to 8 years imprisonment (with three years suspended) and the legal entity was fined R200,000 ($13,600) (suspended for five years).

180. The authorities acknowledged that the potential cases of ML which are identified, and most ML investigations are directly linked to the investigation of the predicate offense. In the assessors' view, less emphasis is placed by SAPS:DPCI on the proactive identification and investigation of ML cases, and the networks and professional enablers behind or linked to the predicate offense. This gap may be remedied in part when the forensics accounting investigation unit within SAPS:DPCI -PCSI, which has already been established, becomes operational and develops a capacity to focus proactively on ML cases, and to identify and investigate third-party ML, professional enablers and ML networks related to the predicate offense. It is also worth noting that while SAPS:DPCI focused on around 250 serious drug trafficking or dealing cases over the period 2014–17; over the same period there were nearly 40,000 total such cases (out of more than 1 million drug crimes), indicating that investigating ML related to drug dealing is not receiving sufficient

attention by the authorities overall although not all of these cases involve high level drug dealing generating significant proceeds.

181. ML investigations conducted by SAPS:DPCI therefore appear to be largely reactive and form part and parcel of the investigation of the predicate offense. Most of the predicate offenses (including offenses against the person such as kidnapping) are major crime proceeds generating offenses which necessarily entail ML activity. Many of the ML cases charged are cases of self-laundering which are prosecuted in conjunction with the predicate offense. The ML aspect charged is frequently the immediate dealing in the proceeds of the predicate offense committed by the defendant or a close associate. The evidence developed by the PFI to prove the predicate offense and related confiscation or forfeiture applications is thus largely the same evidence used for the ML offense, and the ML charge necessarily follows the charge for the predicate offense. As a result of this narrow focus on predicate offenses, the authorities have not been effective in dealing with wider ML activities including third party ML.

182. The authorities provided Table 3.10 below for the overall number of PFIs or ML investigations conducted by SAPS:DPCI-PCSI. Based on this information, it appears that, on average, about 15 percent of the cases they investigate for ML result in ML prosecutions.

Table 3.10. South Africa: Number of ML Investigations, Prosecutions, and Convictions—Five Years to March 31, 2019

Year Ending March 31	2015	2016	2017	2018	2019	Average
Number of ML investigations	358	502	457	418	271	401
Number of ML Prosecutions (Cases)	51	43	59	67	76	59
Number of ML Convictions (Cases)	51	43	59	67	76	59
Percentage of investigations lead to convictions (Cases)	14%	9%	13%	16%	28%	15%
Number of Persons Convicted for ML, of which:	71	71	96	87	116	88
For Foreign Predicates	2	-	2	1	-	1
For legal persons	2	1	3	3	2	2
For self ML	47	50	46	51	73	53
For stand-alone ML	22	20	45	33	41	32

Source: The SAPS:DPCI – PCSI
1: Annual data have been aligned throughout the report by matching all calendar year data to the March 31 year immediately following.
2: Authorities shared 322 cases where ML charges were laid with a total of 516 natural and legal persons convicted. Some of the cases pre- and post-dated the data in this table.

183. The SARS investigates tax and customs offenses. Once the criminal investigation is concluded, the case is referred to the SAPS and the NPA who may add charges such as ML. Based on a review of data provided by the authorities, there have been some but not many ML cases investigated and prosecuted based on tax fraud or customs offenses.

184. The SARS is also obliged to report AML/CFT information it comes across during investigations to the FIC (FIC Act, s.36) or to share information with other relevant LEAs (POCA, ss. 71 and 73). The initial referral of the criminal investigation to SAPS is for the purpose of obtaining a case number and for the assignment of a SAPS investigator to pursue the case and possible additional offenses outside the purview of the SARS and for the purpose of the NPA making a decision to prosecute. A senior SARS official must authorize the laying of a criminal complaint with SAPS whether the offense constitutes a non-compliance offense or a serious tax offense and when an offense concerns a customs offense. The NPA decides if a prosecution should be instituted and for what offenses, which depending on the facts of the case may go beyond tax offenses. If elements of ML are identified, the NPA may work with SAPS:DPCI to prepare the ML case for court.

185. Thus, the SARS does not have a mandate to actively investigate ML cases. In the years ending March 31, for 2017, 2018, and 2019, the SARS referred 660, 500, and 468 tax offenses to the NPA for prosecution respectively. These offenses mainly involved failing to submit tax returns but also involved some tax fraud matters which generate proceeds.

186. The SIU investigates serious malpractices or maladministration in the administration of the State as well as any conduct which may seriously harm the interests of the public, and institutes civil proceedings in court or a Special Tribunal to recover the value of losses incurred. SIU does not investigate ML cases but passes findings of possible criminal offending including corruption and potential ML to the NPA to follow up in conjunction with the SAPS:DPCI. Cases referred to the NPA by the SIU have not been expeditiously investigated and prosecuted in the past, although the authorities report the situation has recently improved due to the signing of an MOU between the NPA and the SIU.

187. The SIU may obtain court orders to recover any wrongful benefits or monies which were intended for the State. Relief sought includes declarations of invalidity followed by orders for just and equitable relief, reviews of administrative decisions and claims for restitution, and action for recovery of losses. It may also work with State institutions to cancel contracts or stop transactions or other actions that were not properly authorized. SIU obtains information from FIC and financial institutions during financial investigations within its mandate.

188. Despite some successful recovery efforts (see IO8), SIU also has a backlog of recovery cases pending in civil litigation process before the courts. Special Tribunals have recently been made operational to help address the problem and expedite the handling of these civil cases. The NPA has also been allocated with more resources in recent budget allocations to help address the issue of the past backlog of criminal referrals by SIU.

Consistency of ML Investigations and Prosecutions with Threats and Risk Profile, and National AML Policies

189. South Africa has achieved a good level of prosecution for the ML offense in terms of the number of convictions. During the last five years the authorities have achieved over 300 convictions for the ML offense. The conviction rate for all crime prosecuted in South Africa is high, at

over 90 percent of cases prosecuted; and nearly 100 percent for ML cases. Most ML cases investigated and prosecuted relate to the predicate offense of fraud, which is somewhat consistent with South Africa's threat and risk profile. There have been fewer prosecutions relating to ML in other high-risk areas such as corruption and bribery, narcotics, and tax offenses. The time taken to litigate and resolve cases is lengthy in many cases.

190. Table 3.9 illustrates the types of ML cases involving predicate offenses investigated and referred for prosecution and prosecuted during the relevant period. Table 3.10 shows the overall number of ML investigations resulting in prosecution. Whilst the conviction rate is high for ML cases prosecuted, the number of ML cases prosecuted from the referrals made is relatively low averaging 15 percent. Taken with the high conviction rate for ML prosecutions, the data suggest that only the obvious cases of ML are being prosecuted. The authorities acknowledge that weakened institutional capacity through *"State capture"* seriously impacted their ability to investigate and prosecute serious corruption and ML and led to the loss of key personnel in LEAs and the freezing on hiring new staff. New heads of the NPA, the SAPS:DPCI, and the SARS have recently been appointed to address the issues arising from *"State capture"* and to focus efforts on rebuilding institutional integrity and capacity in these agencies. Despite the challenges linked to *"State capture"*, the authorities still managed to investigate and secure convictions in ML cases as shown in the number of cases prosecuted.

191. The Investigating Director of NPA:ID was appointed in May 2019. The establishment of NPA:ID is further indication of the commitment by South Africa to address issues arising from major high-profile corruption cases impacting the integrity of state institutions and SOEs. It is too early to assess the effectiveness of the work of the NPA:ID.

192. The NPA and SAPS:DPCI utilize the methodology of PGI in terms of which the prosecutor and the investigator work together from the start through a system of case planning and follow-up meetings. They work as a team, but the prosecutor guides the investigation. The NPA has prioritized the prosecution of ML cases and set up a ML Desk whose objective is to improve the ability of prosecutors to identify and prosecute ML cases thereby increasing the number of cases finalized where ML charges are preferred.

Box 4.1. Case Example – Illegal Mining

Illegal miners, known as Zama Zama's, can be highly organized and generate significant proceeds. Mine Security conducted an underground operation to arrest illegal miners. 21 accused persons all surfaced to ground level over a period of four months, from an unused level of the mine. During the underground investigations, 16 illegal gold processing plants were discovered and processed gold to the value of R120 million ($8.2 million) was given back to the legal mine on whose premises these activities were conducted. The State utilized cell phone evidence and analyzed 3,500 documents found underground, which indicated the miners sold approximately R6.2 million ($421,600) of refined gold to smelters or other buyers and received money which was written on either a credit book or paid over to certain identified persons. The monies so derived were used by the accused to fund their stay underground and it is believed the rest of the monies were transmitted to their families in neighboring countries. Accused person 22 resided on the surface and together with accused person one laundered the money, including for the purchase of a house registered in her name. The accused were prosecuted and found guilty in June 2016 on a total of 577 charges relating to racketeering, theft of gold bearing material to the value of R120 million ($8.2 million), ML, possession or disposal of unwrought gold bearing material, transport of unwrought gold bearing material, and being in the country illegally. All 22 accused were sentenced to 15 years imprisonment that included a concurrent sentence of 13 years for those also convicted of ML. The house was forfeited to the NPA:AFU

Box 5.1. Case Example—VAT Fraud

The accused registered 18 companies for VAT with the SARS and were allocated VAT numbers. The companies initially traded but ceased to trade and thereafter solely existed for purposes of claiming fraudulent VAT refunds from the SARS. VAT refunds in the amount of R216 million ($14.7 million) were claimed, of which R148 million ($10.1 million) was paid out to the companies. The case came to light when the SARS did an audit on one of the entities. Through this audit, they established that the export and import documents supplied by the entity were false. Further investigation established that this entity was linked with the other 17 entities, because the same person submitted the VAT returns. The SARS obtained the company documents from the CIPC and established that the accused were directors of all 18 entities. The bank accounts and opening documents were subpoenaed with the assistance of the SAPS:DPCI and established that three accused had signing powers on these accounts. The SARS did a forensic investigation on the flow of the monies and established that the accused transferred the monies from one entity account to another, and within a month withdrew the bulk of the monies in cash. They purchased property, paid investments, and paid credit card instalments. The charges preferred against the accused were fraud, forgery, uttering and 78 counts of ML. On the ML charges, the accused were sentenced to 20 years imprisonment and for the other offenses to 25 years imprisonment.

193. In the most recent national budget allocation by Treasury, NPA funding has been significantly increased to allow for the injection of additional resources and the hiring of additional prosecutors. This is a positive sign and will assist in efforts to tackle cases, including ML cases, relating to *"State capture"* which have not been sufficiently pursued to date, as well as cases referred to the NPA by the SIU which have not been dealt with expeditiously. As noted, the new NPA:ID will also assist in this work and there are positive signs emerging that consolidated efforts are now underway to address high level corruption in the public sector. These types of cases, however, take time to investigate and prosecute and are often dependent upon international cooperation to obtain evidence or to trace property which has moved offshore. It is too early to assess the effectiveness of these efforts.

194. In the view of the assessors, ML prosecutions are only being pursued to a limited extent for other high-risk offenses that generate significant proceeds such as VAT fraud. South Africa is also a transit and destination country for narcotics, with large scale manufacturing and distribution of drugs for domestic use, yet PFI and ML investigations into drug dealing are low relative to the level of activity. The narcotics trade is also linked to other crimes such as wildlife trafficking, including abalone and rhino poaching, and sometimes corruption involving law enforcement officials at land border points. The lack of ML prosecutions for foreign corruption predicate offending is also inconsistent with South Africa's risk profile as a financial hub for a region with known corruption issues. Overall, despite the good number of ML cases being prosecuted and convictions obtained, ML investigations and prosecutions are not consistent with the size of these threats and risks.

195. The authorities have acknowledged challenges due to the length of time taken to investigate and conclude successful ML prosecutions. The NPA has suffered from serious resource deficiencies and shortages of prosecutors in recent years which has impacted operational capabilities. The challenges are partly attributable to lack of resources and the availability of relevant skill sets, particularly in forensic accounting, as well as the litigious nature of defendants resulting in lengthy court proceedings in many cases.

Types of ML cases Pursued

196. As shown in Error! Reference source not found.**, ML prosecutions mostly concern cases of s elf-laundering based on the predicate offending, which is often prosecuted at the same time.** Standalone ML cases are prosecuted, but there are no third-party ML cases and only a few for ML arising from foreign predicates. This appears to be a consequence of the focus on investigating of predicate offenses rather than identifying and investigating ML networks and professional enablers.

Table 3.11. South Africa: South Africa: ML Convictions—Number of Natural People Convicted – Five Years ending March 31, 2019

Year Ending March 31	2015	2016	2017	2018	2019	Average	Percent
Total Convicted	69	70	93	84	114	86	
For Self-laundering	47	50	46	51	73	53	63%
For Stand-alone	22	20	45	33	41	32	37%

Note: Totals for 2016/17 do not add due to a minor discrepancy in data provided.

197. The authorities noted that an attorney was involved in one case as a third-party launderer but claims to legal privilege proved a challenge during investigation and prosecution. The authorities also acknowledged that they struggle to investigate and prosecute cases of stand-alone and third-party ML. The necessary legislation is in place to tackle such activities; however, the problem appears to lie with lack of resources and expertise available to LEAs and the NPA to proactively identify the networks and ML syndicates operating behind the predicate offense which they do investigate and prosecute, which often have overseas links. Most ML cases

focus on the first level of offending involving dealing in the proceeds of the offense directly by the offender or immediate associates, rather than by the deeper layers and networks operating behind such activity.

198. The authorities did evidence some investigations taken for foreign requests for assistance involving proceeds of crime located in South Africa and the investigation of ML relating to foreign predicates but did not sufficiently demonstrate that ML relating to foreign predicate offenses is being proactively investigated and prosecuted as a policy objective. In particular, they did not provide any ML cases relating to foreign corruption.

Effectiveness, Proportionality, and Dissuasiveness of Sanctions

199. South Africa has a high head sentence of 30 years' imprisonment for the ML offense and sentences of up to 25 years have been handed down in practice, which are dissuasive. There are no set guidelines or tariffs for the ML offense and the sentence is fixed by the court taking account of the circumstances of the defendant, the seriousness of the offense, and the community interest. The most serious offenses result in direct imprisonment, and in most cases the ML offense is linked to the predicate offense for sentencing purposes because the offenses are frequently prosecuted together. Sentences for the predicate offense and the ML offense may run fully or partly concurrent to each other.

200. In a number of cases, non-custodial and suspended sentences and fines are imposed, reflecting the less serious nature of the predicate offense or ML involved and evidencing some degree of proportionality in sentencing. If the ML offense is self-laundering, the court may suspend the sentence for the ML offense and base the sentence of imprisonment on the predicate offense. Due to the length of time taken to prosecute some offending, the time the defendant has spent in custody pending conclusion of the proceedings will also be deducted from the sentence of imprisonment to be served.

201. Data provided by the authorities (see Table 3.12 below) evidence that suspended sentences are the prevalent sanction imposed for the ML offense and they outnumber cases where actual custodial sentences have been imposed. In addition, in about half the cases where the offender was convicted of both the predicate offense and the ML offense, the sentence for the ML offense was the same as the predicate offense (whether the sentence was suspended or not), and only exceeded the sentence for the predicate offense in around six percent of cases (which is rather surprising given the high head sentence available). This pattern indicates penalties for the ML offense do not add much to the penalties imposed for the predicate offending in cases of self-laundering. Overall, sanctions for ML convictions may only be considered effective to some extent.

202. Sanctions have been imposed against legal persons e.g. if an attorney is prosecuted, their law firm may also be charged. During the period under assessment, 11 legal persons were sentenced for ML offenses.

Box 6.1. Case Example—Corruption

The AgriBEE fund was a Parliament approved project administered by the Land Bank as an external agency on behalf of the national Department of Agriculture. The AgriBEE fund received R100 million ($6.8 million) to award as grants to previously disadvantaged individuals, for investment in equity (expansion of existing and rehabilitation of enterprises which are struggling financially) and in Small, Medium and Micro Enterprises within the Agricultural Sector with the focus on skills development and mentorship. A grant of R6 million ($408,000) was paid to an entity on the verbal instruction of the Chief Executive Officer (CEO) of Land Bank and the correct procedures were not followed in approving the said grant. Amongst the beneficiaries was the previous Chairperson of the Portfolio Committee on Agriculture in Parliament, who personally benefitted from the said grant. Three individuals were charged and sentenced as follows: former CEO of Land Bank – seven years imprisonment for fraud; Member of Parliament – 20 years imprisonment for fraud and ML; attorney – 24 years imprisonment for fraud and ML. The attorney's firm was also convicted of ML. An amount of R3.2 million ($217,600) was forfeited and paid to the Land Bank.

Table 3.12. South Africa: Sanctions Imposed for Persons Convicted of ML Only – March 2014 – October 2019

Description	Data
Number of persons convicted of ML only	154
Of which received suspended sentences	119
% Suspended	77%
Of which received non-custodial sentence	133
% Non-custodial	86%
Number receiving custodial sentences	21
Average years of imprisonment	7.6
Max years of imprisonment	20
< 2 years	2
2 to < 5 years	2
5 to < 10 years	11
10 to < 20 years	5
20 to 30 years	1

Use of Alternative Measures

203. South Africa does employ alternative criminal justice measures in ML cases as a policy goal and has a range of options when it is not possible to secure a ML conviction.

204. The NPA:AFU actively pursues asset recovery through civil forfeiture measures (see IO8). SIU also pursues recovery of State losses through its available remedies in civil litigation (see IO8). These processes work in parallel with the ML investigation and continue regardless of any criminal prosecution for the ML offense. The ML offense is considered in all cases investigated by SAPS:DPCI and the NPA will also consider charging persons for other offenses when the ML offense cannot be pursued. For example, in the case of cash seizures at border points where the money cannot be associated with a predicate offense, exchange control offenses may be preferred.

E. Overall conclusion on IO.7

205. ML activities, in particular major-proceeds generating offenses, are investigated, and prosecuted to some extent but only partly consistent with South Africa's risk profile. A reasonable number of convictions have been achieved; however, in most cases these flow directly from the prosecution of the predicate offense and frequently involve self-laundering. ML activities arising from *"State capture"* have not been effectively addressed to date. Wider ML activities by organized crime syndicates, including from outside South Africa, are not being sufficiently identified and targeted in the context of South Africa's role as a regional financial hub. Sanctions set by law are severe, but in practice non-custodial or suspended sentences are often imposed.

206. A focus on cases of self-laundering and the absence of cases of third party ML combined with the lack of concerted action against wider ML networks, as well as the overall impact of "*State capture*", weighs heavily against the reasonably good number of successful prosecutions and convictions for ML being achieved in South Africa.

207. South Africa is rated as having a moderate level of effectiveness for IO.7.

F. Immediate Outcome 8 (Confiscation)

Confiscation of Proceeds, Instrumentalities, and Property of Equivalent Value as a Policy Objective

208. South Africa has adopted a clear policy objective to pursue confiscation of proceeds of crime and this is reflected in the preamble to the POCA legislation itself. It was an early country to adopt procedures that provides for both conviction and non-conviction-based asset recovery for proceeds and the legislation has been used extensively. The POCA legal framework is well developed and has been tried and tested in South Africa's courts including the Constitutional Court. The NPA:AFU can restrain and confiscate the benefit derived by the accused from the offending following conviction but before sentence is imposed (POCA, ch.5). The confiscation order is a for value "money order" based on the assessed benefit the defendant has obtained from criminal activities and acts as a civil judgment. The NPA:AFU is empowered to preserve and forfeit proceeds of crime, instrumentalities of crime and terrorist related assets (POCA, ch.6). This is a civil procedure that is *sui generis*. The procedure is non-conviction based which means the NPA:AFU does not need to wait for a criminal conviction, and it can also undertake action when a decision is made not to prosecute an individual. The application targets the criminal assets and not the person, and the burden of proof required to prove the assets represent proceeds of crime is at a lower civil standard.

209. The POCA has been well-supported and implemented by the NPA:AFU since its establishment in 1999. The NPA:AFU operates as a separate business unit in the NPA headed by a National Deputy Director of Public Prosecutions and it has the sole mandate to perform asset forfeiture functions. The unit is therefore tasked with asset forfeiture throughout the country and maintains a presence in all the major seats of the High Court. The case law surrounding aspects of

asset forfeiture under the POCA has been thoroughly developed over the years and there are in excess of 600 court judgements dealing with a wide variety of principles such as the constitutionality of the asset forfeiture regime, specific legal principles, interpretation principles and process issues arising from the POCA.

210. This court tested and approved model has resulted in an asset forfeiture regime which is regularly used by the authorities and which can be effective in individual cases. Since its establishment in 1999, the NPA:AFU has completed 5,607 confiscations and forfeitures to the value of R8.35 billion ($568 million). The unit has completed 6,245 freezing orders (restraints and preservations) to the value of R16.5 billion ($1.1 billion). The unit has recovered R6.74 billion ($458 million) of which R5.68 billion ($386 million) was paid back (or assets returned) to victims and R1.05 billion ($71.4 million) was paid to the CARA (as at September 30, 2019).

Confiscation of Proceeds from Foreign and Domestic Predicates, and Proceeds Located Abroad

211. The authorities have demonstrated positive results for recovery of proceeds of crime, particularly in the area of fraud and economic crime including ML, and overall, the work and asset forfeiture mechanisms utilized by the NPA:AFU are recognized as being effective in practice. The NPA:AFU was nevertheless impacted by the phenomenon of *"State capture"* and loss of staff. The fact the State was captured meant the authorities were precluded from proceedings with a number of matters. Efforts for recovery of assets from *"State capture"* and proceeds which were moved to other countries have thus been less successful. Recent efforts by the authorities are beginning to show positive results in some major cases, but these efforts are still at the early stage and some difficulties are being encountered in securing international cooperation for recovery of assets. Less emphasis has been placed by the authorities on recovery of proceeds of crime from foreign predicates, and these cases tend be pursued in a reactive manner only e.g. when a MLA request is made by another country to recover the proceeds.

212. The NPA:AFU has a standard form guideline to be used by prosecutors and LEAs when deciding on a referral of a matter to the NPA:AFU. The factors for referral are: all offenses for profit of more than R15,000 ($1,020); corruption involving more than R5,000 ($340); any investigation where SAPS or another investigating agency has seized cash of more than R15,000 ($1,020); all drug dealing cases; other cases which could have a significant impact on crime, such as those involving syndicates; cases of unexplained wealth; and any other reason. The NPA:AFU uses a Case Intake and Allocation Committee to evaluate cases submitted and assess cases with asset recovery potential. The Committee allocates all new incoming cases to legal and investigative staff. It obtains and approves a case plan from the case team within 10 working days or longer if necessary.

213. The SAPS:DPCI – FAFI) has a mandate to trace proceeds of crime and identify instrumentalities and property of equivalent value, which supports the SAPS:DPCI operational environment. All matters investigated by SAPS:DPCI operational environment are referred to SAPS:DPCI – FAFI to determine asset forfeiture potential before referral to the asset investigators. The SAPS:DPCI – FAFI member completes the asset forfeiture investigation and refers the file to the

NPA:AFU for potential application to court for relevant orders. This process takes place in addition to NPA:AFU investigating its own matters using its own investigative capacity.

214. The FIC also works closely with the NPA:AFU and in appropriate cases will issue an order under the FIC Act, s.34 to prohibit a reporting entity from dealing in the property. This order lasts for 10 days, during which time the NPA:AFU prepares an ex parte application to court to obtain a restraint or preservation order. If a restraint order is obtained (under the POCA, ch.5), it will usually remain in effect until determination of the criminal charge. A confiscation order will then be made upon conviction of the accused. If a preservation order is obtained (under the POCA, ch.6), an *inter partes* return date is fixed by the court usually within 30 days to allow an opportunity for persons affected by the order to challenge the making of a final forfeiture order. Longstanding NPA:AFU experience indicates that in most cases the application for a forfeiture order under the POCA, ch.6, is not opposed. This is in part because the affected party must demonstrate how the property came to be lawfully obtained, and South African courts have rejected arguments that such required explanations breach a potential defendant's right against self-incrimination.

215. Restraints in terms of the POCA, ch.5, are optional and are only done when there is a risk of the assets being dissipated. Ch.6 preservations are a requirement before a forfeiture can be obtained. The NPA:AFU demonstrated the ability to act expeditiously and successfully to recover assets particularly under the POCA, ch.6, procedures, including in cases of VAs. It is also beginning to focus its efforts on major cases arising from *"State capture"* and has managed to obtain some significant recoveries in 2018–2019.

Box 7.1. Case Example—Virtual Assets

The perpetrators located in Namibia managed to hack into the bank accounts of two Namibian victims. The money was transferred to a fraudulently opened South African bank account in the amount of N$750,000 and N$500,000 respectively. The case was referred to the NPA:AFU on September 22, 2017. The perpetrators created trading accounts with Altcoin Trader, a Virtual Currency Service Provider registered, and conducting business in South Africa. Two trading accounts were created fraudulently using the credentials of two Namibian citizens. The money transferred to the bank account in South Africa was used to buy Bitcoin, Bitcoin Cash, and Ripple crypto currencies on the Altcoin Trader platform. One Crypto Wallet was created for each of the accounts. By the time the fraud was discovered one wallet was already transferred from the Altcoin Trader platform. FIC instructed Altcoin Trader not to proceed with the transfer of the other wallet in terms of the FIC Act, s.34. The NPA:AFU obtained a preservation order to the value of R343,000 ($23,300) on October 5, 2017 and a forfeiture order for R954,356 ($64,900) on February 2, 2018 (the increase in value of the VAs over that period). An amount of R961,654 ($65,400) was recovered and repatriated to the victims on March 2, 2018.

Box 8.1. Case Example 1—"State Capture"

The Company X was one of the major actors in the *"State capture"* saga. As part of an agreement with Glencore International AG for the acquisition of Optimum Coal Holdings Proprietary Limited, Company X assumed control over the Optimum Mine Rehabilitation and Koornfontein Rehabilitation Trusts. All mines must reserve a portion of their profit in trust for the future rehabilitation of the mine and surrounding area. These funds may not be utilized for any other purpose. As soon as Company X bought the mines the rehabilitation funds were transferred to the Bank of Baroda (often mentioned in the *"State capture"* cases) in contravention of the Mineral and Petroleum Resources Development Act. The NPA:AFU made use of STRs and other reports submitted to the NPA:AFU by the FIC in preparation of the preservation and forfeiture applications and obtained a preservation order on March 8, 2018 to the value of R1.8 billion ($122.4 million). The matter was finalized on April 26, 2018 and R1.9 billion ($129.2 million) was paid to the NT.

Box 9.1. Case Example 2—"State Capture"

Eskom made unlawful payments to McKinsey and Company Africa Pty Ltd (McKinsey) in contravention of its procurements processes totaling R1 billion ($68 million) without a valid contract. The irregularities in the procurement process included criminal activity of monies paid for services that were not rendered. Several Eskom officials colluded with McKinsey to the benefit of McKinsey and to the detriment of Eskom. The NPA:AFU successfully obtained a preservation order in December 2017 for monies paid as proceeds of crime including ML. The preservation order was settled for R902,274,123 ($61.4 million) on July 31, 2018 and the monies paid back to Eskom.

216. South Africa adopts an "all offenses" approach to ML. This means that all cases where the NPA:AFU undertakes restraints and confiscations in terms of ch.5 (conviction-based confiscation) or preservations and forfeitures in terms of ch.6 (non-conviction-based forfeiture) under the POCA are regarded as predicate offenses even though ML may or may not have been involved. Ch.6 POCA powers are being used effectively and in preference to ch.5 POCA powers where a criminal conviction is a prerequisite for confiscation.

217. The authorities demonstrated that a good level of successful actions and recoveries are being achieved. Table 3.13 shows total recoveries for ch.5 and ch.6 recoveries per financial year. There is a spike in the last year due to one or two of the first very significant recoveries involving *"State capture"*.

Table 3.13. South Africa: NPA:AFU POCA Activity – Five Years ending March 31, 2019

Year Ending March 31	2015	2016	2017	2018	2019	Average
Provisional Measures – Restraints and preservations						
Number	482	464	460	355	283	409
Value (R millions)	R 6,699.5	R 9,498.9	R10,292.9	R11,509.2	R15,889.4	R 10,777.9
Value ($ millions)	$ 525.1	$ 645.8	$ 771.9	$ 869.2	$ 1,034.6	$ 769.3
Average Value ($)	$ 1,089,377	$ 1,391,723	$ 1,678,141	$ 2,448,495	$ 3,655,868	$ 1,881,903
Confiscations and Forfeiture Orders						
Number	459	386	459	573	493	474
Value (R millions)	R 1,941.5	R 342.5	R 420.9	R 368.4	R 3,092.1	R 1,233.1
Value ($ millions)	$ 152.2	$ 3.3	$ 31.6	$ 7.8	$ 201.3	$ 87.2
Average Value ($)	$ 331,528	$ 60,322	$ 8,783	$ 48,557	$ 408,387	$ 184,045
Recoveries – incl. victim payments						
Number	571	427	568	649	645	572
Value (R millions)	R 1,705.6	R 446.6	R 221.1	R 293.4	R 3,046.7	R 1,142.7
Value ($)	$133.7	$ 30.4	$ 6.6	$ 22.2	$ 198.4	$ 80.2
Average Value ($)	$ 234,118	$ 71,107	$ 29,192	$ 34,139	$ 307,571	$ 140,267

Note: Large increase in recoveries in 2019 is from cases in Box 7 and 8.

218. The authorities also provided a breakdown of freezing (restraints and preservations) and confiscation/forfeiture action involving ML cases, where ML was either argued in main or in the alternative as a basis for seeking the orders – see **Error! Reference source not found.**.

Table 3.14. South Africa: NPA:AFU Activity Involving ML Related Cases—Five Years to March 31, 2019

Year Ending March 31	2015	2016	2017	2018	2019	Average
Average per provisional measure ($)	$ 983,339	$ 471,038	$2,146,286	$9,483,407	$ 197,184	$2,656,251
Average of Confiscation/Forfeiture Orders ($)	$ 1,358,849	$ 914,444	$1,339,081	$193,476	$10,336,242	$2,828,419
Average of recoveries ($)	$ 459,202	$2,308,480	$ 499,809	$299,162	$4,541,152	$1,621,561

Note: Analysis also indicates that, on average, the authorities recover around 8 percent of the value of the related proceeds in ML related cases, noting, of course, that recovery efforts for some cases are continuing.

219. The authorities have thus demonstrated effective and positive results for asset recovery in a wide variety of cases including fraud, economic crime, and ML. Efforts for the recovery of assets from *"State capture"* and proceeds which have been moved to other countries have been less successful to date and have only recently begun to be undertaken. This significant feature impacts on the quality and thus overall effectiveness of South Africa's asset recovery regime for the purpose of the current assessment. Recent efforts by the authorities to recover the proceeds of *"State capture"* which have moved offshore indicate they have encountered some difficulties in securing adequate cooperation from foreign jurisdictions. Resolution of these matters should be pursued through all available channels, whilst acknowledging that international cooperation by all parties concerned, including foreign jurisdictions, is essential to resolve this issue. South Africa should ensure sufficient resources are made available to the relevant authorities to achieve satisfactory outcomes.

220. Recovered property from proceeds of crime is well-managed by the NPA:AFU and routinely returned to victims including SOEs or is paid to the asset recovery fund. Reviewed data indicates the bulk of property recovered is returned to victims, with the small remainder paid to the asset recovery fund. Sharing of funds with foreign jurisdictions has been pursued in some cases, as per the table below, and whilst the authorities have demonstrated some recovery of proceeds arising from foreign predicate offenses this is not being achieved in a proactive manner consistent with South Africa's risk profile of being a regional financial hub for countries with known crime and corruption issues. The authorities have indicated that evidence from overseas jurisdictions to support such recovery action for foreign predicate offenses is not always available.

Table 3.15. South Africa: Cases Involving Funds Repatriated—Five Years to March 31, 2019

Year Ending March 31	2015	2016	2017	2018	2019	Average
Number	-	3	1	-	3	1.4
Value (R millions)	R 0	R 102.8	R 2.0	R 0	R 3.1	R 21.6
Value ($ millions)	$ 0	$ 6.9	$ 0.15	$ 0	$ 0.2	$ 1.5
Average Value ($ millions)	$ 0	$ 2.3	$ 0.15	$ 0	$ 0.07	$ 0.5
Countries		Nigeria, Eswatini	USA		Germany, USA	

221. The SIU also pursues recovery of State losses through its civil litigation remedies. Whilst it is not necessary to establish a link to criminal activity in these cases, SIU longstanding experience indicates that in most cases some form of fraudulent, corrupt, or other criminal activity is involved in these cases. Table 3.16 sets out the actual recoveries by SIU through civil litigation through entering into Acknowledgements of Debt, other civil litigation outcomes which represents actual recoveries:

Table 3.16. South Africa: SIU Recoveries through Civil Litigation—Six Years to March 31, 2019

Year Ending March 31	2014	2015	2016	2017	2018	2019	Total
Acknowledgement of Debt (R millions)	R 1.6	R 164.9	-	R 8.7	R 5.4	R 2.4	R 183.1
Civil Litigation (R millions)	R 23.7	R 35.5	R 43.5	R 24.8	R 97.9	R 38.6	R 225.5
NPA:AFU recoveries (R millions)	R 119.8						R 119.8
Total Recovered (R millions)	R 145.1	R 52.0	R 43.5	R 33.5	R103.4	R 2.4	R 379.9
Total Recovered ($ millions)	$11.4	$ 3.5	$ 3.3	$ 2.5	$ 6.7	$0.2	$27.6

222. The interdiction and recovery of cash proceeds of crime remains challenging. Authorities acknowledged that many offenders quickly convert their illicit proceeds to cash, which then becomes extremely difficult to trace. Cash is used by the criminal fraternity to maintain a lavish lifestyle for themselves and their immediate families and is spent on luxury items, such as jewelry, high value motor vehicles and property. Use of cash, including in cross-border context (see below), remains a high-risk area in South Africa that the authorities must address as a priority in the ML context.

Confiscation of Falsely or Undeclared Cross-Border Transaction of Currency/BNI

223. The authorities have not positively demonstrated that confiscation of falsely or undeclared cross-border movement of currency is being addressed and applied as an effective, proportionate, and dissuasive sanction despite the use of cash and cross-border movement thereof being assessed as high risk.

224. The SARS:Customs is the first line of control over the movement of goods across South African borders. The Enforcement Division within the SARS has a mandate to ensure compliance with tax, excise, and customs obligations, and to combat fraud. A recently established Illicit Economy Unit, operational since January 2019, focuses on serious non-compliance emanating from industries such as tobacco, gold, clothes, and textiles imports amongst others. Any person entering or leaving South Africa must declare all goods in their possession which are required to be declared, meaning those that are restricted or prohibited under any law (Customs and Excise (C&E) Act, s.15). "Goods" includes cash and under the Exchange Control Regulations, 1961 (ECR), which is the law prohibiting, restricting, or controlling goods, all persons entering or leaving South Africa must declare South African banknotes and foreign currency in their possession. The ECRs do not restrict or control incoming BNIs payable in foreign currency.

225. The authorities suspended the requirement to make a written declaration in respect of cash at border points in 2008. Currently they expect persons to make an oral declaration if they are carrying cash in excess of R25,000 ($1,700) or foreign currency exceeding $10,000 or equivalent. However, the assessors noted that this requirement is not well-advertised to travelers, thus impacting effectiveness. The SARS:Customs officers may search for and seize currency under the ECR

when travelers have South African banknotes in excess of R25,000 ($1,700) unless the traveler is going to a country with the CMA, when the foreign currency is not less or equal to what was declared upon arrival by the non-resident, and when the travelers does not have permission granted by the NT. Overall, the authorities rely on their powers under foreign exchange controls to regulate cross-border movement of cash. The primary focus of the authorities appears to be on outgoing movements of cash with little or less attention paid to incoming movements of cash.

226. Undeclared cross-border movements of significant amounts of cash appears prevalent in South African context. This is due in part to widespread cash use in South Africa's informal economy and in neighboring countries in the region and the widespread use of cash for foreign import and export of goods. Whilst the phenomenon of undeclared cash at land border points is reportedly prevalent, and sometimes occurs with the complicit involvement of border agents, the authorities indicated the largest movements of undeclared cash are made through airport border points, in particular through OR Tambo International Airport in Johannesburg with centers such as Dubai and Hong Kong as major destination points. Statistics confirmed that most interceptions of undeclared cash movements involved Dubai as the destination point. A total of 40 cash seizures by the SARS over five years from 2014 to 2019 does not match South Africa's risk profile for cash smuggling – see **Error! Reference source not found.**

227. Cash couriers intercepted upon departure are stopped including by use of trained dogs and taken to a secure room under camera for investigation purposes. A criminal investigation is opened, and the authorities have 48 hours within which to charge the person. The SARS:Customs informs the NPA:AFU and the FIC of the seizure and, if the person is charged, the person will appear in court. The NPA:AFU applies for a preservation order under the POCA to seize the cash followed by a forfeiture order, regardless of whether the person is prosecuted. According to the authorities, criminal investigations have led to 14 prosecutions for cash smuggling during the last five years. This does not appear to be a significant number of prosecutions in view of the reported size of the illicit activity and the fund flows involved. The authorities indicated that trends for cash smuggling have changed and it now often occurs between passengers during airport transits, so that intervention is difficult.

228. It is not easy to assess what proportion of illicit cross-border movement of cash may be linked to ML/TF. In South African context all illicit cash movements are liable to forfeiture as cash smuggling contrary to the ECR and a link to ML/TF activity or evidence is not necessary for seizure and confiscation purposes. **Error! Reference source not found.** represents the number and v alue of cash smuggling forfeitures made by the authorities and the NPA:AFU during the last five years. These figures are low in number and value in view of the reported size and frequency of the activity. The authorities also shared experiences indicating that many smugglers often confess to, or their travel patterns indicate, that they completed many successful smuggling journeys before being caught. South Africa should therefore expedite a review of the cash declaration system and implement a revised system which is effective in countering these widespread cash smuggling activities. This action should include the introduction of enhanced monitoring systems and increased resources for staff and monitoring.

Table 3.17. South Africa: SARS:Customs, Border Cash Seizures—Five Years to March 31, 2019

Year	2015	2016	2017	2018	2019	Total	Percent
Total Seizures	4	9	8	14	5	40	
Total Value (R)	R 89,292,379	R 28,499,097	R 19,053,371	R 55,026,433	R 23,175,912	R 215,047,192	
Total Value ($)	$6,998,422	$1,937,447	$ 1,428,955	$ 4,155,789	$ 1,509,057	$ 16,029,670	
Location							
Courier/Mail	R 242,379	R 97,945	R 2,400	R 35,875	R 212,931	R 591,530	0%
Border Posts	-	R 35,000	R 1,513,030	R 1,508,505	-	R 3,056,535	2%
Airports	R 242,379	R 97,945	R 2,400	R 35,875	R 212,931	R 591,530	0%
Airports – In	-	R 50,760	-	-	-	R 50,760	
Airports – Out	R 89,050,000	R 28,315,392	R 17,537,941	R 53,482,053	R 22,962,981	R 211,348,367	98%
Airports – Average	R 29,683,333	R 5,673,230	R 5,845,980	R 5,942,450	R5,740,745	R 8,808,297	
Airports – Average ($)	$ 2,326,475	$ 385,682	$ 438,434	$ 448,795	$ 373,798	$ 656,562	

1: Two-thirds of the seized currency is USD, 28 percent ZAR, and five percent GBP.
2: Ninety percent of outward seizures are headed for the United Arab Emirates, and four percent Hong Kong.

Consistency of Confiscation Results with ML/TF Risks and National AML/CFT Policies and Priorities

229. Confiscation of proceeds of crime partially reflects South Africa's ML/TF risk and national AML/CFT policies and priorities. Most tainted property recovered by the authorities stems from economic crime and fraud, as well as corruption. This is consistent with some identified high-risk predicate offenses in South Africa. The high volume and frequency of recoveries is also consistent with South Africa's policy to deprive criminals of the benefits of their crime under the POCA through cooperation between FIC, LEAs and the NPA:AFU to freeze and then confiscate or forfeit the property as a priority. The civil recovery regime under the POCA, ch.6, is particularly effective, having been well-established in law by the courts and well-implemented in practice. The SIU also has an established framework to pursue State losses through civil litigation and other remedies, and the recent operation of Special Tribunals to expedite these claims will add impetus to efforts consistent with AML/CFT policies.

230. Recovery of assets from the effects of *"State capture"* and the most egregious public sector corruption cases has been less successful to date, as well as recoveries from proceeds of narcotics and tax evasion. This outcome is not consistent with South Africa's ML risk. The authorities are fully aware that action needs to be taken to recover criminal assets that have been looted from

State entities and moved offshore and they appear fully committed to doing so. Requests for international cooperation have been made and are being pursued, but with difficulty in some cases. Overall, it is too early to measure the success of South Africa's action concerning *"State capture"* corruption recoveries despite the recent positive signs.

231. The interdiction and recovery of cash proceeds of crime remains challenging and results to date are not consistent with South Africa's ML/TF risks. This includes cash which is used widely within South Africa outside the formal economy and in cross-border context. The seizures for cash smuggling, whilst sizable in some individual cases, do not adequately reflect the volumes being smuggled and the risks remain high in both ML and TF context.

G. Overall Conclusion on IO.8

232. Criminals are being deprived of the proceeds and instrumentalities of their crimes to some extent. South Africa has a well-developed regime for the civil forfeiture of proceeds of crime which continues to achieve good results. However, to date the regime has not been used effectively for the most serious crimes arising from *"State capture"*, including proceeds which have moved outside South Africa to other countries. In addition, recovering the proceeds of criminal offenses occurring outside South Africa are not being sufficiently targeted taking account of South Africa's role as a regional financial hub. Criminal confiscation of proceeds of crime has been less effective overall. Cross-border movement of cash is prevalent and is not being adequately addressed.

233. The impact and non-recovery to date of the bulk of proceeds of crime from "*State capture*" as well as the prevalence of undetected cross-border movement of cash weighs heavily against the good results otherwise being achieved using civil forfeiture.

234. South Africa is rated as having a moderate level of effectiveness for IO.8.

TERRORIST FINANCING AND FINANCING OF PROLIFERATION

A. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 9

- While there is evidence of some investigative activity from an intelligence gathering perspective, the authorities take a conservative approach to classifying politically motivated acts of violence as terrorism resulting in a low number of official terrorism and TF investigations and prosecutions. This may be partly linked to technical deficiencies in the TF offense. South Africa has failed to demonstrate that they are effectively identifying the specific roles played by terrorist financiers.

- South Africa has limited experience prosecuting TF offenses. The authorities are prosecuting one case of TF and investigating three other potential cases. There have been no other prosecutions in the past five years with only one person convicted of TF in March 2013 for attacks which took place in 2010.

- A single person convicted on two counts of TF since the last ME is not consistent with South Africa's TF risk profile. The authorities indicate that domestic terrorism risk is low but, while they are still developing their assessment of TF risks, they have identified significant risks such as international terrorist groups soliciting support within the country, and having FTFs, which suggests that the number of prosecutions for TF should be much higher.

- South Africa takes a collaborative approach to TF cases. The CTFC meets regularly to discuss ongoing cases, including potential TF cases. LEAs follow up on TF related proactive disclosures from the FIC and during their inquiries make numerous requests of the FIC for TF related financial intelligence. However, the LEAs have not demonstrated that they are adequately identifying TF cases proactively, with the majority of potential TF cases being derived from foreign agencies.

- The investigation of TF is not properly integrated into countering terrorism. South Africa's NCTS, to the extent it mentions TF, does not identify the pursuit of terrorist financiers as an operational mitigant to combat terrorism. Neither does the NCTS identify the designation of terrorists, terrorist organizations, and terrorist support networks as a tool to counter terrorism or TF.

Immediate Outcome 10

- Authorities have not implemented any designations adopted by the UNSC pursuant to resolutions 1267/1989 and 1988 since July 2017. Authorities do not communicate effectively new designations or de listings to obliged entities.

- Authorities have never used TFS under the UNSCR 1373 framework and would not be able to communicate such designations. They rely on a freezing mechanism that does not amount to a proper designation.

- The CFTC could be used as a mechanism to identify potential targets for designation, but authorities have not demonstrated they actively consider whether targets under scrutiny meet or do not meet the UNSCR criteria for designation. South Africa's approach of testing evidence in court through a criminal proceeding before making a designation is impeding authorities to actively consider TFS as a preemptive tool to fight TF. Authorities use alternative civil and criminal confiscation processes to deprive terrorist of their assets but only to a limited extent.

- Larger FIs with an international exposure show a good understanding of their obligations in relation to TFS for TF and implement them at their own motion. Other FIs and DNFBPs have a limited understanding of their obligations, mostly due to the lack of appropriate mechanisms for communication. Implementation of TFS by smaller FIs and DNFBPs is not effective.

- South Africa, through the formation of an NPO Task Team, has begun the process of identifying NPOs who, based on their activities or characteristics, are at risk of TF abuse. The authorities, however, have not applied specific measures, nor commenced monitoring or supervision, of organizations at risk of TF abuse.

- Measures taken to deprive terrorists of their assets and to combat abuse of NPOs are not in line with South Africa's TF risk profile. They do not reflect the number of terrorist related activities being monitored in the country nor the risk posed by FTFs.

Immediate Outcome 11

- South Africa started to implement TFS for PF in April 2019, and no assets have been frozen nor identified since then.

- Implementation occurs most of the time without delay when updating existing UNSCRs' lists but is unlikely to be without delay for new UNSCRs. The process used – even if yet to be tested for PF – ensures implementation in most cases within 24 hours when lists are updated but can take a matter of days for a new UNSCR.

- Communication by the FIC about changes to PF TFS lists is very effective for obliged entities that subscribe to the in real time free alert notification but does not reach other entities. Existing guidance documents do not provide enough specific details to guide entities with implementation of PF TFS.

- Coordination among authorities specifically on PF began recently and still remains at its initial stages but benefits from existing coordination mechanisms on proliferation that support early identification of proliferation through screening and verifications mechanisms.

- Early detection of activities specifically related to PF is to some extent ongoing, relying mostly on STRs and foreign intelligence. South Africa has developed a framework that allows the FIC, and LEAs, to receive, share, and act on information gathered from the private sector. The lack of access to BO information hinders the identification of PF-related assets and funds.

- Despite positive and repeated outreach efforts by the FIC on PF obligations, understanding remains uneven among FIs, DNFBPs, and VASPs. Only large FIs with international exposure understand the new PF obligations and implement them to an acceptable degree. Understanding by other FIs, DNFBPS, and VASPs is more limited. The overall level of compliance remains, however, uncertain.

- The authorities could not demonstrate how effectively they supervise implementation of PF obligations. Supervision and compliance monitoring commenced only in April 2019 and has a limited focus and scope; VASPs are not supervised at all.

Recommended Actions

Immediate Outcome 9

- South Africa should substantially increase its ability to proactively identify potential TF cases by broadening its perspective, at the investigative stage, of acts that may be terrorism related.
- South Africa should more effectively integrate TF investigations into its NCTS.
- South Africa should reconsider its policy of not pursuing the domestic designation of terrorists, terrorist organizations and terrorist support networks as a tool to counter terrorism or TF.
- South Africa should ensure that it has policies, procedures, and strategies in place to identify, investigate and prosecute all the different types of TF activity (e.g. collection, movement and use of funds or other assets).
- South Africa should complete its TF Risk Assessment process, develop an Implementation Plan specific to TF investigations and set detailed TF performance indicators for government departments.
- South Africa should amend the POCDATARA to remove exceptions from the definition of terrorist activity that are inconsistent with the TF Convention.

Immediate Outcome 10

- Authorities should address the major shortcomings identified in R.6 by revising their framework and strengthening their procedures for implementing UN listings, both for UNSCR1267/1988 and 1989 and subsequent resolutions as well as for UNSCR 1373.
- In the interim, authorities should resume, immediately, with implementation of TFS for UNSCRs 1267, 1988 and 1989 and subsequent resolutions.
- The mechanisms for communicating listings to the private sector should be improved for UNSCRs 1267, 1988 and 1989, and established for UNSCR 1373. Authorities should consider establishing a consolidated list for TFS.
- Authorities should increase outreach to FIs, DNFBPs, and VASPs, to improve the level of understanding of TFS obligations under South Africa law.
- The authorities should adopt a specific strategy to use TFS or alternative processes to deprive terrorists of their assets. They should disseminate operational procedures to relevant stakeholders, including IDCs such as the CFTC and the IDWG-CT, to develop a more proactive approach in considering potential eligible targets for designation and in using – when appropriate – TFS as a tool to fight TF.

- LEAs, intelligence, and prosecutors should be trained on the procedures to promote a more proactive approach in the use of available tools, including TFS and alternative processes, to pre-emptively deprive terrorists of their assets.

- To mitigate against the risk of TF abuse of the NPO sector, South Africa should implement an action plan with clear departmental responsibilities and deliverables. They should designate a competent authority responsible for the supervision or monitoring of NPOs, ensuring that the designated competent authority is fully integrated within the country's AML/CFT regime as being a member of the security cluster.

- South Africa should use the work done in reviewing its NPO sector to identify the subset or types of NPOs within its broader NPO sector that are at risk of TF abuse. This identification should be independent from any general assessment of organizations that pose a risk to the sector for other compliance matters.

Immediate Outcome 11

Authorities should:

  - Address the moderate shortcomings identified in R.7 to ensure – amongst other things – that implementation of TFS related to PF is without delay in all cases, including in cases where the UNSC adopts a new Resolution.

  - Increase the reach of communication of consolidated lists to all AIs and RIs through the FIC distribution list and through supervisors notifying their supervised entities.

  - Further improve coordination among authorities on PF, including by involving appropriate supervisors as necessary, to better and more proactively identify assets and funds held by designated persons/entities.

  - Continue to improve the identification of assets and funds held by designated persons or entities by building upon the recently developed framework that allows the FIC to receive, share, and act on information gathered from the private sector.

  - Provide more detailed written guidance focusing on implementation in practice (such as freezing) and tailored, as appropriate, to specific sectors. Continue ongoing outreach efforts to the private sector, focusing on those sectors that have likely more exposure to PF activity and where the understanding of obligations is lower.

  - Ensure and demonstrate, through effective monitoring and enforcement, that FIs, DNFBPs, and VASPs comply with their obligations.

The relevant Immediate Outcomes considered and assessed in this chapter are IO.9-11. The Recommendations relevant for the assessment of effectiveness under this section are R.1, 4, 5–8, 30, 31 and 39, and elements of R.2, 14, 15, 16, 32, 37, 38 and 40.

B. Immediate Outcome 9 (TF investigation and Prosecution)

Prosecution/Conviction of Types of TF Activity Consistent with the Country's Risk-Profile

235. South Africa has only convicted one person for TF since the last ME in 2009 (See Box 10.1). With a single person convicted for two counts of TF and with only one ongoing prosecution (see Box 11.1), South Africa has failed to demonstrate that it is prosecuting and convicting offenders with the different types of TF activity (e.g., collection, movement, and use of funds or other assets). See section on ML/TF Risks and Context and IO.1 for an assessment of South Africa's TF risks and their understanding of same.

236. Authorities take a conservative approach to classifying politically motivated violent acts as terrorism. One such example is that South Africa would not presume a terrorist act had occurred upon identifying evidence of domestic political violence or extremism. While they indicate that right-wing extremists have been convicted of planned acts of violence, they suggest that the current threat has been neutralized. They further suggest that the current solicitation of crowdfunding for funds and VAs, along with funds collected through self-funding activities, are used for financing the day-to-day activities and propaganda efforts. They suggest that since it is not being utilized to support the planning of potential terror attacks, such fund raising cannot be considered to be TF. These views negatively impact on the number of TF cases that South Africa is prepared to prosecute and raises concerns that the authorities are not then making efforts to identify financing networks and other financing activities without supporting evidence of an identifiable terrorist act. While gaps in technical compliance (see R.5) may account for some of this, the approach is also having a detrimental effect on international cooperation (see IO.2) particularly in respect of seeking formal assistance due to the low number of official investigations and prosecutions. South Africa is therefore not pursuing investigations of TF offenses consistent with the FATF Standards.

Box 10.1. The Conviction of Henry Okah

Henry Okah was the leader of the Movement for the Emancipation of the Niger Delta (MEND). A rebel militant group from the Niger Delta region in Nigeria. In 2005 he relocated to South Africa.

In March 2010, he travelled to Warri, Nigeria where he provided co-conspirators with funds to purchase dynamite, detonators, timing devices as well as two vehicles to construct vehicle bombs. On March 15, 2010, two vehicles were detonated in Warri, killing one civilian, and injuring 11 others. MEND claimed responsibly. Okah returned to South Africa undetected.

In September 2010, Okah again funded materials to create four vehicle bombs. On October 1, 2010, two vehicles exploded in Abuja, Nigeria, killing 12 civilians and injuring 53 others. Again, MEND claimed responsibility.

Okah was arrested by South African authorities in October 2010 after a joint operation. Cell phones and electronic devices were seized which revealed that Okah used text messages to send instructions regarding the payments of funds to associates in Nigeria. Okah was charged with planning and financing the Warri and Abuja bombings.

The investigation further revealed that Nigerian individuals and entities funded $4.5 million to accounts in Okah's name. The funds were used to set up operations in South Africa and purchase nine properties, valued at R8.6 million ($584,800). Okah also registered two shell companies.

Okah was convicted in South Africa in March 2013 on six counts filed under the POCDATARA for each of the bombings in Nigeria. A TF charge was included for each attack. Okah was sentenced to an effective 24 year imprisonment for all the offenses he committed in relation to the two bombings.

In November 2014, South African authorities obtained a preservation order for Okah's residence, which was forfeited on March 31, 2015.

Box 11.1. The Prosecution of the Thulsie Twins

The Thulsie twins were indicted on 12 charges under the POCDATARA (including TF) and one of fraud. The charges relate to attempts by the accused to further the activities of the Islamic State (IS).

The twins made two attempts to join IS in Syria and/or Libya. The main offense is contravention of section 2 of the POCDATARA relating to plans to carry out attacks in South Africa, which had been incited by external, IS operators. Another key offense is the solicitation of support for IS using Facebook. Several charges also relate to the acquisition of jihadist material containing information to poison persons, manufacture explosives, and handle firearms. The fraud charge relates to acquisition of false Lesotho passports after the accused were twice prevented from joining IS using South African passports.

The FIC identified accounts held by the twins as well as the source of funds. The twins relied on financial support from close associates as well as funds from a personal loan taken out by one of them. One twin was employed and received a salary. The twins used the funds to purchase air tickets and accommodation to facilitate their attempted travel to Syria.

The matter is currently awaiting trial and relies heavily on digital evidence seized from the two accused. Assistance has been provided by Syria, Iraq, Kenya, Lesotho, UK, USA, and France.

237. Given the risks identified by the authorities, the conviction of one person and one other prosecution in the past several years is not consistent with the country's TF risk profile.

TF Identification and Investigation

238. TF is not being effectively identified nor investigated. Given the low number of investigations and prosecutions, the authorities failed to demonstrate that they are identifying specific roles played by terrorist financiers. Terrorism and TF cases in South Africa are managed by the CTFC. The authorities indicated that all terrorism cases and inquiries have a TF component.

239. As of the onsite, there was only one ongoing TF prosecutions and three other TF investigative dockets that had been opened between April 1, 2013 and March 31, 2018. Investigative dockets are only opened upon consultation with the NPA:PCLU when enough evidence has been collected to support a TF charge. LEAs have, however, conducted 154 inquiries into potential national security activities. Authorities indicate that these inquiries seek to identify any criminal offenses potentially occurring, which could include TF. The source of those inquiries is detailed in the following table:

Table 4.1. South Africa: Source of Terrorism and TF Investigative Inquiries—Five Years to March 31, 2018

Source	Number	Percentage
Foreign Police Agency	93	60%
Internal Information	20	13%
FIC	16	10%
DIRCO	6	4%
Media	6	4%
SSA / SA Intelligence Service	3	2%
Interpol	3	2%
Other (crime scene etc.)	3	2%
Criminal Intelligence Head Office	2	1%
DoJ&CD (MLA)	2	1%
Total	**154**	**100%**

240. More than half (60 percent) of the investigative inquiries are generated from foreign police agencies. Much of this can be attributed to increased cooperation between SAPS:DPCI – CATS and foreign LEAs. An additional 11 percent (the DIRCO through diplomatic discussions, the DoJ&CD, through MLAs, the International Criminal Police Organization (Interpol), and the media) are being generated from external sources. Only 29 percent of potential TF activity therefore is being identified directly by domestic authorities. Of the 16 inquiries where the FIC is identified as being the source of the information, 14 were closed sighting that no terrorism, TF or any other criminal activity was identified, one was still ongoing and one, related to a violation of the FIC Act, was declined to be prosecuted by NPA:PCLU.

241. The FIC responds to requests for information related to ongoing terrorism and TF inquiries. Given that SAPS:DPCI – CATS is the authority within South Africa with the mandate to investigate terrorism and terrorism financing, it stands to reason that they are the ones making the most requests for financial intelligence from the FIC.

Table 4.2. South Africa: Requests to FIC for Terrorism Related Intelligence—Six Years to March 31, 2019

Year Ending March 31	2014	2015	2016	2017	2018	2019	Total	Average
SAPS:DPCI – CATS	4	30	101	4	18	157	314	52
SAPS:DPCI – PCMC	-	1	-	-	1	2	4	1
SAPS CI	-	3	5	22	22	52	104	17
SSA	2	-	6	-	2	10	20	3
NPA:AFU	1	1	-	-	-	2	4	1
Total	**7**	**35**	**112**	**26**	**43**	**223**	**446**	**74**

242. In addition to providing financial intelligence related to regulatory reports, the FIC has also used its powers to apply for Monitoring Orders to assist with ongoing terrorism and TF investigative inquiries (see Table 3.7 on page 55.).

243. Of the 154 national security inquiry files initiated during the five years ending March 31, 2018, 141 or 91 percent of them were closed for various reasons as detailed in **Error! Reference s ource not found.**.

Table 4.3. South Africa: Reasons for Closing National Security Inquiries—Five Years to March 31, 2019

Reason for Closing Inquiry Files	Number	Percentage
Unfounded/Undetected/Lack of Information	102	72%
Disruptive Operation – Non-TF	7	5%
Responded to a Foreign Request	6	4%
Referred to Other Investigative Units	5	4%
MLAT request not met	5	4%
Alternative Charges Laid Non-TF	4	3%
TF Docket Registered	3	2%
NPA Declined to Prosecute	3	2%
Terrorism Docket Registered	3	2%
Other	3	2%
Totals	**141**	**100%**

244. South Africa indicated that inquiry files are intelligence investigations and not specific to, or limited by, any particular criminal act. Authorities further indicated that various investigative steps are taken which could include electronic monitoring, authorized undercover agents, communications analysis, identification of financial footprints, lifestyle audits, engagement with foreign LEA's, and obtaining of statements, all with a view to converting intelligence into evidence. They indicated that it is standard procedure to have the FIC conduct a full financial analysis which would include analysis of available domestic and international transactional data. In consultation with the investigating officer the FIC may request additional information through informal (Egmont) channels in an attempt to identify or substantiate links to terrorism or TF. Beyond

these high-level generalized statements, authorities were unable and/or unwilling to share specifics regarding individual inquiry files with the assessment team. Despite the number of inquiry files initiated, only three led to TF investigative dockets being registered with only one of those advancing to the prosecution stage as of the onsite. The fact that 71 percent of these inquiry files are closed due to a lack of information to advance them, the inability to detect any crime or the fact that the lead was found to be false, is indicative of simply following up on possible national security leads and should not be characterized as TF investigations. The cases transferred to other investigative units is done when no terrorism or TF crimes are identified but the possibility of other crimes to be further investigated is warranted.

245. South Africa has a trained and resourced specialized police section to address terrorism and TF cases (SAPS:DPCI – CATS), complemented by a specialized prosecution unit (NPA:PCLU). The police have powers to use a range of special investigative techniques, including interception of communications, undercover operations, and, through the FIC, live monitoring of suspect accounts. In spite of this, and the reasonable number of inquiry files considering the risk profile, South African authorities are failing to successfully identify evidence of TF activity.[50] Given the low number of investigative dockets opened and the high number of closed inquiry files without conclusively identifying TF activity, South Africa has failed to demonstrate that they are successfully identifying TF activity, nor have they demonstrated that they are able to identify the specific roles played by terrorist financiers.

246. Authorities take a conservative approach to classifying politically motivated acts of violence as terrorism. Assessors formed the opinion that authorities would prefer to pursue acts, where circumstances suggest extremist motivation may exist, as simple acts of violence rather than terrorist acts. There seems to be a reluctance to characterize such acts as terrorism. This approach indirectly impacts on the authorities' ability to pursue TF investigations, as there is no offense for financing simple acts of violence.

TF Investigation Integrated with–and supportive of–National Strategies

247. South Africa did not demonstrate that its NCTS effectively identifies TF investigations as a mitigating strategy to combat terrorism. Only a summary of the NCTS dated 2013 was shared with the assessment team as South Africa indicated security concerns. The Strategy's effectiveness is measured by an Implementation Plan that contains specific Action Steps which provides clear departmental responsibilities and timeframes for implementation, assessment, and re-assessment. The Implementation Plan is updated on an annual basis and quarterly feedback is provided to inter-departmental forums. A one-page excerpt from the 14-page 2016 Implementation Plan was provided to assessors. One action item was presented: "*Assess and report on the capacity of government to conduct financial investigations into terror financing*". This item is assigned to FIC and was to be completed in the 3rd quarter of 2016. Related to the same item under the heading 'Modalities', the Implementation Plan states that: "*The report will focus on the capacity and*

[50] South Africa asserts that the reason for this is because TF networks are not active in South Africa.

coordination within and between law enforcement, intelligence and investigating agencies to conduct terror financing investigations". No such report was provided to the assessment team.

248. The Strategy has five pillars but for TF focuses on investigating terrorism and terrorists not others financing terrorism. The third pillar, 'Mitigation' talks about improving border controls, identity documentation, and the identification and management of risks based on updated intelligence assessments. The fourth pillar, 'Combatting', references a multi-agency approach; indicates that creating a hostile operating environment for terrorists necessitates that financial investigations should form an integral part of all terrorism investigations; encouraging regional, continental, and international cooperation; the application of legislation, including MLAs; and, the achievement of higher prosecution rates, increased successful convictions, and more comprehensive forfeiture of terrorist assets. While the forfeiture of terrorist assets is an important strategy to fight terrorism and TF, there is no reference to the forfeiture of assets held by terrorist financiers.

249. As discussed in IO.10, the authorities do not consider administrative TFS designations as a relevant tool to fight TF. They explicitly favor a policy that requires obtaining compelling evidence and testing that evidence in court before they would consider making a designation under UNSCRs for TFS. Given the reluctance to characterize acts of violence as terrorism, the financiers of such acts are not being investigated for TF, nor are they being assessed as potential subjects for designation.

250. The low number of TF investigations as a mitigating strategy against terrorism and the policy of not making use of domestic designations under UN sanctions hinder South Africa's ability to effectively demonstrate that these tools are used as part of a broader terrorism strategy.

Effectiveness, Proportionality, and Dissuasiveness of Sanctions

251. South Africa has convicted one person for TF since the last ME in 2009 – Henry Okah, see Box 10.1. Okah was convicted on six charges for each bombing attack and received a 12-year sentence for each charge including one TF conviction for each attack. The sentences relating to the same attack were to be served concurrently but the two sets of convictions were to be served consecutively resulting in a 24-year prison term. South Africa has a maximum penalty for a TF conviction of 15 years. When compared to a maximum penalty of 30 years for ML, it is not possible to conclude that the sanction for TF is proportionate. With the conviction of only one individual since the last ME in 2009, South Africa is unable to demonstrate that sanctions imposed for TF are effective or dissuasive.

Alternative Measures used where TF Conviction is Not Possible (e.g. Disruption)

252. South Africa has not demonstrated that is has effectively used alternative measures where TF convictions are not possible. As indicated earlier, 71 percent of national security inquiries are closed as they are deemed to be unfounded, undetected or there is a lack of information to advance them. Given the main sources of those inquiries (foreign police, internal sources, and FIC) the determination that the cases were unfounded, undetected or there is a lack of

information to advance them seems high. Given the concerns raised above that South Africa is taking a conservative approach to classifying politically motivated acts of violence as terrorism, assessors felt that this may contribute to inquiries into possible TF being terminated as being unfounded before an exhaustive inquiry is made.

253. South Africa does not pursue domestic designations as an alternative measure where a TF conviction is not possible. According to the authorities, a handful of the terrorism and TF inquiries were referred to other LEAs to pursue investigations into other criminal acts or were dealt with by disruptive operations. However, the authorities could not elaborate on these cases to provide evidence of whether or not these were in fact TF cases, whether alternative measures were being used successfully to disrupt TF activities or whether these alternative measures were being used where a TF conviction is not possible.

C. Overall Conclusions on IO.9

254. The pursuit of TF is done in a coordinated way through the CTFC which includes all the relevant security cluster government stakeholders. However, pursuing TF investigations is not properly integrated in the NCTS and authorities are failing to produce results reflective of the country's identified TF risk.

255. South Africa has failed to demonstrate that it is effectively identifying, investigating, or prosecuting terrorist financiers or addressing TF through alternative measures.

256. The low level of viable investigations and prosecutions into TF in South Africa is not consistent with the country's recognized TF risk profile as a country with FTFs and from which terrorist groups are soliciting support and using as a transit point and a base for planning and logistics. Fundamental improvements are needed to demonstrate effectiveness in this area.

257. South Africa is rated as having a low level of effectiveness for IO.9.

D. Immediate Outcome 10 (TF Preventive Measures and Financial Sanctions)

Implementation of Targeted Financial Sanctions for TF without Delay

258. South Africa's implementation of TFS against TF is not effective and suffers from deficiencies that are inherent to the applicable framework.

259. The applicable framework does not ensure that implementation of UNSCRs 1267/1988 and 1989 and subsequent resolutions is without delay. As described in R.6, South Africa's framework allows for implementation in national law, but the process is dependent upon publishing a proclamation in the Official Gazette, to bring changes to TFS obligations into effect. There is no statutory time limit for such action, and FIs and DNFBPs must implement TFS only when the

proclamation is published, as changes to UN lists do not create direct legal obligations in South Africa.

260. Authorities have not implemented any designations adopted by the UNSC pursuant to resolutions 1267/1289 and 1988 since July 2017. The last proclamation was signed on June 29, 2017 to implement a UNSCR from December 2016 and was published in the Official Gazette only on July 14, 2017. No proclamation has been published since then, i.e. no designations or de-listings decided since then have been implemented. Over the period under review, no assets have been frozen pursuant to UNSCRs 1267/1988 and 1989 and subsequent resolutions.[51] In addition, there is no provision establishing a mechanism to identify targets for designations and authorities have not demonstrated they actively consider whether targets under the CTFC scrutiny meet or do not meet the UNSCR criteria for designation (see below 4.3.3). South Africa has not proposed on its own initiative, nor co-sponsored, any person for designation, but has supported all listing proposals submitted to the UNSC.

261. To implement UNSCR 1373, authorities rely on a mechanism that enables a Court to order an ex parte freezing obligation for an indefinite duration. As described in R.6, the High Court may order a freezing based on such an application by the NPA. When a request to freeze is received from another country, the NPA, would assess the nature of the request and notify all the relevant agencies (FIC, SAPS, security services) who in turn would provide advice for deciding to submit or not an application to the court. Authorities report that they have not received or made any foreign requests and have not made any designation on their own motion, i.e. these provisions have not been used in the context of UNSCR 1373.

262. This mechanism suffers from major deficiencies in terms of scope and implementation. An order can only apply to identified property in South Africa rather than to any asset of a designated person. This means that the order can only focus on property located at the time of the order. It would not be a general freezing order prohibiting all dealing with any asset of a designated person. In addition, this has also an impact when implementing foreign requests as no freezing order can be issued if there is no property located in South Africa at the time of the request. Any assets entering South Africa after the request would thus not be covered. Finally, communication of the High Court decision would be limited only to the affected parties, and the FIC's would contact other FIs but only to identify (and not freeze for indefinite duration) other potential assets.

263. Larger FIs with an international exposure show a good understanding of their obligations in relation to TFS for TF and implement them at their own motion. They are driven by global policies or requirements of correspondent banks and use screening mechanisms against international lists at the onboarding phase and whenever an international list is updated. They do not rely on information provided by authorities, nor wait for a national designation to implement TFS.

[51] NB: one listed individual resided in South Africa in 2002 but did not have any assets in South Africa.

264. Other FIs and DNFBPs have a limited understanding of their TFS obligations for TF, mostly due to the lack of appropriate mechanisms for communication. As per UNSCR 1267/1988 and 1989, publication of a proclamation is not done on a systematic basis. It is therefore unclear to obliged entities if changes to the UN lists create legal obligations to freeze in South Africa or not. In addition, there is no active communications to obliged entities to inform them of changes in the lists. The "TFS list" published on the FIC website does not apply for TF TFS and does not incorporate – nor match with – the concurrent "Consolidated List of Individuals and Entities Subject to Measures Imposed by the United Nations Security Council" published on the SAPS website for TF which is not updated. These different listing mechanisms create confusion regarding obligations for entities, and existing guidance is not helpful in that regard. For UNSCR 1373, there is no communication mechanism. Authorities have not demonstrated active outreach to FIs and DNFBPs on TF TFS obligations.

265. Against this background, implementation of TFS by smaller FIs and DNFBPs cannot be effective. As mentioned, large FIs implement TFS mostly on a voluntary basis as a result of their group policies rather than obligations arising in South Africa. Supervisors for FIs do incorporate TF TFS as part of their supervisory activities, both at market entry and as part of ongoing monitoring. Supervisors have assessed screening mechanisms for banks in 2014 and 2017. The SARB:PA noticed improvements with a reduction of false positives or alerts between these two exercises but concluded in 2017 there was still a lot of work to do at many FIs. Up to 2019, in nearly all cases the SARB:PA fined an FI, it was related to deficiencies in TFS reporting. However, supervisory activities for TFS in other sectors remain nascent, and it is therefore difficult to confirm compliance of other FIs, DNFBPs with their obligations. There is no supervision of VASPs.

Targeted Approach, Outreach, and Oversight of At-Risk Non-Profit Organizations

266. While South Africa has begun the process of reviewing their NPO sector, this review has not yet focused on the risk of TF abuse nor have they identified the subset of organizations, based on their characteristic or activities, that are at risk of TF abuse. Government officials responsible for oversight of the sector are not trained in TF matters and are not members of the Government's security cluster.

267. The NPO sector in South Africa is well established and is comprised of various voluntary associations, charitable trust and corporations for education, health, faith, environment, arts and culture, sports, and recreation. South Africa has over 220,000 known NPOs operating in the country. There is no central registration database for NPOs, and registration with the NPO Directorate at the DSD is voluntary.

268. While the majority of NPOs are registered with the NPO Directorate, there are instances where these NPOs are registered with more than one government body. There are also instances where NPOs are registered with a government body to the exclusion of registration with the NPO Directorate. There are 2,500 non-profit trusts registered with the Master's Office, 6,700 non-profit companies registered by the CIPC, and 21,250 Public Benefit Organizations (PBOs) registered with the SARS.

269. In December 2018, South Africa established the NPOTT to review the sector to identify high risk NPOs, both registered and unregistered. Given the vulnerabilities, due to the lack of a mature oversight mechanism for compliance in the sector, the review was not specific to the risk of TF abuse but rather included a wide range of risks including ML, PF, financial integrity, good governance and other general regulation compliance matters. While the review did identify approximately 5,000 organizations believed to be most at risk, these risks were not specific to TF abuse and the review failed to identify the specific subset or types of NPOs that based on their characteristics and activities puts them at risk of TF abuse.

270. South Africa does, however, recognize the threat of TF abuse to its NPO sector. Concerns pertaining to vulnerabilities within its regulatory system played a predominant role in the Preliminary Findings of the TF NRA. South Africa has identified the following risks of TF abuse to its NPO sector:

- Many South African NPOs provide relief efforts in conflict areas with terrorist entities present, where they could be wittingly or unwittingly exploited for TF purposes.
- While large amounts are donated to NPOs through financial channels that are regulated and declared in South Africa, this type of oversight is not extended to the complete cycle of NPO funding activities.
- The ultimate beneficiaries of NPO funding are unaccounted for and there are no oversight mechanisms in place to ensure that funds are not diverted to support terror groups abroad.
- South African NPOs have been known to be involved in ransom negotiations for the release of hostages through the payment of large amounts of money contrary to UNSCRs.
- NPOs process large amounts of cash and regularly transmit funds between jurisdictions. NPOs operate in a less regulated environment and administrative and financial management lacks rigor.
- There are no mandatory registration requirements for NPOs in South Africa which represents a vulnerability for deceptive NPOs to mask ill intent.
- The regulatory framework is fragmented and lacks sufficient oversight mechanisms
- There is a lack of sufficient proactive interaction between relevant government stakeholders to comprehensively monitor the NPO sector having an adverse effect on the country's ability to proactively identify TF cases.
- The DSD, the main NPO regulator, does not have the monitoring nor investigative capacity as it relates to national security. It is not a security cluster department and it does not consider national security risks.

- The oversight mechanisms for NPOs have inadequate capacity and lack sufficiently trained personnel to ensure oversight of the sector to guard against the risk of TF abuse.
- The NPO sector in general is not sufficiently aware of the risks posed by TF.

271. The lack of a designated department or other mechanism responsible for safeguarding South Africa's NPO sector against the threat of TF abuse hinders South Africa to address the risk effectively.

272. The NPOTT has identified steps that need to be taken to address the risk of TF abuse but not yet applied any measures to mitigate the risks identified nor begun specific monitoring of any organizations deemed vulnerable to TF abuse.

Deprivation of TF Assets and Instrumentalities

273. South Africa's NCTS does not identify the pursuit of terrorist financiers as an operational mitigant in the fight against terrorism (see IO.9). Neither does the Strategy identify the designation of terrorists, terrorist organizations and terrorist support networks as a tool to counter terrorism or TF.

274. There is no specific approach or strategy to use TFS or related mechanisms to deprive terrorists of their assets.

275. Authorities responsible for combating TF do not use administrative TFS designations as a relevant tool to manage the TF risk. Even though designation is not conditional upon the existence of a criminal investigation, they favor an approach that requires obtaining compelling evidence and testing that in court through a criminal proceeding before they would consider making a designation under UNSCRs for TFS.

276. Authorities have not demonstrated they actively consider whether targets under the CTFC's scrutiny meet or do not meet the UNSCR criteria for designation. As described in R.6 (see c.6.1 and c.6.2), there is no provision establishing a mechanism to identify targets for designations. However, the authorities claim that the CFTC, which coordinates all TF operational matters, could be used as such a mechanism. They advise that the designation – if it were to occur – would be decided by the CFTC in consultation with the CTWG, and eventually confirmed by the Cabinet before being communicated through the DIRCO. However, authorities did not demonstrate that the CFTC procedures include or refer to UNSCR criteria to identify targets for TFS designation; nor were they able to demonstrate that any of the 154 TF inquiry files has been assessed against the designation criteria.

277. As a policy, authorities favor using civil and criminal confiscation processes to deprive assets and instrumentalities related to TF activities rather than TFS.

278. The authorities have used their non-conviction-based forfeiture mechanism (the POCA, ch.6) to target instrumentalities and specific tainted property associated with terrorist and related activity.

279. In practice, the authorities have used these alternative processes to deprive terrorist of their assets only to a limited extent relative to South Africa's TF exposure. They have seized or confiscated TF-related assets in three instances. Over the period under review amounts frozen, seized, or confiscated amounted to around R6 million ($408,000) (of which R4.5 million ($306,000) was confiscated; R1.5 million ($102,000) being frozen or seized). One case involved a preservation order obtained under the POCA, ch.6 followed by a post-conviction confiscation (see Box 10.1: Okah case). The second relates to the freeze of assets, stolen from victims of a kidnapping, to impede their use for TF, whereas the third (see Box 11.1. Thulsie Twins) involves seizing of proceeds and instrumentalities during the investigation phase.

280. Those cases, however, do not demonstrate the active use of freezing mechanisms to preemptively deprive terrorists of assets and prevent them from raising funds. The limited number of cases and the low amounts is not in line with South Africa's TF exposure.

Consistency of Measures with Overall TF Risk Profile

281. The measures implemented for TFS and to combat abuse of NPOs are not in line with the TF risk profile that shows that South Africa is exposed to TF. The authorities have investigated financing activities to facilitate foreign terrorism including linked to organized groups such as ISIL and have acknowledged the presence of facilitation networks and cells. South Africa has also dealt with FTFs, including observing some returnees. Measures taken by authorities do not reflect these activities.

E. Overall Conclusions on IO.10

282. Terrorists are identified and deprived of their resources and means to finance or support their activities only to a negligible extent considering the TF risk and activities under monitoring in the country. The use of TFS is not proactive nor used as a tool to mitigate TF risk (including for FTFs).

283. There are major shortcomings in the framework that impede – among other things - implementation of TFS without delay for UNSCR 1267, and appropriate identification and proposal of targets for designation. More importantly, the last time a UNSCR 1267/1988 and 1989 and subsequent resolutions has entered into force in South Africa was in July 2017. This fundamentally hinders the effectiveness of the system. In addition, the mechanism to implement UNSCR 1373 is not consistent with the UNSCR requirements, as it does not provide for a general freezing order.

284. South Africa has not identified the subset of NPOs that, based on their characteristics or activities, are at risk of TF abuse. The government authority responsible for oversight of the

NPO sector has not had any TF training nor has it applied any measures to address the risk to NPOs of TF abuse nor begun monitoring of organizations deemed to be vulnerable.

285. South Africa is rated as having a low level of effectiveness for IO.10.

F. Immediate Outcome 11 (PF Financial Sanctions)

286. S**outh Africa's economy includes industries and companies producing military or dual-use** nuclear related items, some special fissionable materials as well as equipment or material especially designed or prepared for their processing, use, or production. South Africa has some nuclear power production and companies offering international trade and shipping services. As of November 2019, 481 traders and manufacturers (including chemical, biological, nuclear, and missile related), and 30 freight forwarders or shipping agents are registered with the NPC.

287. There are substantial cross-border financial and trade flows with Iran and with the Democratic People's Republic of Korea (DPRK) (Table 4.4). These flows relate notably to mineral products, iron and steel, machinery, chemicals, vehicles, aircraft, and vessels for DPRK. DPRK has an embassy in South Africa and diplomatic personnel. For Iran, flows relate notably to copper and precious metals but are subject to stronger fluctuations.

Table 4.4. South Africa: Financial and Trade Flows with Iran and DPRK in the Four Years ending March 31, 2018

Country	Currency	Total Value per Year (millions)					
		2015	2016	2017	2018	Annual Average	Total Value 2014-2018
DPRK Incoming	Z	592.3	581.7	635.0	646.2	613.8	**2,455.2**
Financial Flows	$	46.4	39.5	47.6	48.8	45.6	**182.4**
Iran Incoming	Z	154.1	102.4	1,626.3	446.3	582.3	**2,329.2**
Financial Flows	$	12.1	7.0	122.0	33.7	43.7	**174.7**
DPRK Outgoing	Z	2,357.0	1,033.0	888.6	1370.9	1412.4	**5,649.4**
Financial Flows	$	184.7	70.2	66.6	102.8	106.1	**424.4**
Iran Outgoing	Z	20.4	34.1	32.0	48.4	33.7	**134.8**
Financial Flows	$	1.6	2.3	2.4	3.6	2.5	**9.9**

Implementation of Targeted Financial Sanctions Related to Proliferation Financing without Delay

288. South Africa's freezing regime to implement TFS related to PF came into force only in April 2019 (i.e. six months prior to the onsite).[52] Since then, South Africa began implementing the process described in R.7 for publishing updated sanctions lists, which triggers a prohibition on

[52] Note that all PF designations adopted by the UNSC before April 2019 have only been implemented in South Africa since the freezing regime entered into force.

dealing with funds or assets of any designated person or entity. The prohibition obligation applies to all persons in South Africa (including VASPs) –see page 98 for how well FIs and DNFBPs are complying.

289. Since April 2019, South Africa has implemented TFS for PF fairly well, but some improvements are needed. These relate to communication about lists are available on the FIC website and can be accessed by the public through a free email alert subscription but does not reach all AIs and RIs, and implementation may not be without delay in all circumstances.

290. The FIC provides a free searchable consolidated list of persons and entities designated for PF through its website. This website sends in real time – upon subscription – an automated email alert as soon as the list is amended on the website. Between April 2019 and the onsite, 1,822 users had registered to the email alert, representing nearly five percent of AIs and RIs and the FIC contributed to the increase of these numbers over time with its awareness events. In addition, a user guide on how to conduct basis searches on the TFS list is also available to the public on the FIC website. However, supervisors do not notify their supervised entities, which limits the reach of communication.

291. Implementation without delay occurs most of the time for existing UNSCRs but is unlikely to be without delay for new UNSCRs. For existing UNSCRs, the FIC has demonstrated that, since April 2019, it issues Director's notifications (albeit in cases not directly related to PF designations) in most cases within 24 hours after changes to a UNSCR list. The process is however longer over weekends although still normally within one business day, but it took up to three to five business days in a few cases. If the UNSC adopts any new PF resolutions, the requirement for publication in the Gazette (see c.7.1) – which would then trigger the related freezing obligation – would, however, take a matter of days, which is not without delay. This demonstrates that the process that would be used to implement TFS related to PF – even it has yet to be tested in practice for PF specifically – is without delay most of the time for updates to UNSCRs lists but not when a new UNSCRs is adopted.

Identification of Assets and Funds held by Designated Persons/Entities and Prohibitions

292. As of the onsite and since April 2019, no PF-related assets had been frozen pursuant to UN designations in South Africa.

293. The identification of assets and funds held by designated persons and entities is hindered by the limited access to accurate and up to date beneficial ownership information (see IO.5). This affects the capacity of AIs and authorities to identify the use of legal persons and arrangements to evade sanctions and the effectiveness of the regime by limiting its ability to identify assets held by designated persons.

294. Specific coordination on PF is recent and still remains at its initial stage but benefits from existing proliferation coordination mechanisms that support early identification of proliferation. Authorities espouse a multi-agency approach to mitigate operational risk. IDCs link

the DIRCO, the SAPS:DPCI, the NPA, the FIC and the SARS with three nonproliferation control bodies that focus on export controls, dual goods nuclear items and imposes trade and export controls through a mandatory registration mechanism and cover brokering, freight forwarding and shipping services, as well as PF. The SARS:Customs use a proactive RBA involving intelligence information including related to high risk jurisdictions. Control bodies conduct inspections, outreach programs, and refer potential regulatory non-compliance detected to SAPS:DPCI and the NPA to decide whether to pursue administrative or criminal charges. The NPA also trains LEAs and the SARS:Customs on investigations to promote detection and investigation of WMD offenses. Regulators overseeing implementation by AIs and RIs, except the FIC, are not part of these groups, which limits early detection of PF activities. The framework has proven to be effective as South Africa successful convicted in 2007 individuals for their role in the Aq Khan network and significant forfeitures of assets inside the country and abroad were obtained.

295. South Africa has developed a framework that is allowing FIC, and LEAs, to receive, share, and act on information gathered from the private sector. Going beyond FATF standards, authorities have chosen to extend STR obligations to activities that relate to the contravention of the prohibition regime for PF. STRs for PF have proven to be a useful resource for FIC which operates a daily screening of its STR database against UNSCRs lists and to strengthen its detection capacity.

296. Early detection of activities specifically related to PF is to some extent ongoing, relying mostly on STRs and foreign intelligence. LEAs (NPA, SAPS:DPCI, NPA:AFU), intelligence agencies (FIC) and export control bodies coordinate when investigating PF as demonstrated in three cases they shared. These cases demonstrate that authorities investigate potential PF activities as a reaction to STRs and foreign intelligence. STRs were sent before the entry into force of the reporting obligation, which demonstrates sensitivity from some FIs to potential PF activities and ongoing interactions between the regulatory bodies, the FIC, LEAs, and intelligence with the financial and banking sector. The FIC conducted analysis to contribute to the investigation of potential PF activities and referred to SAPS:DPCI and SSA. In one case, a team was set up comprising of the NPA, SAPS:DPCI, FIC, NPA:AFU asset tracking and control bodies. Investigations are still ongoing in two of these cases, while no PF was involved in the third case.

297. South Africa has never co-sponsored nor proposed a designation to the UN, as no activity falling within the scope of the UNSCR regimes was detected to the knowledge of authorities nor reported by foreign jurisdictions.

FIs and DNFBPs' Understanding of and Compliance with Obligations

298. Despite extensive outreach efforts by FIC to provide guidance on new obligations, understanding of and compliance with obligations remains uneven among FIs, DNFBPs, and VASPs.

299. The materially important larger FIs with an international exposure show a more developed understanding of their obligations and implement appropriate screening measures commensurate with their exposures. They understand the new PF obligations and seem to comply with their obligations by applying on-boarding and real-time screening of their client base

(including their back book) and transactions against PF-related TFS lists. From a materiality perspective, the banking arms of these groups represent 85 percent of total banking assets and their FSPs and investment scheme managers control around 20 percent and 27 percent of assets under management.

300. Understanding by other FIs, DNFBPs, and VASPs is limited to screening obligations and reporting to FIC in case of a match and remains very uneven among them. Many of them, however, do not screen against PF-related lists in practice. The understanding of how other FIs, DNFBPs, and VASPs deal with assets identified when there is a match cannot be assessed due to no matches nor potential matches found yet; however, there has been some regulatory engagement through public awareness raising sessions to provide guidance on how to proceed once assets are identified.

301. The level of compliance by FIs and DNFBPs with PF-related TFS prior to April 2019 cannot be ascertained as supervision and compliance monitoring of PF-related obligations commenced only in April 2019. No supervision with respect to PF-related TFS was conducted before this because no legal obligation to implement PF-related TFS was in place. Supervisors have nevertheless assessed other UNSCR screening mechanisms for banks in 2014 and 2017 and noticed improvements with a reduction of false positives or alerts between these two exercises but concluded that many FIs required further improvements as of 2017. As supervision and compliance monitoring of PF-related obligations is still at an early stage (see core issue 4 below), the current level of compliance of FIs, DNFBPs, and VASPs was not possible to assess yet but is likely to reflect the uneven level of understanding in the private sector.

302. In 2017, before the PF obligations came into force, the FIC started to incorporate public awareness sessions on PF, including TFS, as part of its engagement program with AIs and RIs (which do not include VASPs). These programs focused mostly on new obligations emanating from the revised legal framework and included case studies and lessons learned on sanctions evasion techniques based on country experiences and international best practices.

303. In March 2018, two workshops were conducted with public and private sector stakeholders to discuss PF-related challenges. The Royal United Services Institute attended and shared its findings on topics such as PF risks (through case studies) and compliance programs (know your customer (KYC) checks, enhanced CDD, screening, STRs). As of the onsite, those lessons learned and shared best practices had not yet resulted in concrete developments but authorities were in the process of developing a revised and more detailed GN on implementation of UNSCRs related to PF. Authorities also advised that they intended to reflect those in a future NRA for PF.

Competent Authorities Ensuring and Monitoring Compliance

304. Supervision and compliance monitoring of PF-related obligations is at an early stage as it commenced only in April 2019, and no sanctions have been applied so far. Supervisors do not perform PF-related inspections; supervision is limited to checking how some banks screen

against TFS lists. Supervision of VASPs does not occur. Accordingly, the authorities cannot yet demonstrate how effectively they supervise PF obligations.

G. Overall Conclusion on IO.11

305. South Africa has implemented fairly well PF related TFS since April 2019, consistent with its exposure to PF. Even though the process in place remains to be tested in practice for PF specifically, implementation would occur without delay most of the time when updating existing UNSCRs' lists but is unlikely to be without delay for any new UNSCR.

306. Specific coordination on PF is recent and still remains at an initial stage but benefits from existing proliferation coordination mechanisms that support early identification of proliferation. Detection and investigations of activities specifically related to PF is to some extent ongoing, relying mostly on STRs and foreign intelligence. The authorities' ability to proactively identify and detect PF-related assets is, however, challenged by an uneven level of understanding of PF obligations in the private sector and limited access to accurate and up to date BO information.

307. The overall level of compliance of FIs, DNFBPs, and VASPs cannot be demonstrated but is likely to reflect the uneven level of understanding in the private sector, with only larger FIs with international exposure having a more developed understanding and a likely appropriate level of compliance. Guidance documents do not provide enough details to guide entities with implementation of PF TFS. Supervision and compliance monitoring of PF-related obligations is still at an early stage and no sanctions have been applied so far for non-compliance with the new PF obligations.

308. South Africa is rated as having a moderate level of effectiveness for IO.11.

PREVENTIVE MEASURES

A. Key Findings and Recommended Actions

Key Findings

- The larger banks show a developed understanding of ML risks and seem better at implementing mitigating measures commensurate with their risks than most smaller FIs, which are rule-based compliance focused, rather than identifying and understanding risks.
- AIs understand and mitigate TF risk commensurate with their risks to some extent, primarily due to a lack of information from the authorities.
- Overall, DNFBP's understanding of ML risks and AML/CFT obligations is underdeveloped and mitigating measures are not risk-based, with casinos as a positive outlier.

- Basic CDD is satisfactorily applied by many AIs, but AIs only apply BO requirements to some extent, which is inadequate given the vulnerability of legal entities. The larger banks are better at applying such requirements but remain challenged at obtaining sufficient BO information. DNFBPs and FIs with an underdeveloped understanding of their risks conduct ongoing monitoring only to some extent.

- The limited implementation of the RBA by most AIs causes insufficient application of enhanced measures. Targeted measures to address high-risk scenarios, such as use of cash and corruption are applied to some extent, mainly by larger FIs, while a deficient legal definition of PEPs limits effectiveness. AIs play down the risks of operating internationally.

- The larger banks and ADLAs meet reporting obligations to a large extent, where most other sectors fail to do so commensurate with their risk profiles. Some (high-risk) sectors rarely file STRs.

- FIs apply internal controls and procedures ensuring compliance with the requirements depending on their ability to apply an RBA, but there are concerns that larger banks' group controls may not be adequately applied in their foreign entities in all instances.

- Some financial sectors and DNFBPs, including CSPs and DPMS, which are potentially high-risk, and VASPs are not covered under the AML/CFT regime, save for a general reporting obligation as a "business."

Recommended Actions

- South Africa should ensure that AIs conduct business risk assessments systematically while including a sufficient range of inherent risk factors to identify and understanding their ML/TF risks at entity level. TF, corruption, geographical risks, and the use of cash should particularly be addressed. Their RMCPs should be dynamic exercises and target their risks beyond rule-based compliance with legal requirements. The authorities should provide better guidance on these matters.

- South Africa should ensure that AIs significantly improve the application of all CDD obligations, especially ongoing due diligence, and BO requirements. The authorities need to provide AIs with better access to reliable BO information so AIs can adequately verify the natural persons controlling legal persons and arrangements.

- South Africa should analyze ways to substantially improve the information available on domestic PEPs and then reach out to support AIs in effectively identifying such PEPs across all governmental levels (state, provincial, and municipal). Furthermore, the legal definition of PEP should be rectified in line with R.12.

- South Africa should ensure that AIs—beyond the larger banks and ADLAs—and especially those in high-risk sectors, file more STRs in line with their risk profiles.

- The larger banks should effectively implement adequate AML/CFT group controls in the operations of their foreign entities.

- Those sectors currently out of scope of the AML/CFT requirements—in particular, the CSPs, accountants, DPMS, and VASPs—need to be included.

The relevant Immediate Outcome considered and assessed in this chapter is IO.4. The Recommendations relevant for the assessment of effectiveness under this section are R.9–23, and elements of R.1, 6, 15, and 29.

B. Immediate Outcome 4 (Preventive Measures)

309. With reference to chapter 1, it is important to focus on the larger banks from a material and risk perspectives, the securities sector (FSPs and CIS managers) mostly from a material perspective, on the high-risk sectors: estate agents and attorneys, and on casinos.[53] Some FIs and DNFBPs (including CSPs and DPMS that are potentially high risk) and VASPs are not subject to most AML/CFT obligations, and this impacts the effectiveness of preventive measures (see para. 133. and c.1.6). Furthermore, the active informal network of MVTS's operating in South Africa is also a matter of concern.

310. T he RBA to CDD, business risk assessments, and many obligations for key preventive measures (understanding and obtaining client information, ongoing due diligence, PEPs, and BO) are relatively new (October 2017) and have only been enforced since April 2019. Exemptions previously applicable to the securities sector without any justification have been removed. The larger banks commenced implementing such key preventive measures prior to 2019, particularly due to their international exposure.

Understanding of ML/TF Risks and AML/CFT Obligations

311. FIs overall show an acceptable understanding of their AML/CFT obligations, but only the larger banks and large insurance companies show a developed understanding of their ML risks. These larger FIs benefit from their international exposure and experience and are better at assessing ML risk.

312. The larger banks understand the main threats and vulnerabilities in the NRA to a large extent, including corruption, fraud, crypto asset exchanges, tax offenses, use of shell companies and complex structures, use of cash, and environmental crimes such as illegal wild-life trafficking. Corruption is regarded as a major threat, and some of these banks have performed focused risk assessments on corruption and bribery.

[53] Assessors consider casinos to have less risk than attorneys and estate agents even though the NRA regards the gambling service providers (predominantly casinos) and KRDs to be high risk sectors.

313. The use of cross-border bank transfers to move proceeds of crime abroad is recognized by most banks as an important channel exploited by launderers, but only to some extent identified as a risk that needs to be managed consistently. This requires further attention also given that some banks not only provide such transfers for their own clients, but also for (clients of) smaller banks that do not offer cross-border services, and they may function as platform for ADLAs.

314. The larger banks' understanding of ML risk relevant to their business is based on their business risk assessments, which are adequately performed to some extent. These banks undertook such assessments before the legal obligation came into force, being part of global, group-wide risk management initiatives to meet international best practices. However, the assessments seem to be conducted predominantly from a client risk perspective, with risks from products and services, and operating internationally not being understood adequately at the entity level. Second, most business risk assessments are not systematically updated and do not sufficiently capture emerging risks.[54] They are static and reactive rather than dynamic and may miss important trigger events, incidents, and structural changes to threats and vulnerabilities (e.g., trends or patterns following Zondo Commission subpoenas, media coverage of relevant developments, or the introduction of new statutory requirements).

315. Other FIs, including smaller banks, have a basic understanding of their ML risks with a predominantly rule-based compliance-focused approach. They do recognize common threats and vulnerabilities, but mostly in the context of legal compliance with the FIC Act. This generic understanding of threats and vulnerabilities is not translated into an understanding of risks specific to their own institutions. The fact that until recently the AML/CFT regime was primarily rules-focused with extensive preventive measures exemptions has limited the incentives of AIs to mitigate risks and build risk-focused AML/CFT programs. Smaller FIs are initiating or improving their risk assessments, following the new requirement to develop and implement RMCPs. RMCPs that are in place reflect understanding of client risk, whereas other risk factors (e.g., product/service risks) seem to be considered only to a limited degree.

316. While VASPs (CASPs) are not regulated in South Africa, the three largest VASPs generally understand AML/CFT obligations[55] and show a proper understanding of their ML risks. These risks include high volumes of deposits, followed by sending and selling behavior in short intervals by clients from rural areas logged in from foreign jurisdictions (e.g., China) or scenarios in which the funds do not align with the client profile (mostly age and geographical background). The top ML threats identified by the VASPs relate to darknet transactions, fraud, child abuse, pornography, and illegal gambling. These entities could place more focus on mitigating the risk that criminal funds may be externalized utilizing methods that fall outside of traditional payment systems.

[54] Most of these banks performed a first institutional ML risk assessment in 2015 followed by a refresher exercise in 2019. Some expressed their intention to implement regular updates (every 12–18 months) starting from 2019 onwards.

[55] There is a legal obligation on VASPs, like any other business, to report suspicious transactions to FIC (FIC Act, s.29).

317. Amongst regulated DNFBPs, only casinos seem to understand their AML/CFT obligations to a large extent.** Most DNFBP sectors seem to have a basic understanding of customer identification and verification requirements, where the casinos' understanding is more developed. Estate agents and attorneys tend to heavily rely on other partners in the AML-chain (e.g., banks or other DNFBPs involved in the transaction) to effectively perform these requirements even where this is not allowed. Based on discussions with the DNFBP sectors, assessors believe this comes from a limited knowledge of applicable (amended) FIC Act requirements, following the removal of many exemptions applicable under the old FIC Act and limited supervision. The new RMCP requirement is a big challenge for most DNFBPs to understand, but the casino sector may be considered a more positive outlier.

318. DNFBPs' have an undeveloped understanding of ML risks that varies significantly. While casinos are better, estate agents and attorneys are basic to limited in their knowledge of ML risks based on vulnerabilities such as the use of cash and the failure of their controls. ML threats (e.g., corruption, environmental crimes) are recognized to a much lesser extent. DNFBPs do not perform ML risk assessments that include a sufficient range of inherent risk factors but seem to be limited to an assessment of required controls. Casinos are better in assessing ML risk but need to take further steps to improve their RBA. The lack of adequate supervision compounds this issue for attorneys. Estate agents and attorneys do not appear to adequately identify the ML risks associated with real estate.

319. TF risk is only to some extent understood by AIs, mainly referring to typologies and obligations and often primarily based on TFS screening obligations. FIs may apply groupwide programs and refer to relevant global or regional developments, but do not seem to adequately identify and understand their TF risk in the context of South Africa to effectively mitigate this risk. This follows the very limited attention placed on TF risk by the authorities.

Application of risk Mitigating Measures

320. The larger banks apply mitigating measures commensurate with their risks to some extent, but the majority of AIs do not, as they fail to adequately assess their ML/TF risks (see previous page). RMCPs viewed by the assessment team can be predominantly categorized as rule-based policies and procedures manuals and not (or at least not demonstrated to be) founded on an adequate assessment of the entity's risks.

321. Major threats and vulnerabilities are addressed with the predominant focus on rule-based compliance with regulatory requirements rather than mitigation of ML/TF risk. For example, AIs typically address and take measures to mitigate the risk of laundering proceeds of corruption with an exclusive focus on complying with FIC Act PEPs requirements and not by proactively monitoring client relationships and transactions, beyond the PEP status of the client (e.g., considering particular transaction, client, and product- or service-related factors such as transactions related to government procurement contracts where a PEP is not necessarily involved). Only some banks are applying risk-based mitigating measures through monitoring or applying surveillance models aligned with specific corruption threats of jurisdictions in which they operate.

322. Where no specific detailed AML/CFT controls are required, most AIs do not take focused mitigating measures to address high-risk scenarios as envisaged under an RBA. For example, most AIs do not address risks associated with use of cash, despite it being an important vulnerability of the South African financial system as there is no specific legal requirement for mitigating risks associated with cash. The absence of such a requirement should not prevent AIs from taking risk-mitigating measures but only banks seem to do so to some extent. One bank indicated that it is in a process of limiting or even exiting cash business to address the issue. As a result, only two percent of the total value payment flow of this important market participant is still in cash, digitizing its cash services to further identify vulnerabilities. Most AIs indicated that they mitigate the risks, including those associated with the use of cash, by filing CTRs.

323. Many FIs assess client risk in the process of developing their RMCPs, in that different levels of CDD are performed in accordance with the risk rating of the client, but doubts regarding effectively implementing an RBA exist. AIs seem to consider a limited set of risk factors or indicators in assessing clients' ML/TF risks. The PEP status of a prospective client is often the only—or one in few—risk factor(s) considered when determining client risk profile, particularly at the onboarding stage. This is reflected in the very low share of clients categorized as high and very high risk at the larger banks. FIs tend to apply more client risk factors during the ongoing monitoring stage when determining adjustment of the risk profile, though this does not appear to assist FIs in classifying clients as high or very high risk, given the low overall percentage. The necessary enhanced measures may therefore not always be applied from onboarding onwards.

Application of CDD and Record-Keeping Requirements

324. B

asic CDD and record-keeping measures are generally applied by many AIs to a large extent. Supervisors observed that larger FIs have enhanced systems over the years for identifying and verifying clients, as well as clients' sources of funds and of wealth. Developments in applying digital identification initiatives at larger banks are also positive.

325. While banks in practice undertake BO enquiries seriously, they only seem to adequately implement the BO requirements to some extent. According to FIs and supervisors, FIs are challenged to implement requirements to identify, obtain, and verify adequate BO information, particularly for complex structures. The requirements became enforceable in 2019, and both the SARB:PA and the FIC observes that the BO recorded by FIs is not always a natural person. The challenge is largely related to a lack of transparency in corporates (see section on Legal Persons and Arrangements). Where public information is available it is utilized by banks,[56] but they expressed that there are no other ways to obtain readily available verifiable information beyond self-declaration by the client. To obtain relevant information, some FIs request clients to submit information on group structure, financial statements, voting rights, along with attestations from accountants or auditors, therefore leaning on indirect information regarding ownership. Some FIs

[56] Banks have an online process to verify ownership with CIPC (share percentages and directors), but this information is not always accurate or up-to-date, and therefore needs comparison with ownership information as provided by customer.

state they—as a last resort—obtain information on control by senior management. Regarding trusts, information from the Master's Office is obtained to verify BO, but this does not always contain all relevant BO information (see section on Legal Persons and Arrangements). Only some FIs—banks being amongst them—explicitly apply the principle to refuse onboarding when submitted information is insufficient or just absent to establish the identity of the BOs. The identification and verification of the identity of a natural person controlling an individual is not addressed in the FIC Act at all, as no obligation exists, and given the previously described rule-based compliance approach applied by many AIs (see page103), assessors have doubts as to whether adequate measures are being taken.

326. To assess influence exerted over a legal person not through direct means, some banks said that they rely on information obtained during their ongoing monitoring exercises when refreshing the BO information previously obtained. Based on network analysis and financial flows, they seek to understand the linkages between these flows and try to establish the beneficiaries of the funds which may indicate such BO. The larger banks are also beginning to implement behavioral analytics, which may help to distinguish real companies from shell companies as they behave differently.

327. FSPs, CIS managers, attorneys, and estate agents do not yet adequately apply CDD measures as the related obligations have only been fully enforced since April 2019. Before the withdrawal of the exemptions under the FIC Act (2017), FSPs and CIS managers could—as a secondary AI—rely on the primary AI involved in a transaction to perform identification and verification. Those AIs are struggling now to implement CDD measures and to apply their own judgement as to whether information is sufficient in relation to risks. This is especially the case for sole proprietors. The CDD obligations on attorneys have also expanded. The sector is still working to implement the full set of CDD obligations, let alone the BO challenges in complex structures. Estate agents seem to be more transaction focused ('to close the deal') than focused on implementing CDD measures as required, and almost completely rely on other parties involved in transactions (banks and attorneys) to carry out CDD even where those AIs are not necessarily as informed about both selling and buying sides of the transaction. They do not identify sellers who are not their customers.

328. The larger banks and insurers—overall, the FIs with a developed risk understanding—and ADLAs seem more effective in implementing ongoing monitoring requirements for clients and transactions. Transaction monitoring systems are often combined with network analysis, and initiatives are underway to allow analyses of potential deviant behavior, given the risk profile as established per client and related transactions. Some banks have implemented transaction monitoring systems that generate a fair range of alerts to be examined for follow up, such as adjustment of client risk profiles and reporting suspicions.

329. Owing to their basic understanding of the ML risks, smaller FIs (including FSPs and CIS managers) and casinos conduct ongoing monitoring to some extent, predominantly from a compliance and CTR perspective. However, most FIs' monitoring activities are not sufficiently risk focused and seem to almost exclusively focus on ensuring that transactions reaching the threshold

of R25,000 are detected and reported as CTRs. Ongoing monitoring by DNFBPs other than casinos is done to a negligible extent, mostly due to an underdeveloped understanding of risks and obligations.

Application of EDD Measures

Application of EDD Measures – (a) PEPs

330. Systems and measures to determine whether a customer or BO is a PEP are effective to some extent. Most AIs take such measures to the extent as prescribed by the FIC Act, notwithstanding the fact the legal definition of PEP is deficient because it only includes persons holding such position in the preceding 12 months. Only FIs with a developed understanding of risk, seem to go beyond the strict legal requirement and apply a broader approach. Domestic PEPs at the provincial and municipal level are not consistently identified by AIs, mostly due to the fact that AIs use screening systems and databases that do not necessarily include such PEPs. This is a concern given South Africa's risk profile compounded by a lack of transparency over corporate ownership and given the level of corruption over recent years. While the higher risk and subsequent need to take additional mitigating measures is acknowledged by many AIs, only some (mostly banks) take such additional measures and apply network screening tools to identify these domestic PEPs and persons associated to PEPs. Overall, screening initiatives are predominantly based on ad hoc information requests from the authorities (e.g., from the FIC or from the Zondo Commission) and to a lesser extent on systematic screening efforts at onboarding of clients, and even much less on an ongoing basis on the existing client base. This means that these AIs may have unidentified PEPs in their client base that are not subject to mitigating measures.

331. When a client is determined to be a PEP, AIs seem to effectively take enhanced measures to a large extent. Such measures consist of establishing source of income and of wealth, obtaining approval from senior management to establish the relationship, and often enhanced monitoring of the relationship.

Application of EDD Measures – (b) Correspondent Banking

332. Where applicable, most banks apply enhanced measures to mitigate risks stemming from CBRs to some extent. This is primarily done from a business need perspective by mirroring or relying on what their overseas clearing system partners are doing rather than actively managing their own CBR exposure from an AML/CFT perspective. Mitigating the risks stemming from such relationships is seen to be an important issue for banks as de-risking may be a serious threat for South African banks. However, some larger banks have themselves de-risked CBRs with banks in the region because they consider the risk to be unacceptably high. Some (larger) banks that do not de-risk such CBRs have face-to-face onsite engagements with their counterparts at the onboarding stage and periodic intervals thereafter while treating such relationships as higher risk to perform EDD to some extent.

Application of EDD Measures – (c) New Technologies

333. Most banks do not take enhanced measures to address identified higher risk of VASPs, but de-risk VASPs mainly because VASPs are unregulated and unsupervised in South Africa. Three banks as of the onsite accept VASPs as clients and identify them as high risk. Other banks recognize that they may not be in a position to fully understand the activities and associated ML/TF risks of VASPs and therefore seem to avoid any exposure, including by refusing onboarding. Such recognition is not necessarily based on an appropriate assessment of ML/TF risks of VASPs. However, enhanced measures are adequately taken to mitigate the risk that bank clients might use their accounts to trade in crypto assets.

334. On the other hand, banks have incorporated FinTech products in line with their RBAs to inter alia boost financial inclusion. These product offerings are subject to conditions and transaction thresholds, based on an assessment of ML risk. Some banks ensure new product launches are triggers to refresh their business risk assessment.

Application of EDD Measures – (d) Wire Transfers

335. In general, banks apply specific measures regarding wire transfers to a large extent, despite needed adjustments to CMA electronic fund transfers (EFTs) and deficiencies in capturing beneficiary information. A deficiency was identified and addressed in 2019 by regulators and FIs concerning EFTs between South Africa and other CMA countries (see **Error! Reference source not f ound.** and **Error! Reference source not found.** for transaction volumes). These EFTs were, until very recently, regarded from a payment system perspective as domestic, whereas they are de facto and from a legal (and R.16) perspective cross-border. As of the onsite, this systemic weakness was being addressed through applying additional systems and rules[57] to treat them as cross-border EFTs. Domestic payments are not wired using SWIFT, and therefore the solution consists of adding a supplementary file to every CMA-related EFT to ensure the level of information is according to the requirements on cross-border EFTs. As these initiatives were in progress as of the onsite, effectiveness cannot be established. SARB confirms that the results of the application of the additional systems and rules need to be assessed through supervision as well. Even though the volume of transactions within the CMA is rather limited for South African banks (as compared to their overall international transfers), some have de-risked CMA-related EFTs.

[57] CMA active banks were challenged to implement the additional systems and rules ultimately 20 October 2019. Authorities have also prepared a draft Directive 01 of 2019 and related draft GN in terms of the FIC Act, 2001 (Act 38 of 2001) in respect of the FATF Recommendations for EFTs; September 23, 2019.

Table 5.1. South Africa: CMA: Total Inwards Transaction Values and Volumes in 2018 (excl. card transactions)

Country	Amount	Transactions	Average Transaction Value
Inwards:			
Lesotho	R 14 billion ($ 1 billion)	63,142	R 221,722 ($ 15,437)
Namibia	R 45 billion ($ 3 billion)	21,039	R 2,138,885 ($ 139,370)
Eswatini	R 23.8 billion ($ 1.7 billion)	49,009	R 485,625 ($ 31 621)
Total:	**R 82.8 billion ($ 5.8 billion)**	**133,190**	R 622,419 ($ 40,528)

Table 5.2. South Africa: CMA: Total Outwards Transaction Values and Volumes in 2018 (excl. card transactions)

Country	Amount	Transactions	Average Transaction Value
Outwards:			
Lesotho	R 12 billion ($ 0.8 billion)	611,741	R 19,616 ($ 1,277)
Namibia	R 107 billion ($ 7.4 billion)	37,054	R 2,887,677 ($ 188,026)
Eswatini	R 16 billion ($ 1.1 billion)	9,999	R 1,600,160 ($ 104,191)
Total:	**R 136 billion ($9.5 billion)**	**658,794**	**R 206,438 ($ 13,442)**

336. Notwithstanding the CMA issue, the SARB:PA identified that some FIs seem to have issues with capturing information on originator's physical address on cross-border EFTs, and it is not established that necessary originator information in domestic (including CMA) EFTs can be provided within three days.

337. VASPs are not subject to the EFT requirements yet and are not effectively applying specific measures. They do not voluntarily apply the relevant requirements.

Application of EDD Measures – (e) TFS-TF

338. Generally, AIs indicate they screen (prospective) clients at onboarding and transactions (real time or daily) for potential hits with relevant lists, but there is limited proof of effective implementation. AIs mentioned that they would apply necessary screening systems and procedures to ensure reporting hits against these lists to the FIC, with transactions not executed and some of them indicated they will freeze the funds until further notice from the FIC. However, no funds have been frozen up to the end of the onsite, nor any information on effective implementation of the screening systems and relevant follow-up (e.g., false positives, relevant monitoring reports, or audit reports) shared with assessors. The SARB:PA found improvements in sanction screening results since 2014 but concluded that many FIs required further improvements as of 2017. The SARB:PA confirms that banks apply a range of screening systems, but nearly all monetary sanctions issued to FIs by the SARB:PA up to 2019 related to deficiencies in TFS controls. There are no indications VASPs are adequately implementing TFS controls.

Application of EDD Measures – (f) High-Risk Countries

339. Many FIs and DNFBPs apply EDD measures only regarding the jurisdictions as listed by FATF and subsequently communicated via the FIC website or jurisdictions related to TF sanctions. Only a small number of FIs (larger banks and larger ADLAs) classify jurisdictions with strategic AML/CFT weaknesses as higher risk based on their own risk assessment. Overall, AIs seem to underestimate the risks of operating internationally, in particular on the African continent, and therefore do not initiate EDD to mitigate these risks.

Reporting Obligations and Tipping Off

340. Overall, the larger banks and ADLAs meet their ML reporting obligations to a large extent, while other high-risk sectors fail to do so commensurate with their risk profiles. Banks and ADLAs report by far the most s.29 reports,[58] including per AI: in 2018/2019 banks reported 175,580 and ADLAs 96,748, respectively—59 percent and 37 percent, or 96 percent of the total number of s.29 reports filed in this period. This means an average of 5,164 per bank and 5,691 per ADLA. Most of the reports in the banking sector come from the larger banks, with other banks showing a very mixed picture. One (top 10) bank, offering high-risk products to high-risk clients, files around 450 s.29 reports a year, where the bank next in size, but with a lower risk client base and product portfolio, files around 40,000 s.29 reports a year. These outcomes do not meet expectations from a risk perspective, where banks with higher risk client and transaction profiles could be expected to file more reports than banks with lower risk profiles when the size of institution(s) is similar. From a materiality perspective, it is expected that FSPs and CIS managers would file more reports than currently reported by these sectors. Where casinos are the best DNFBP reporters, estate agents, attorneys, and TSPs file a very low number of reports (see Table 5.3). Underreporting may stem from an underdeveloped understanding of ML/TF risks and obligations and the absence of effective supervision. VASPs file STRs to some extent.

341. FIs are improving their transaction monitoring systems to disclose suspicious transactions in a risk-sensitive manner. Supervisors and FIs noted failures in implementing effective automated transaction monitoring systems, where applied parameters were often insufficiently adjusted to risk profiles of clients and transactions as they were set to vendor settings. Authorities addressed the issue by issuing Directive 5 of 2019,[59] and FIs are in the process of implementing such guidance as of the onsite to further improve transaction monitoring controls and governance to be more risk sensitive. However, during the onsite, many FIs (as well as DNFBPs) indicated that they are compliant once they file CTRs correctly, without paying sufficient attention to potential suspicions. Furthermore, some smaller FIs use less efficient manual transaction monitoring systems.

[58] This includes STRs, SARS, TFTRs, TFARs, and batch reporting.

[59] FIC Directive 5 of 2019 on the usage of an automated transaction monitoring system for the detection and submission of regulatory reports to the FIC in terms of s.29 of the FIC Act, issued March 29, 2019.

Table 5.3. South Africa: Number of STRs and Suspicious Activity Reports Filed per Type of AI: Five Years ending March 31, 2019

Type AI/RI	2015	2016	2017	2018	2019	Total	Percent of Total	Reports per AI/RI (average) 2019
Financial Institutions								
Bank	95,744	98,054	193,609	209,020	175,580	578,209	59.15%	*5,164*
Mutual Bank	4	3	22	78	70	170	0.02%	*23.3*
Postbank	379	154	83	60	363	506	0.05%	*363*
ADLA	143,869	58,338	155,185	108,722	96,748	360,655	36.90%	*5,691*
Authorized Exchange User	12	27	36	127	106	269	0.03%	*0.7*
CIS managers	153	186	125	64	29	218	0.02%	*0.5*
FSP	18,140	13,310	2,41	1,164	2,294	5,868	0.60%	*0.2*
Ithala	0	2	1	0	1	2	0.00%	*1*
Long-term insurers	151	180	114	110	205	429	0.04%	*2.6*
Money Lender Against Securities	7	9	5	8	8	21	0.00%	*0.1*
Total Financial Institutions	**258,459**	**170,263**	**170,263**	**351,59**	**319,353**	**275,404**	96.81%	
DNFBPs								
Gambling (excl. casinos)	600	1030	213	210	232	655	0.08%	*0.07*
Casinos			1160	1,683	1,832	4,675	0.46%	*46.97*
Estate agent	15	11	6	22	71	99	0.01%	*0.002*
RDs	11	63	3	26	98	127	0.01%	*0.4*
Attorneys	162	265	133	123	430	686	0.07%	*0.02*

Table 5.3. South Africa: Number of STRs and Suspicious Activity Reports Filed per Type of AI: Five years ending March 31, 2019 (concluded)

TSPs	10	10	22	7	15	44	0.00%	*0.05*
Total DNDBPs	**798**	**1379**	**1537**	**2071**	**2678**	**6,286**	0.64%	
Other Sectors								
MVDs	8141	8721	5,271	9,118	10,274	24,663	2.52%	*2.6*
Other Business Entity	0	0	14	97	78	189	0.02%	
Total Other Sectors	**8141**	**8721**	**5,285**	**9,215**	**10,352**	**24,852**	2.54%	
Grand Total	**267,398**	**180,363**	**358,412**	**330,639**	**288,434**	**977,485**	100.00%	

Source: The FIC.
Note: For 2015 and 2016 the STRs filed by casinos are included in the broad gambling category.

342. According to the FIC, the best quality reports are filed by the larger banks (but still need improvement) and the worst by attorneys and estate agents. The volume of reports has decreased over the last two years, while the quality has gone up, according to the FIC. The banking sector could further improve by providing better information to link both ends of the transaction. The main challenge for ADLAs is to include more context in their reports, and estate agents should improve by disclosing information on the person(s) buying the property where this party is a corporation, or a complex structure is involved. The FIC indicated that this is the same with the attorneys, while this sector also needs to improve disclosure of information on transactions going through their trust accounts.

343. There is no issue identified with regard to tipping off. Many FIs cite problems with sharing client and transaction related information with other FIs (even within the same financial group) based on a strict legal interpretation of the FIC Act tipping off prohibition.

Internal Controls and Legal/Regulatory Requirements Impeding Implementation

344. FIs generally apply internal controls and procedures ensuring compliance with the requirements depending on their ability to apply an RBA. Where applicable, this is done at group level. Most AIs have compliance officers, but DNFBPs, except the large casinos and smaller nonbanking FIs, have problems setting up an independent compliance function given their size and limited knowledge of such controls. Some FSPs address this problem by outsourcing the compliance function, but others seem to operate with no compliance function at all. Banks in general seem to

have set up a Three Lines of Defense model[60] attributing an independent monitoring function to the compliance department. Most banks state that they provide for direct reporting lines from compliance to the board. Some larger banks have (several layers of) compliance committee structures that may block effective reporting due to organizational and formal constraints which may hinder the ability of senior management to engage sufficiently. Implementation of the compliance function is less effective at many of the smaller banks due to a combination of understaffing, unsophisticated monitoring systems, and an inadequate RBA. All larger FIs and DNFBPs employ an independent audit function, most of them performing AML/CFT-related audits yearly. Limitations following a less developed RBA are also relevant as far as the focus of these third-line activities is concerned.

345. There are concerns regarding application of adequate controls by FIs with subsidiaries and branches abroad. The FIs themselves report that they apply the stricter AML/CFT standards in home-host situations, often but not exclusively applying the South African requirements through setting up group-wide AML/CFT programs and standards. It was not possible for assessors to establish the adequacy of group-wide application beyond the self-declared strength of such programs and controls. Moreover, supervisors shared their concerns that the larger banking groups' controls in their foreign entities do not seem adequate in all instances. Supervisors agreed they had to further address these concerns as they have performed a limited number of onsite inspections at subsidiaries and branches abroad. Moreover, such inspections, even if triggered by issues identified at the FI's HQ, were conducted as stand-alone inspections rather than as a part of consolidated supervision of groups (see section on Supervision). This is a concern, particularly given the vast pan-African and global network of the large banking groups.

346. AIs with a dedicated compliance function organize and conduct AML/CFT-related training for their staff. However, given the structural shortcomings in the implementation of an RBA as mentioned above, assessors doubt whether training focused on ML/TF risks and RBA at AIs with an underdeveloped understanding of risk are adequate, in particular, to change to an RBA.

347. FIs report an obstacle in the sharing of transaction-related information between FIs involved in a transaction—even within the same financial group—as the POPI Act does not allow for adequate exchange of information for the purposes of effective transaction monitoring. Sharing of information between FIs is only allowed under that Act if it can be considered to be processing in order to comply with obligations imposed by law. This may cause a legal issue as essential AML/CFT and related obligations are imposed by secondary legislation (e.g., regulations and directives) and therefore are not within the confines of the POPI Act. The financial sector in cooperation with the regulators intend to launch a public private financial information sharing partnership (SAMLIT) to address these issues.

C. Overall Conclusions on IO.4

[60] In the Three Lines of Defense model, management control is the first line of defense in risk management, the compliance oversight functions are the second line of defense, and independent audit is the third.

348. FIs overall show an acceptable understanding of their AML/CFT obligations. The larger banks show a developed understanding of their ML risks as well and therefore seem better at implementing mitigating measures commensurate with their risks. Smaller FIs show a basic understanding of ML risks and are transitioning from a rule-based approach to an RBA. It is of concern that estate agents and attorneys have an underdeveloped understanding of risks and obligations given ML typologies in South Africa, while some other potentially high-risk sectors are not fully AML/CFT regulated and supervised. Overall, TF risk is understood to some extent. AIs apply basic CDD measures to a large extent, but all are challenged to implement BO requirements adequately. The larger banks seem to apply a broader range of CDD measures that could be regarded as somewhat sufficient, including risk-based ongoing due diligence, as well as enhanced or specific measures. While AIs take enhanced measures to mitigate risks posed by identified PEPs, there are concerns regarding determination of the PEP status of clients and BOs in general, partially due to a deficient legal definition. The larger banks and ADLAs meet their reporting requirements to a large extent, where other high-risk and materially important sectors underreport substantially. FIs generally apply internal controls and procedures ensuring compliance with the requirements depending on their ability to apply an RBA. Given South Africa's regional and economic position, assessors emphasize the need to ensure that larger banks adequately apply their group-wide AML/CFT programs and controls at subsidiaries and branches abroad. Overall, major improvements are needed.

349. South Africa is rated as having a moderate level of effectiveness for IO.4.

SUPERVISION

A. Key Findings and Recommended Actions

Key Findings

- While fit and proper criteria are in place for many sectors, these often do not apply to beneficial owners. Even though there was an isolated case where a bank application was rejected due to BO issues, the authorities could not demonstrate that they implement adequate controls to prevent criminality from infiltrating FIs and DNFBPs. Most regulators do not conduct criminal checks or verify self-declarations of applicants, although police criminal clearance certificates are required for applicants in the ADLA and CIS manager sectors. Unlicensed cross-border MVTS are not being systematically identified, sanctioned, or removed from the market.

- Supervisors' understanding of ML risks varies with the SARB:PA having a relatively good understanding of sector-level risks, followed by SARB:FinSurv, while others understand the risks in the potential high-risk DNFBP sectors (estate agents, attorneys, and TSPs) to a limited or negligible extent. Banks and ADLAs are the only AIs rated for ML/TF risks but with limited consideration of their inherent risks. All supervisors understand AML/CFT controls better than inherent and residual ML/TF risks and their TF risk understanding is very limited.

- The SARB:PA's supervision of the materially important banking sector checks compliance with AML/CFT requirements thoroughly but not yet using a proper RBA. The SARB:FinSurv's inspections adequately cover ADLAs but are based on risks only to a limited extent. For all other supervisors, inspections are too infrequent or rare to be effective, and attorneys are subject to essentially no AML/CFT oversight. These inspections are not prioritized based on risks and focus on the presence of basic controls (such as appointing a compliance officer) rather than the soundness of AML/CFT programs. The effectiveness of supervision by the FSCA and the EAAB (for estate agents) is hampered by a severe lack of resources. The SARB:PA and the FSCA coordinate or share information with each other on AML/CFT, but not yet on supervision of FIs in different sectors that belong to the same group, nor do they coordinate their inspections.

- The SARB:PA has imposed a range of remedial actions and sanctions against banks for AML/CFT breaches, but the penalties have not always been proportionate or dissuasive. Most other supervisors, except those for attorneys and casinos, apply remedial actions, but the sanctions imposed are often too low and infrequent to be dissuasive or effective. Financial supervisors demonstrated some impact in improving FIs' compliance with basic obligations. Enforcement of the amended FIC Act only started in April 2019, and supervisory impact that improves compliance with the new risk-based obligations was not demonstrated.

- The FIC provides a wide range of AML/CFT guidance and conducts outreach nationally, supplemented by other supervisors, to promote a consistent understanding of AML/CFT obligations in the FIC Act. Only limited information has been provided to help the private sector identify and understand ML/TF risks.

- Some financial sectors, DNFBPs including CSPs and DPMS which are potentially high risk, and VASPs are not subject to most AML/CFT obligations or supervision. Their risks are not understood or mitigated.

Recommended Actions

- All regulatory authorities should subject beneficial owners to fit and proper tests and verify that directors, senior managers and beneficial owners or their associates are not criminals as part of market entry controls and apply this standard upon renewal of current market participants and on an ongoing basis.

- Unlicensed cross-border MVTS should be proactively identified and addressed either through sanctioning or removal from the marketplace (including through improved coordination between the SARB:FinSurv and the SAPS) or by bringing them into the AML/CFT framework through licensing or registration; providers of domestic MVTS should be subject to licensing or registration.

- All supervisors should improve their understanding of ML/TF risk, in particular inherent and residual risks for both sectors and institutions, including through collecting and analyzing inherent risk information.

- The SARB:PA and the SARB:FinSurv should do better in prioritizing and scoping their onsite inspections on the basis of ML/TF risk, which should be informed by offsite monitoring and findings from previous inspections. All other supervisors should start following this approach. The SARB:PA should ensure that higher-risk FIs are inspected with more frequency consistent with their risks. During onsite inspections, supervisors should focus more on the effectiveness of controls, including on the obligations to obtain and hold accurate and up-to-date information on beneficial owners of companies and trusts, given the risk context of the institution, rather than the presence of controls.

- Financial supervisors should supervise financial groups for AML/CFT on a consolidated basis, including international operations and coordinate their supervision of FIs in different sectors which belong to the same group.

- The authorities should ensure the level of oversight of FSPs (Cat II), CIS managers, attorneys, estate agents, and TSPs are commensurate with their ML/TF risk profiles, including by substantially increasing the supervisory resources and capacity of the FSCA, the EAAB, the Legal Practice Council (LPC), and the FIC.

- All supervisors should use a full suite of enforcement measures including monetary penalties to sanction AML/CFT breaches, dissuasive and proportionate to the size of the entity and severity of the breaches.

- More sector specific guidance (including typologies) should be provided to help the private sector identify and understand ML/TF risk.

The relevant Immediate Outcome considered and assessed in this chapter is IO.3. The Recommendations relevant for the assessment of effectiveness under this section are R.14, 15, 26–28, 34, 35, and elements of R.1 and 40.

B. Immediate Outcome 3 (Supervision)

350. As detailed in chapter 1, when considering the effectiveness of South Africa's risk-based AML/CFT supervision system, the assessment team assigned the highest importance to banks, followed by attorneys and estate agents. ADLAs, asset managers (FSP Cat II), CIS managers, and TSPs were considered to be of a medium level of importance. Less importance was given to life insurers and financial advisors (FSP Cat I).

351. Some FIs and DNFBPs (including CSPs and DPMS which are potentially high-risk), and VASPs are not subject to most AML/CFT obligations and are not supervised (see para. 133. and c.1.6). Their risk exposures are not understood, except for some awareness of the abuse of VASPs for ML and TF, nor mitigated by any supervisor. Except for some CFIs and accountants, these sectors are not subject to regulatory frameworks, so there are no market entry controls to prevent criminals from owning or controlling the businesses.

Licensing, Registration, and Controls Preventing Criminals and Associates from Entering the Market

352. South Africa has market entry control systems in place for FIs and some DNFBPs, but their robustness varies significantly by sector. While fit and proper criteria are in place for many sectors, they often do not cover beneficial owners. Most regulatory authorities require a declaration of previous convictions, but no independent verification is done.

353. The SARB:PA has some market entry controls in place to prevent criminals from entering the banking and life insurance sectors but is yet to implement fit and proper criteria for significant owners of banks and does little to validate the information submitted. Significant shareholders (owning 15 percent or more) of banks, which may not necessarily go to the level of beneficial owner, must be fit and proper; however, the development of this criteria was ongoing (jointly with the FSCA) as of the onsite. For directors or executive officers who are subject to existing fit and proper criteria, the SARB:PA relies on self-declarations of previous convictions, if any, without verifying these with LEAs. Until 2019, the SARB:PA's primary method to assess licensing applications was open source searches for negative media coverage. In 2019, the SARB:PA began to engage with the FIC as part of its licensing process, and recently began screening for PEPs and TFS listings and requesting information from international counterparts as part of its licensing due diligence as necessary. From 2014 to 2019, the SARB:PA received 11 applications for new licenses or acquisition of banks, approved 5, rejected 2, and 4 are pending. Despite the absence of fit and proper criteria for beneficial owners, the SARB:PA, when reviewing a proposed acquisition of an existing licensee, conducted due diligence on the proposed new beneficial owner and found links to *"State capture",* based on which it rejected the application. The SARB:PA indicated that rejection of key persons (which generally include directors and senior management) happens due to fit and proper concerns often, and may take place during application to form or acquire a bank or during approval of the appointment of senior persons on an ongoing basis, but it is unclear how many rejections are due to issues related to criminality. The SARB:PA also rejected the appointment of a senior person having a criminal record to a cooperative bank. However, an instance of an existing bank deeply involved in *"State capture"* raises questions about the robustness of safeguards to prevent criminality from operating in the banking sector on an ongoing basis. In the case of life insurers, directors, senior managers, and significant owners are also subject to fit and proper requirements and criteria. The SARB:PA actively monitors for unlicensed deposit taking institutions through its Illegal Deposit Taking Unit and investigated 156 schemes between 2014 and 2018.

354. The SARB:FinSurv approves ADLA applications if the shareholders (that may not be natural persons) and directors are deemed to be fit and proper, but these controls do not apply to beneficial owners or senior managers. The SARB:FinSurv requires police criminal clearance certificates for applicants and conducts screening for TFS status. Out of the 24 applications for ADLA received between 2014 and 2018, 1 was declined in 2017 for fit and proper concerns in respect of 1 shareholder who had previously submitted fraudulent financial statements resulting in the withdrawal of the authorization of that ADLA. According to the SARB:FinSurv, reports of unlicensed cross-border MVTS activity are referred to SAPS but were not often actioned. Overall, the authorities

could not demonstrate that unlicensed market participants are being effectively identified and sanctioned.

355. The FSCA's market entry controls in the securities sector suffer from similar weaknesses as those of the SARB:PA. The FSCA requires a self-declaration of previous convictions by directors, members, partners, and trustees ("key individuals")—shareholders and beneficial owners are not subject to this disclosure. In the FSP sector, the FSCA does not verify self-declarations. In the CIS manager sector, self-declarations are supported by a police clearance certificate. The FSCA authorized 6,918 key individuals in the FSP sector from 1 April 2014 to 31 March 2019, of which 44 (0.64 percent) were later debarred for honesty and integrity issues. Thus, while gaps may exist with the initial licensing process, the authorities monitor the population for fitness and propriety by reacting to complaints filed with it. The FSCA also proactively acts against unlicensed or unregistered business identified through adverse media coverage, a dedicated hotline, and referrals. To apply for authorization as an AU of the JSE, a criminal self-declaration from directors and shareholders with 10 percent ownership or higher must be provided, but this is not verified.

356. South Africa's licensing framework for casinos appears solid, but it is unclear how fit and proper checks are done, including on groups. Each PLA uses its own criteria for fitness and propriety, which are not fully consistent and the persons who must be fit and proper vary amongst the PLAs. At least some PLAs indicated that they validate self-declarations of applicants, but it is unclear how this is done and whether other PLAs verify such information. As the market is dominated by a few large groups, PLAs consult each other when an existing licensee of one province applies for license in another, but it is unclear whether the PLAs' fit and proper test extends to persons who control the group beyond the entity (licensee) level. Between 2016–2019, one license application was rejected as a result of a fraud conviction of a key individual. PEP status is considered as part of the assessment. PLAs and LEAs actively work together to shut down illegal gambling ventures including those online.

357. Market entry controls to preventing criminal elements from operating in other covered DNFBP sectors are inadequate. While there are integrity-related requirements for estate agents, TSPs, and attorneys to be authorized, the criteria used for attorneys and TSPs are unclear. Regulators generally rely on self-disclosure without verification.

Supervisors' Understanding and Identification of ML/TF Risks

358. The level of identification and understanding of ML/TF risks varies by supervisor, with the SARB:PA demonstrating the strongest understanding at both a sector and institution level. Interim SRAs were concluded by the SARB:PA, the SARB:FinSurv, the FSCA, and the FIC (on several DNFBP sectors) shortly before the onsite and fed into the NRA. DNFBP supervisors were not involved in the formulation of the SRAs for their sectors.

SARB:PA

359. The SARB:PA has a relatively good understanding of the ML risks impacting banks at the sector level, but this is not the case for TF risks. Before the SRA, the SARB:PA used information from public sources, AML/CFT meetings (see below), and inspections to inform its views on the threats and vulnerabilities. The SRA exercise provided an opportunity to further its understanding of risks at the sector level by drawing from banks' feedback provided in SRA surveys. The ML threats identified by banks in the SRA, including fraud, corruption, tax evasion, environmental crimes, and prevalence of cash in the economy, correlate to the SARB:PA's understanding. The SARB:PA's views on sector vulnerabilities of banks are reflected in a risk matrix (see below) it uses to risk-rate banks, in which customers, products and services, and delivery channels considered to be inherently high risk by the SARB:PA are identified. These include PEPs, corporates, non-residents, private banking, cross-border wire transfers, trade finance, online banking, etc. No geographic risks have been identified. Though some of the higher risks identified may be relevant to TF, the SARB:PA's understanding of threats or vulnerabilities specific to TF is underdeveloped.

360. While the SARB:PA understands risks at the level of the banking sector, comparative understanding of risks at the institution level is less developed. The SARB:PA has used a risk matrix to assess and risk-rate banks since 2016. The matrix encompasses analysis of inherent risks, sizes, adverse media coverage, and quality of controls. Apart from findings about AML/CFT controls from previous supervisory activity (inspections, AML/CFT meetings, etc.), inputs are primarily drawn from prudential returns rather than systematic information gathering on ML/TF inherent risks. Thus, the analysis of inherent risks is limited to whether the bank is exposed to high-risk customers, products, services, or delivery channels mentioned in the previous paragraph without assessing the extent of such exposure. It does not consider geographic risk factors. The SARB:PA acknowledges that more data should be considered, and the SRA exercise highlighted the need for improved offsite monitoring to further its inherent risk understanding at the institution level. The matrix does not consider TF risks beyond controls that apply to both AML and CFT. The matrix generated its first set of risk ratings in 2016, which has only been updated once in 2019. Thus, it is unlikely to have captured the evolving risks in a dynamic manner. As of the onsite, there were 4 banks rated very high for ML/TF risk (the "big four"), 3 banks rated high, and 27 rated medium. The three mutual banks were all rated medium. It is noteworthy that the bank revealed to be involved in *"State-capture"* was risk-rated medium, even after concerns had come to light.

361. The SARB:PA is developing its understanding of the ML/TF risks for life insurers at the sector level and had not yet risk-rated institutions as of the onsite. Since taking responsibility for insurance sector supervision from the FSCA in February 2019, the SARB:PA has undertaken an SRA to develop its understanding of this sector. The SRA concluded that the sector is at medium risk of being abused for ML/TF. The SARB:PA is yet to develop and implement tools for institution-level risk rating of the life insurers.

SARB:FinSurv

362. The SARB:FinSurv has some understanding of ML risks in the ADLA sector but understanding of TF risks is limited to controls. The first ML/TF SRA of ADLAs was completed in

2019, which focused on compliance with legal obligations. Since April 2019, the SARB:FinSurv has implemented a risk matrix that it uses to risk-rate ADLAs' branches (rather than at the ADLA entity level, since all head offices are inspected every year) for both AML/CFT and compliance with exchange controls. This suggests that the SARB:FinSurv's approach is not focused on institutional-level (as opposed to branch-level) compliance or risk management. The matrix considers a very limited number of inherent ML risk factors related to customers (PEPs, walk-in customers), products and services (transfer versus exchange), and geographic locations (airports, border areas, etc.). No specific consideration is given to TF threats and associated vulnerabilities. The quality of controls is assessed primarily based on findings of previous inspections with no inputs from offsite analysis.

FSCA

363. The FSCA is developing its understanding of ML/TF risk in the securities sector (FSPs, CIS managers, AUs) at the sector level and is yet to understand ML/TF risks at the entity level. The FSCA has taken initial steps to assess the ML/TF risks at the sector level by conducting its first SRA, which considers ML risks from threats and vulnerability perspectives. While the SRA helped the FSCA collect useful feedback from the sectors, certain aspects of the methodology used (e.g., relying primarily on reporting statistics to assess threats), and some of the conclusions reached (e.g., CIS managers that have a significant offshore client base are rated as low risk) do not appear reasonable and suggest room for improvement. While the FSCA noted some threats facing the securities sector, including fraud and tax evasion, its understanding of vulnerabilities specific to the ways that the securities sector may be exploited for ML/TF is less pronounced. At the institutional level, the FSCA does not rate entities for ML/TF risks. Its assessment of FSPs' conduct-related risks considers AML/CFT controls only to a limited extent[61] and does not capture inherent ML/TF risks. The risk assessment of CIS managers is similar. The FSCA recognizes the challenges caused by the lack of specific tools to assess ML/TF risks. It is taking steps to set up an integrated AML/CFT unit that will conduct specific ML/TF risk assessment for all sectors. This is a welcome move forward. The JSE, which has delegated responsibility to oversee its AUs for AML/CFT, rates AUs for market and ML/TF risks with a 50 percent weight for each. The ML/TF risks are measured mainly by quality of controls learned in previous inspections with little consideration of inherent risks.

364. The FIC's understanding of ML/TF risk in the FI and DNFBP sectors it supervises is driven by use of cash (including CTR reporting) and entities' FIC registration status. At the sector level, the FIC's understanding of risks is primarily informed by interim SRAs completed in April 2019 on the public FIs, money lenders against securities, TSPs and MVDs.[62] MVDs and KRDs are considered high risk due to the cash-intensive nature of their businesses, and the fact that they are not subject to most of the preventive measure obligations. In comparison, TSPs are rated as medium risk, suggesting an insufficient appreciation of their risk exposure in the South Africa risk context (see section on ML/TF Risks and Context). For all sectors, the SRAs outlined some high-level ML

[61] These include AML/CFT controls with a negligible weight (three percent) and general controls that may have implications for AML/CFT controls, including board governance, compliance, risk management, etc.

[62] They are not covered by the FATF Standards but were brought into the South African regime, see section on National AML/CFT Policies and Coordination.

vulnerabilities, but TF consideration was limited to self-reported TFS compliance data. Consistent with its views that MVDs and KRDs are of the highest risks, the FIC developed a risk matrix to assess risks of MVDs and KRDs at an institutional level but only a portion of them are risk rated. The matrix includes some inherent risk factors such as geographic and product risk, but these are fairly simplistic. The assessment of controls is narrowly focused on the level of CTRs and FIC registration status, consistent with their supervisory focus (see below under 6.2.3). TSPs and other sectors supervised by the FIC are not risk rated nor is risk understood by the FIC at an institutional level.

365. The ML/TF risks within estate agents are understood to some extent while those in casinos and attorneys are understood by their supervisors to a much lesser or negligible extent. No systematic sector or institutional risk assessment has been undertaken by any of the DNFBP supervisors other than the FIC.[63] The EAAB views estate agents as high-risk and attractive for launderers. It is aware of ML vulnerabilities associated with some geographic regions and the use of complex corporate structures. The EAAB does not use a risk matrix but does consider which estate agents are most risky, mainly based on turnover, value of commissions, and complaints received. The PLAs considered risk only for legal compliance and did not demonstrate understanding of the inherent risks of the gambling sector. The LPC does not see itself in a position to have a view on ML/TF risks of the legal sectors. No understanding of TF risk was demonstrated by any DNFBP supervisors.

Risk-Based Supervision of Compliance with AML/CFT Requirements

366. While some supervisors are checking compliance with AML/CFT requirements, they are not prioritizing or tailoring their supervisory engagement on an ML/TF-risk basis. This is partially due to their lack of understanding of ML/TF risks at the institutional level (see page 119). Except for ADLAs, inspections are too infrequent (to varied degrees across sectors) to align with each sector's size and risk. Supervisors do not systematically supplement their onsite programs with offsite monitoring or engage in scoping to allow targeted onsite inspections. With the exception of the SARB:PA, they generally use a tick-box approach to test the presence of controls rather than soundness of the AML/CFT program.

367. The SARB:PA and the FSCA started coordinating on AML/CFT and sharing of high-level information in 2018 but are yet to share specific information with each other on FIs that belong to the same group or conduct joint inspections. Given the dominance of financial groups in the market (see section on ML/TF Risks and Context), this is a serious concern. In 2018, the SARB:PA and the FSCA started meeting regularly[64] to discuss AML/CFT matters ranging from licensing, legal issues pertaining the FIC Act, SRAs, inspections and sanctions, and to share high-level information in these

[63] The EAAB, the LPC and the PLAs are not involved in SRAs of their respective sectors conducted by the FIC and the EAAB and the PLAs do not agree with the conclusions reached.

[64] The authorities intend to formalize this as the *Financial Sector Regulators Forum on the FIC Act 38 of 2001*, and draft Terms of Reference have been prepared.

regards. They also started exploring ways to enable sharing entity-specific information and conducting joint inspections of entities that belong to the same group in the future.

Table 6.1. South Africa: Supervisory Resourcing and Activities by Sector—Time Periods Vary

Supervisor	No. of AIs or RIs	NRA Risk Rating	FTE Staff for AML/CFT inspections	AIs per FTE	Average Inspections Annually	% of AIs inspected Annually	Average Inspection Duration
PA	**115 Total**	**M-H**	19[2]	6	**11**	**10%**	**9–16 days**
	37 banks[3]	M-H			7	20%	16 days
	78 life insurance	M			4	5%	9 days
FSCA	**12,098 Total**	**L-M**	**74 general + 3 AML**	**163[4]**	**185[5]**	**2%**	**3 days**
	12,028 FSPs				158[5]	1%	
	70 CIS managers				28[5]	40%	
JSE	**100 AUs**	**M**	**10**	**10**	**24[5]**	**24%**	**3 days**
SARB:FinSurv	**255 ADLA branches**	**L-M**	**17**	**15**	**72**	**28%**	**1–2 days**
FIC	**4,385 Total**	**M-H**	**9**	**487**	**137**	**3%**	**1 day**
	223 KRDs	H			16	7%	
	189 TSPs[6]	M			7	4%	
	6 Public FIs	H			3	50%	
	76 money lenders against securities	M			4	5%	
	3,891 MVDs[7]	H			107	3%	
	60,246 AIs in support role	L-H		6,694	64	0.1%	
LPC	**19,119 attorneys**	**M**	**0**	**N/A**	**1**	**0%**	**N/A**
EAAB	**27,568 estate agents**	**M**	**4[8]**	**6,892**	**360**	**1%**	**1 day**

Table 6.1. South Africa: Supervisory Resourcing and Activities by Sector—Time Periods Vary (concluded)

PLAs (Total)	937 Total	**H**	**81**	**12**	390	42%	2 days
	39 casinos				**32**	**83%**	**2 days**
	898 other gambling[9]				358	40%	1 day

Source: South African Authorities
1: Totals may not sum due to rounding errors.
2: One of these positions was vacant as of the onsite.
3: 34 banks and 3 mutual banks in business as of the onsite. Does not include: one bank that exited July 2019, three banks in the process of exiting the market and one mutual bank that had been granted license but was yet to commence business
4: For general FTEs; the FSCA's AML/CFT-specific resources provide guidance to the FSCA and do not conduct inspections
5: These are AML/CFT-specific inspections conducted sequentially with prudential inspections, using the same staff
6: There are estimated to be 300 TSPs in South Africa, but only 189 are registered with the FIC and supervised for compliance.
7: The total number of MVDs in South Africa is unknown. 3,891 are registered with FIC.
8: Supported by nine private sector auditing firms, which conduct the bulk of inspections without FTE EAAB staff participation.
9: Betting, bingo, bookmakers, and limited payout machines supervised for FIC Act compliance. Three thousand five hundred and ninety branches registered with FIC.

368. A positive feature of the supervisory framework is the FIC's support for other supervisory bodies in their AML/CFT supervision including by joining inspections, outreach, and guidance to promote a consistent interpretation of legislation. In particular, since 2017, the FIC has supported other supervisors' understanding of the revised (2017) legal framework. During 2015 to 2019, the FIC participated in over 256 joint inspections conducted by other supervisors—the SARB:FinSurv, the PLAs, the EAAB, and, to a lesser extent, the FSCA and the SARB:PA. The FIC also conducts desk reviews (including providing registration and reporting data) to support the planning of inspections even when it is not participating in the onsite.

369. Compliance with TFS obligations are covered only by the SARB:PA and SARB:FinSurv. The SARB:PA reviews banks' TF-related TFS screening systems in regular inspections as well as during two thematic reviews in 2014 and 2017. However, these inspections are somewhat narrowly focused on screening systems without paying enough attention to related internal controls, such as policies and procedures, to ensure screening is done not only at the on-boarding stage and against all applicable UNSCR lists. SARB:FinSurv also covers TFS in its inspections and during a thematic review in 2017. Other supervisors do not supervise for TFS.

SARB:PA

370. The SARB:PA's supervision of the materially important banking sector checks compliance with AML/CFT requirements thoroughly but not yet in accordance with a proper

RBA. While the SARB:PA has a risk-based AML/CFT supervisory manual and uses a risk matrix to risk rate banks since 2016, the matrix does not capture risks in a comprehensive and dynamic manner (see para. 360. above). Furthermore, in practice, supervisory engagements are not fully prioritized on a risk basis (see Table 6.2). In particular, inspections of banks rated very high and high risk are too infrequent to be in line with their risk profile. For very high-risk banks (i.e., the "big four"), more than five years on average passed between inspections. Two banks rated high risk had two and four years in between inspections respectively. The SARB:PA intends to increase the frequency of inspections for higher risk banks. Its 2019 supervisory framework dictates that very high-risk banks should be inspected every 12–18 months while high-risk banks will be inspected every 24 months. Non-routine inspections are relatively few, and the majority were triggered by referrals by other supervisors or adverse media coverage. The current rate of inspections means that the SARB:PA takes around five years to complete an inspection cycle for all banks, and the SARB:PA completes roughly a third of the number of inspections per year required under its stated risk-cycle (see c.26.5). As such, the SARB:PA seems to overly rely on regular AML meetings with large banks to compensate the relatively infrequent inspections. It is noted that the reduced numbers of bank inspections during 2018–2019 can be attributed largely to the transition period following the FIC Act amendments in 2017 in which greater resources were devoted to engagements with banks on the new legal framework, and a focus on the life insurance sector newly under the SARB:PA's supervision.

Table 6.2. South Africa: SARB:PA AML/CFT Inspections 2012 to 2019 (year ending Dec 31)

Bank Size*	2012	2013	2014	2015	Bank Risk[1]	2016	2017	2018	2019[2]	Average Per Annum
Very Large	2	3	0	0	Very High	1	0	1	2	1.1
Large	0	1	0	1	High	1	3	1	0	0.9
Medium	3	1	2	3	Med	6	3	3	2	2.9
Small	3	1	2	1	Low	0	1	0	0	1.0
Very Small	0	2	3	3	Very Low	0	0	0	0	1.0
Total Domestic Bank Inspections	**8**	**8**	**7**	**8**		**8**	**7**	**5**	**4**	**6.9**
Inspection Rate (Domestic Banks)	**24%**	**24%**	**21%**	**23%**		**23%**	**20%**	**14%**	**11%**	**20%**
Inspections: cross-border bank subs	0	0	1	2		2	2	1	0	1
Life Insurers:	**2012**	**2013**	**2014**	**2015**		**2016**	**2017**	**2018**	**2019**	**Average Per Annum**
Onsite Inspections[3]	**0**	**6**	**4**	**3**		**3**	**5**	**1**	**8**	**3.8**
Inspection Rate (Life Insurers)	**0%**	**9%**	**6%**	**4%**		**4%**	**7%**	**1%**	**10%**	**5%**

1: Bank data 2012–2015 categorized by bank size, data 2016–2019 data categorized by bank risk rating.
2: Data as of November 2019
3: The PA began inspections of life insurers in February 2019, replacing the Financial Services Board.

371. The SARB:PA's onsite inspections appear to be thorough but not tailored to target individual banks' residual risk exposure due to a lack of in-depth understanding of inherent risk at the entity level. The SARB:PA uses a scoping exercise to determine the scope, depth, and focus of inspections. The main inputs into this exercise are information on AML/CFT controls, in particular recent feedback from the FIC on reporting, deficiencies previously identified, and follow up of remedial actions, and the latest findings on controls with respect to business lines deemed by the SARB:PA as inherently high risk across the sector. Any actions taken by other authorities (either in South Africa or abroad) on the bank or related media coverage that comes to the SARB:PA's awareness will be considered, too. In the absence of an in-depth understanding of inherent risks (see para. 360. above), the selection of business lines or aspects of controls for review is informed only to a limited extent by the individual bank's specific inherent exposure. As such, for all banks, inspections have been focused on areas where control deficiencies have been noted before. During inspections, the SARB:PA takes a thorough approach that involves review of procedures, sample testing and testing of IT systems. The AML/CFT supervision team within the SARB:PA has 19 dedicated staff (see Table 6.1), the largest within the SARB:PA's supervision department.

372. The SARB:PA expends some resources supervising foreign operations of South African banks including within the CMA but did not demonstrate that these activities are risk driven. Inspections conducted of foreign branches of South African banks are typically triggered by regulatory actions taken by host supervisors, adverse media coverage of the jurisdiction concerned, or deficiencies found in headquarters. While in preparation for inspections of a foreign branch, the SARB:PA consults the bank HQ to obtain information specific to that branch, these inspections are not conducted as part of consolidated group supervision. They are carried out jointly with the home regulator, sometimes with the host FIU in attendance. The inspections cover the main aspects of controls, including CBRs, and, in a few cases, special attention was given to PEPs due to public information on corruption in that country. However, no evidence suggests the inspection programs target risks based on a sound assessment of risks specific to that institution or jurisdiction in a systematic way.

373. The SARB:PA conducts offsite supervision primarily through AML/CFT meetings held with large banks. It engages with the largest or very high-risk banks via AML/CFT meetings on a semiannual or triannual basis. The focus of these meetings is updating the SARB:PA on remediation of deficiencies previously identified, advances in control framework including with respect to risk management, and feedback on STR and CTR reporting. As indicated above, the SARB:PA seems to rely on these meetings to get updates including on remedial actions, but it is unclear how the SARB:PA verifies and follows up on what it was told during the meetings. Furthermore, such engagement takes place with small and medium-sized banks much less frequently. The SARB:PA also monitors external developments concerning banks, including adverse media coverage or actions taken by other authorities domestically or abroad. No systematic supervisory returns are used to gather information to feed into the risk matrix or supervision scoping exercise (see para. 360.

374. The SARB:PA began onsite inspections of life insurers in early 2019, starting with large institutions. These early inspections are full scope to allow it to gain an overview of the institution's businesses and AML/CFT controls. Except for FIC reporting data, no offsite data gathering was undertaken in advance to inform these initial inspections.

375. The SARB:PA started covering the new requirements in the amended FIC Act in inspections of banks and life insurers in early 2019. The new legal requirements were introduced in 2017 but became enforceable only in April 2019. These include developing and implementing an RMCP, assessing ML/TF risks, and identifying beneficial owners.

SARB:FinSurv

376. The SARB:FinSurv demonstrated generally adequate supervisory coverage of the ADLA sector but is focused on rules-based compliance with the FIC Act and ECR. Each ADLA head office is inspected annually alongside branches selected for inspection (see Table 6.3 for inspection volumes). Before April 2019, selection of branches was not based on risks. Since then, the selection has been informed by the risk matrix described above, which considers limited ML/TF risks as well as factors related to exchange control compliance. In practice, it means branches that operate in high-risk areas such as border posts, casinos, and airports are inspected more frequently but other AML/CFT risk factors are not considered as part of inspection prioritization or scoping.

Table 6.3. South Africa: SARB:FinSurv ADLA AML/CFT Inspections- Five Years ending Dec 31

Year	2014	2015	2016	2017	2018	Average
Inspections	68	86	70	83	51	72

FSCA

377. The FSCA's supervision of the securities sector is not ML/TF risk sensitive and is primarily concerned with the presence rather than effectiveness of controls. Before the 2017 FIC Act amendments, aspects of AML/CFT were covered in conduct inspections. Since then, more dedicated AML/CFT inspections have occurred. There is substantial variation in the number of annual inspections, particularly in the FSP sector. In 2018, inspections ceased to focus on outreach for the FIC Act amendments. See Table 6.4 for inspection volumes.

378. The FSCA does not use ML/TF risk to prioritize onsite AML/CFT inspections. Though higher risk (for conduct with limited regard to ML/TF, see page 122), FSPs are supposed to submit a broad compliance report twice yearly providing reporting statistics, CDD, and governance updates but it was not demonstrated how or if these reports inform selection of FSPs and scoping of onsite inspections. In practice, FSPs without an in-house compliance officer were prioritized during 2017–2018 and, since 2019, emphasis has been given to FSPs who have never been inspected before. No evidence suggests different types of FSPs are treated differently in light of their levels of risk exposure. All onsite inspections are compliance- rather than risk-focused and appear to lack depth.

Except the semi-annual returns filed by some FSPs and non-AML/CFT-focused management meetings with large FSPs, there is no off-site monitoring.

379. The FSCA is under-resourced such that it cannot effectively supervise its population of entities for AML/CFT. As of the onsite, there were 43 inspectors (most with some AML/CFT training) for the 900 or so higher risk institutions for both AML/CFT and conduct supervision (see Table 6.1). They are supported by an AML Advisory Unit of three staff. As noted above, the FSCA is aiming to set up a dedicated team for AML/CFT supervision.

Table 6.4. South Africa: FSCA—Onsite Examinations that included Aspects of AML/CFT—Five Years ending Dec 31

Type of Financial Institution	2014	2015	2016	2017	2018	Average
FSPs	227	160	250	151	0[1]	158
CIS managers	52	21	20	24	20	27
Hedge Fund CIS manager	n/a	n/a	n/a	0	3	2
AUs	6	12	35	32	33	24
Total	285	193	305	207	56	209

1: The FSCA conducted 297 outreach visits to small FSPs to assist them to comply with the amended requirements of the FIC Act. These visits were not examinations to assess the effectiveness of the FSPs' AML/CFT programs.

380. The FIC's supervisory activity is driven by its deficient understandings of risks (see page 119) and addresses risks of TSPs only to a very limited extent. On average, the entities inspected by the FIC are mostly MVDs (78 percent) followed by KRDs (12 percent), while only 5 percent are TSPs (see Table 6.1). The selection of TSPs for inspection is informed primarily by non-registration with the FIC or randomly rather than ML/TF risk. Onsite inspections of TSPs typically take one day and are focused on general AML/CFT controls. Across all sectors, onsite inspections are heavily focused on registration and reporting, rather than the effective mitigation of risks. Constrained in resources (see Table 6.1), the FIC does little offsite monitoring to complement its onsite inspection program, and the majority of its 121 offsite exercises (which began in 2018) focus on MVDs rather than sectors covered under the FATF Standards. It is unclear what these exercises entail.

Table 6.5. South Africa: FIC—Number of Onsite Examinations—Four Years ending March 31

Type of Institution	2016	2017	2018	2019	Total	Average	Percent
TSPs	8	6	7	6	**27**	**7**	**5%**
Money lenders against securities	5	4	4	4	**17**	**4**	**3%**
FIs	2	2	3	4	**11**	**3**	**2%**
KRDs	16	19	18	12	**65**	**16**	**12%**
MVDs	114	101	101	112	**428**	**107**	**78%**
Total	**145**	**132**	**133**	**138**	**548**	**137**	**100%**

381. Given their risk exposure, the lack of effective AML/CFT supervision or monitoring of estate agents and attorneys is a great concern. Estate agents are not receiving AML/CFT supervision commensurate with their risks. The EAAB selects estate agents for inspections based on size, whether registered with the FIC and complaints received. Typically lasting one day, inspections are compliance based, testing for presence rather than effectiveness of controls. Due to the sector's size, there is inadequate coverage given its risks and materiality (see Table 6.6). The EAAB is also severely under-resourced with only four staff members working on AML/CFT (see Table 6.1). Prior to 2016, nine audit firms conducted the bulk of the EAAB inspections. In 2016, the EAAB lost a court challenge regarding inspection powers, and the audit firms' contracts were not extended. Essentially no AML/CFT supervision has been conducted for attorneys, aside from 4 inspections conducted in 2016 by the Free State Law Society[65] with the FIC on attorneys referenced in the Panama Papers. The LPC entered an MOU with the FIC on November 5, 2019, so that the latter will conduct AML/CFT inspections going forward.

Table 6.6. South Africa: EAAB Inspections that Include AML/CFT Elements—Five years ending March 31, 2019

Year	**2015**	**2016**	**2017**	**2018**	**2019**	**Total**	**Average**
Number of Inspections	1,025	474	63	108	130	1,800	360

382. Supervision of casinos is not conducted on the basis of ML/TF risk. The PLAs supervise casinos for compliance with the Gambling Act and factor FIC Act compliance into inspections; there is no dedicated AML/CFT supervision. Casinos are chosen for inspection based on size or randomly selected. Coverage varies greatly between PLAs, with some inspecting 100 percent of gambling operators annually, and others inspecting only a small proportion of the sector. Inspections focus on a compliance checklist covering STR, SAR, and CTR reporting and more recently, the existence rather than soundness of RMCPs. Effectiveness of controls is not assessed.

[65] A provincial pre-cursor to the LPC.

Table 6 .7. South Africa: Gambling—Number of AML/CFT Inspections that Covered AML/CFT—Five Years ending Dec 31

Type	2015	2016	2017	2018	2019	Total	Average	Percent
Casino	38	47	24	29	23	161	32	8%
Bingo	23	27	24	27	41	143	28	7%
Bookmaker	132	132	122	135	236	757	151	39%
Limited Payout Machines	110	195	124	149	314	892	178	46%
Total	**303**	**401**	**294**	**340**	**614**	**1,952**	390	100%

Remedial Actions and Effective, Proportionate, and Dissuasive Sanctions

383. Upon identification of breaches of AML/CFT obligations, a majority of supervisors have been relying on remedial actions and some of them have applied only very limited sanctions. All monetary penalties issued by financial supervisors are publicized. Only the FSCA has issued a small fine for non-compliance with the amended FIC Act, all other sanctions were imposed for non-compliance with requirements in the previous FIC Act. The DNFBP supervisors have issued only limited remedial actions and no monetary sanctions.

Table 6.8. South Africa: Supervisory Inspections and Enforcement Actions by Sector—Periods Vary

Supervisor	No. of AIs or RIs (See notes)	Average Inspections Annually (see **Error! Reference source not found.** notes)	Average Breaches Identified Annually	Average Remedial Actions Issued Annually	Average. Monetary Penalties Issued Annually	Average Monetary Penalty Value per Institution Across all Years[1]
SARB:PA	**115 Total**	**11**	**187**	**172**	**3**	**R 13,675,000 ($929,900)**
	37 banks	7	172	172	3	R13,675,000 ($929,900)
	78 life insurance	4[2]	15	109	0	0
FSCA	**12,098 Total**	**185**	**103**	**107**	**0.2**[3]	**R60,000 ($4,080)**
	12,028 FSPs	158	93	95	0	0
	70 CIS managers	28	10	12	0.2	R60,000 ($4,080)
JSE	**100 AUs**	**24**	**96**	**24**	**0.2**[4]	**R500,000 ($34,000)**

Table 6.8. South Africa: Supervisory Inspections and Enforcement Actions by Sector—Periods Vary (concluded)

SARB:FinSurv	**255 ADLA branches**	**72**	**27**	**182**	**1**	**R326,667($24,100)**
FIC	**4,385 Total**	**137**	**87**	**87**	**15**	**R220,054 ($15,000)**
	223 KRDs	16	13	13	2	R67,255 ($4,570)
	189 TSPs	7	11	11	0	0
	6 Public FIs	3	6	6	0	0
	76 money lenders against securities	4	6	6	0	0
	3,891 MVDs	107	51	51	13	R237,685 ($16,200)
LPC	**19,119 attorneys**	**1**	**2**	**2**	**0**	**0**
EAAB	**27,568 estate agents**	**360**	**305**	**305**	**0**	**0**
PLAs (Total)	937 Total	390	6	6	0	0
	39 casinos	**32**	**0**	**0**	**0**	**0**
	898 other gambling	358	6	6	0	0

1: Only includes sanctions payable, not suspended sanctions.
2: Until 2018, life insurers were supervised by the FSCA or its predecessor. Remedial action data from 2019 inspections only.
3: The FSCA issued one financial penalty in five years on a CIS manager and revoked two FSP licenses.
4: The FSCA issued one financial penalty over 2014–2018. It delegated supervision to the JSE but retains sanctioning powers.

384. The SARB:PA has used a range of tools against banks, including remedial actions and financial sanctions, but these may not always be proportionate and dissuasive. All financial sanctions are accompanied with either a reprimand, a caution, or directive to remediate deficiencies identified. Most inspections identify compliance deficiencies (an average of 17 per inspection or 187 annually), and progress on remediation plans are systematically monitored. However, there are concerns about the length of time some banks have taken to remedy issues identified. While all the "big four" have been penalized with fines that appeared to be generally proportionate to their sizes, all of these took place before 2016. The number of banks sanctioned has dropped during 2017–

2018, while the average financial penalty per institution varies substantially (see Table 6.9 below). Penalties on the lower end may not be sufficiently dissuasive. Moreover, the extent to which the size of penalties is proportionate to the nature and severity of the breaches identified is unclear. In a recent case believed to be a systematic failure, a court ruled that the penalties issued by the SARB:PA be reduced significantly, from R11,000,000 to R400,000, signaling potential legal challenges for the SARB:PA to effectively exercise its sanctioning powers.[66] No sanctions have been issued to life insurers as the SARB:PA only started supervising them in early 2019.

Table 6.9. South Africa: Monetary Penalties Imposed by the SARB:PA to Banks for AML/CFT Breaches

Year Ending March 31	2014	2015	2016	2017	2018	2019	Average
Administrative sanctions imposed (R million)	125.0	15.0	35.0	2.5	62.5	6.2	41.0
Administrative sanctions imposed ($ millions)	8.5	1.0	2.4	0.2	4.3	0.4	2.8
Number of Banks Sanctioned	4	2	6	1	2	3	3.0
Average Sanction per Bank (R million)	31.3	7.5	5.8	2.5	31.3	2.1	13.4
Average Sanction per bank ($ millions)	2.1	0.5	0.4	0.2	2.1	0.1	0.9

385. The SARB:FinSurv is applying remedial actions but the number of monetary penalty sanctions remains low considering the number of breaches identified. Since 2014, it has issued 909 AML/CFT related directives with an annual average of 182 (see Table 6.8 above) while only one financial sanction was issued per year since 2014 (none in 2014 or 2015). One ADLA lost its license for breaches of AML/CFT requirements.

386. While the FSCA has applied sanctions including monetary sanctions, these were very few and low in value and none against FSPs, hence not dissuasive or effective. During 2015–2019, monetary penalties for AML/CFT breaches were issued to one AU (R500,000 or $33,991 for not having the RMCP finalized) and one CIS manager (R60,000 or $3,907). Assessors are concerned about the FSCA's general policy not to apply monetary penalties against FSPs. Two FSPs have had their licenses withdrawn for multiple reasons including non-compliance with AML/CFT obligations. The FSCA has applied a few remedial actions only to AUs. Between May 2017 and February 2018, seven AUs received cautions not to repeat non-compliance and/or directives to take remedial action.

387. The FIC did not apply remedial actions or proportionate and dissuasive sanctions for non-compliance with AML/CFT obligations to entities other than MVDs and KRDs. Monetary sanctions issued to MVDs and KRDs pertain only to non-compliance with registration and reporting

[66] The FIC subsequently issued a directive to address the shortcomings highlighted in the judgment.

requirements (since they, as RIs, are not subject to other preventive measures obligations). Only one TSP was referred for enforcement actions.

388. No effective, dissuasive, or proportionate enforcement actions have been taken against estate agents, attorneys, or casinos. While the EAAB applied a limited number of remedial actions to estate agents, attorneys received none, due to lack of supervision. When deficiencies were noted by PLAs, corrective measures were recommended, but no penalty has been issued despite a relatively large number of inspections.

Impact of Supervisory Actions on Compliance

389. For all sectors, supervisory impacts in promoting entities' compliance with the new requirements introduced in the amended FIC Act with respect to, *inter alia*, RMCP, risk assessment, and beneficial owners cannot be demonstrated since these requirements became enforceable only in April 2019, and most supervisors only started supervision with respect to them very recently.

390. The SARB:PA's supervisory actions have had some impact on AML/CFT compliance by banks with the FIC Act provisions prior to the 2017 amendments, and exogenous factors have also helped promote compliance in the banking sector. There is evidence that supervisory actions led to increased compliance with CDD obligations between 2012 and 2014, and that TFS compliance increased between thematic reviews conducted in 2014 and 2017, though some remediation items are still outstanding. However, the extent to which the SARB:PA's supervisory activities lead to improvements in other aspects of controls, in particular the application of risk-based controls, was not demonstrated. Apart from supervisory impacts, external factors such as pressure from CBRs to ensure access to external markets such as the United States and United Kingdom seem to be a key incentive for large banks to improve AML/CFT controls.

391. Similarly, the SARB:FinSurv inspections and remedial directives have had some impact increasing ADLA compliance with basic AML/CFT obligations in the old FIC Act. This includes increasing number of entities appointing compliance officers, improved training, more CTR reporting, etc. The impacts of SARB:FinSurv's supervisory actions on ADLAs with respect to identifying and effectively mitigating the ML/TF risks envisaged under the amended FIC Act are yet to be seen.

392. The supervisory actions of the FSCA and the JSE have led to limited improvements of AML/CFT controls in the securities sector. The FSCA has seen a decline in compliance levels across FSPs, CIS managers, and AUs since 2017 as the entities were struggling to comply with the new obligations. As of the onsite, non-compliance remains high, including for basic rules-based obligations, though there are some recent indications that the RBA is being adopted by a majority of FSPs in their policies. Overall, the securities sector is early in the process of moving away from the rule-based approach to an RBA.

393. DNFBP supervisors were unable to demonstrate that supervision impacted compliance. While FIC registration and reporting increased in some sectors, evidence of increased compliance with most preventive measures obligations was not available.

Promoting Clear Understanding of AML/CFT Obligations and ML/TF Risks

394. The authorities, led by the FIC, provide guidance, and undertake outreach and engagement with regulated FIs and DNFBPs to promote understanding of AML/CFT obligations, including after the FIC Act amendment, but only limited information has been provided on ML/TF risks. As the private sector struggles in identifying and understanding ML/TF risks (see section on Preventative Measures), representatives of all sectors indicated to the team the need for them to get more guidance on identifying and understanding ML/TF risks.

- The FIC produces GNs, PCCs, and other publications to promote awareness and consistent interpretation of the legal framework within the private sector, which include general and sector-specific guidance,[67] the latter often developed in collaboration with supervisors. It also conducts virtual and physical outreach ("road shows") on a regular basis, to which all registered entities are invited, including those voluntarily registered, such as VASPs. However, most guidance provided is policy or compliance focused, with limited materials to help entities understand ML/TF risk.

- For all the financial supervisors, the recent SRA exercises were their first engagement with the private sector on ML/TF risks.

- The SARB:PA uses AML/CFT meetings (see above under 6.2.3) to share national and international policy and regulatory developments with banks. For life insurers that came under its purview recently, the SARB:PA held a one-day introductory workshop to sensitize them with respect to the amended FIC Act. The SARB:PA and FIC also engage with private sector bodies on a quarterly basis to discuss issues pertaining guidance. SAMLIT was established recently to facilitate public-private partnership in identifying ML/TF trends and typologies in the banking sector (see para. 142. above).

- Following the FIC Act amendment, the FSCA hosted over a dozen sector-specific conferences across South Africa to outline changes to requirements in light of the elimination of exemptions that previously applied to the securities sector. AUs supervised by the JSE attended FIC roadshows only.

- DNFBP supervisors have conducted limited outreach, focused only on compliance. The EAAB and four provincial law societies have produced material to raise awareness of the obligations in the amended FIC Act. The EAAB conducts annual industry meetings that sometimes cover

[67] FSPs—3 guidance products; Banks—3 guidance products; Estate Agents—2 guidance products; MVDs—1 guidance product; Gambling—3 guidance products; KRDs—1 guidance product; Securities—1 guidance product.

AML/CFT issues, provides materials to help estate agents develop an RMCP and a self-assessment of their AML/CFT controls.

C. Overall Conclusion on IO.3

395. Given its size and materiality, assessors have weighted banking sector supervision much higher than supervision occurring in other sectors. South Africa's system for market entry controls is deficient as fit and proper criteria often do not apply to beneficial owners nor do regulators conduct criminal checks or verify applicants' declarations. And even though there was an isolated case where a bank application was rejected due to beneficial owners' links to *"State capture,"* the authorities could not demonstrate that they implement adequate controls to prevent criminality from infiltrating FIs and DNFBPs. The SARB:PA's understanding of banking sector ML risks is relatively good, but this is not the case for other supervisors. Only banks and ADLAs are risk rated for ML/TF. It is a significant concern that all supervisors' understanding of inherent ML risks is insufficient and their understanding of TF risks is nascent. The SARB:PA's onsite inspections of banks appear thorough, while other supervisors focus on the presence of basic controls rather than the soundness of AML/CFT programs. Across all sectors, it is a serious concern that supervisory prioritization or scoping is not driven by ML/TF risks, in some cases due to insufficient or poor risk understanding. Limited or nonexistent supervision of high-risk DNFBPs (attorneys, estate agents, and TSPs) is a serious concern. Not all supervisors apply remedial actions or monetary penalties, but when they do so, the sanctions are often too low and infrequent to be effective or dissuasive. Only financial supervisors demonstrated some impact in improving FIs' compliance with basic obligations but not for the risk-based measures in the amended FIC Act. A fundamental issue in the context of South Africa is that unlicensed cross-border MVTS are not being systematically identified and addressed.

396. South Africa is rated as having a moderate level of effectiveness for IO.3.

LEGAL PERSONS AND ARRANGEMENTS

A. Key Findings and Recommended Actions

Key Findings

- A wide range of public information on the types of legal persons and arrangements which can be created in South Africa can be accessed through various means.
- There are serious challenges in obtaining BO information on companies and trusts. The authorities rely primarily on obtaining such information from AIs, but the measures in place are not sufficient to ensure that AIs are able to provide adequate, accurate, up-to-date, and verified BO information in a timely manner. Where such information is available, it takes LEAs too long to obtain it.

- The measures which South Africa has put in place to promote transparency and BO of legal persons and arrangements address only to a limited extent the main vulnerabilities that allow abuse of legal persons and trusts for ML/TF.
- Competent authorities have a general understanding that legal persons and trusts are exposed to ML/TF but have not properly identified or assessed the specific ML or TF vulnerabilities that lead to that exposure.
- Companies are abused for ML and used regularly to facilitate corruption in the awarding of government tenders and laundering of proceeds thereof.
- CSPs, when selling and transferring shell companies to new ownership, are not subjected to AML/CFT measures. Not all CSPs are AIs which limits the availability of BO information on companies.
- The Master's Office maintains a register of trusts which is a positive feature of the regime. It holds only basic information which is publicly available but may not always be accurate as the only information verified is trustees' identity.
- The authorities could not demonstrate that they applied effective, proportionate, and dissuasive sanctions for failure to comply with information requirements.

Recommended Actions

- South Africa should revise and substantially improve its mechanisms for ensuring that accurate, up-to-date, and verified BO information is timely available to competent authorities and consider having a competent authority responsible for obtaining and maintaining BO information.
- South Africa should thoroughly assess the ML/TF vulnerabilities of all types of legal persons, including vulnerabilities that facilitate corruption in government procurement.
- The CIPC should verify information of all foreign officers and foreign shareholders of South African companies.
- LEAs should be granted better powers to gain direct and timely access to ownership and control information for legal persons and trusts and LEA officers, who investigate financial crimes, be further trained about company and trust structures to enable them to more quickly identify and obtain BO information.
- The authorities should expand the Trust Property Control Act to require that sufficient information be held by trustees and provided to the Master's Office to help identify any other natural person in ultimate control of the trust.

- Empower the CIPC to impose administrative penalties directly; then the CIPC should apply sanctions for failure to comply with information requirements.

The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The Recommendations relevant for the assessment of effectiveness under this section are R.24-25, and elements of R.1, 10, 37, and 40.[68]

B. Immediate Outcome 5 (Legal Persons and Arrangements)

Public Availability of Information on the Creation and Types of Legal Persons and Arrangements

397. There is a good range of public information about the types of legal persons and arrangements which can be created in South Africa and how to create them that can be accessed in various ways from the CIPC and Master's Office. The means used by the CIPC include: its website (which is the most used); social media;[69] walk-in self-service terminals; booklets and pamphlets; and requests made at its offices. However, information on the CIPC website is only from 2016, and information before that has to be searched for manually. The CIPC has also partnered with three major banks that provide information on how to create and register a company and also a registration service. The CIPC also often carries out public awareness-raising on how to create legal persons. All means provide information on the types of legal persons that can be created. The Master's Office provides information on creation of trusts on its website, as well as in a booklet that it distributes to the public for information.

Identification, Assessment, and Understanding of ML/TF Risks and Vulnerabilities of Legal Entities

398. Most competent authorities have a general understanding that legal persons created in South Africa are often involved when ML occurs, but this is not grounded in proper efforts to identify and assess the ML or TF vulnerabilities that legal persons have. A comprehensive ML/TF vulnerability assessment of legal persons created in South Africa has not yet been undertaken. South Africa carried out an NRA on transparency of BO of companies in May 2018. The assessment recognized the problems of secrecy; operations, systems, and resourcing capability; coordination and access of BO information; inadequate legislation and oversight as posing vulnerabilities to transparency of BO information. However, the assessment did not focus on ML/TF vulnerabilities nor

[68] The availability of accurate and up-to-date basic and BO information is also assessed by the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes. In some cases, the findings may differ due to differences in the FATF and Global Forum's respective methodologies, objectives, and scope of the standards.

[69] Facebook, Instagram, and Twitter.

on the different types of legal persons created in South Africa. It mostly centered on theoretical findings.[70]

399. On the ground, the understanding of the concept of BO varies across competent authorities which led to different levels of understanding of the ML/TF vulnerabilities and the extent to which those vulnerabilities could be contributing to the ML/TF abuse of legal persons. Although, the SRAs conducted by the FIC, the SARB:PA, and the FSCA acknowledged that legal structures can be abused for ML, the assessments did not identify specific vulnerabilities linked to the different types of companies. The LEAs and the NPA appreciate that companies can be abused for ML/TF. However, that appreciation is not informed through identifying and assessing any types of ML/TF vulnerabilities in any of the specific types of companies that exist. These agencies also indicated that they were aware that complex structures of companies were often used in ML schemes but did not demonstrate much understanding of any specific vulnerabilities associated with types of complex company structures nor were specific examples of cases provided. This also applies to the misuse of legal persons for TF purposes.

400. The CIPC, while being aware of abuses of companies carrying out predicate crimes mainly through complaints that had been reported to it (e.g., 'company hijackings'[71] or directors manipulating shares), showed only a limited understanding of how companies are abused for ML. Although, the CIPC did indicate that, in general, the risk to companies of being abused for ML is probably quite high, in practice it did not consider or determine any ML/TF risks at the time of registering the legal persons and seemed unaware of any specific cases where companies had been abused for ML purposes.

401. The authorities acknowledged vulnerabilities associated with CSPs, many of which are not AIs, creating shelf companies which they later resell or transfer to new ownership without any AML/CFT measures being implemented but did not know the extent to which such activity was being abused for ML/TF. Similarly, they were aware that CSPs can also act as nominee directors and shareholders. However, they did not show knowledge about the extent to which these matters lead to ML/TF abuse; and the vulnerabilities have not been assessed.

402. Overall, due to the gaps existing in the different approaches to identifying the ML/TF vulnerabilities associated with legal persons, the understanding by the authorities of the kind of ML vulnerabilities affecting the different types of companies created in South Africa and the extent of ML/TF abuse is limited.

Mitigating Measures to Prevent the Misuse of Legal Persons and Arrangements

403. South Africa has implemented some measures to prevent the misuse of legal persons and arrangements for ML/TF purposes, but companies and trusts still feature prominently in ML

[70] *NRA for BO Transparency in South Africa, May 2018*. A report prepared for the South African Government's IDC on BO Transparency.

[71] When legitimate directors are illegally replaced by others without their knowledge with the intent to defraud SARS.

schemes. These measures include company and trust registration (see c.24.3); basic information being made available publicly (see c.24.3); and requiring AIs to obtain BO information during CDD (see section on Preventative Measures). In addition, for companies there are background and validation checks on directors and requirements to file documents (see c.24.3 and c.24.5). In the absence of risk assessment to identify, assess, and mitigate the specific ML/TF risks associated with each type of legal person and arrangement created in South Africa, the current measures might not be addressing the specific areas of ML/TF risk

404. All companies must be registered in South Africa. However, the process does not result in BO information being obtained either by the CIPC or the companies themselves resulting in a vulnerability that could be exploited for ML/TF.[72] Related to this, companies, being custodians of shareholder information, are not required to obtain information on foreign corporates that are shareholders. The facilitation of registration of companies through three major banks (see section on *Public Availability of Information above*) could be assisting in reducing some ML/TF risks associated with company creation depending on the extent to which the banks are able to obtain BO information as part of their own CDD occurring in parallel to the creation process. However, in general, banks indicated that they were still facing challenges in getting BO information (see paras. 325. and 326. above under IO.4). Trust registration is a positive requirement, but the level of information required during the creation and registration process does not result in full information on BO and control of trusts being collected.

405. While basic information is available publicly, it may not always be accurate and reliable in the case of trusts. Of the basic information publicly available, only the trustee's identity is verified (see para. 410.

406. The requirements since 2017 for AIs to obtain BO information has improved on the amount of basic and BO information available to the authorities. However, not all FIs, DNFBPs, and VASPs are subject to the requirements and compliance with the requirements varies or cannot be demonstrated yet (see section on Preventative Measures). Access to the information is not always timely (see below), and the information is not always accurate or comprehensive.

407. The CIPC cross checks the names of proposed company directors with its register of delinquent directors and verifies their particulars with the DHA database if they are South African. However, no verification occurs for foreign directors; the CIPC only obtains a copy of their passports.

408. Filing of documents by companies includes annual returns and changes in their directors and registered address. The information kept may not always be up to date and enforcement of the requirements needs to be improved (see para. 450).

[72] The CIPC indicated that the Companies Act was in the process of being amended to require companies to file beneficial interest holder information with it, but it is not known if the amended Act will align with the FATF definition on BO.

409. Overall, the measures implemented to prevent the misuse of legal persons and arrangements for ML/TF purposes still leave companies and trusts open to ML/TF abuse due to several factors. The measures are not comprehensive, due in part to the lack of a proper assessment of the ML/TF vulnerabilities (see 7.2.2). Those that are in place are affected by the limitations described earlier. In addition, LEAs could not demonstrate through the cases finalized their ability to identify BO in complex company or trust structures, suggesting better training is required. No cases were provided to demonstrate their ability to address ML/TF where foreign corporations were involved. ML cases in South Africa also suggest that companies are abused for ML purposes. In addition, public information from inquiries into *"State capture"* also suggest that companies are abused regularly to facilitate corruption in the awarding of government tenders and soliciting of favors and the subsequent laundering of the proceeds. The extent to which companies and trusts are abused for TF, and hence, how well measures are implemented to prevent such abuse is unknown.

Timely Access to Adequate, Accurate, and Current Basic and Beneficial Ownership Information on Legal Persons and Arrangements

410. Basic information for legal persons is not always accurate as only information about South African directors is verified. For trusts, the Master's Office is only an office of record and does not verify the information maintained in the register other than the identity of a trustee. The authorities primarily rely on AIs (in practice, large banks) to obtain both basic and BO information, as well as accessing such information through the other sources such as credit databases. Discussions with the FIC and some LEAs indicated that often ownership information obtained only relates to the legal not beneficial ownership. The timeline for accessing the BO information varies (see details below).

Access to basic information on companies held by the CIPC

411. LEAs and prosecutors (for free) can also access information directly from the CIPC through requests, rather than the CIPC website. In such cases, the CIPC provides the information within two days to two weeks, depending on the request's complexity. The SAPS, the FIC, the SARS, and the NPA also have direct access to the CIPC's database, although they do not use it often, preferring to get information directly from the CIPC for use as evidence. Information on the website is only available from 2016, and information on companies registered before that has to be searched for manually. This poses challenges in getting the required information on time and the extent to which the information is kept accurate and reliable.

412. Competent authorities can also access basic and shareholder information from the companies themselves to the extent that the information is accurate and available. Where LEAs find that not to be the case, they notify the CIPC. Legal persons are meant to keep information up to date by filing annual returns and notices of certain changes in the company with the CIPC. However, these requirements are only enforced to a certain extent with limitations on the period provided by the law for the CIPC to strike off a company after two years for non-filing of returns also negatively affecting the process as it is rather long. As mentioned earlier, the only information held

by the CIPC that is verified relates to the identity of local directors. Similarly, shareholding information held by the companies is not verified. Thus, basic information obtained via the CIPC or companies might not always be reliable.

Access to basic and BO information on legal persons by LEAs using subpoenas

413. The SAPS obtains BO information on legal persons by applying for a subpoena (CPA, s. 205) that it serves directly or through the FIC on the reporting entity of interest (most often a bank). Subpoenas are often issued within half a day and state the timeline for providing the BO information. Both the LEAs and AIs indicated that it took on average 7–10 days for the information to be provided. However, in cases with complex company structures it can take SAPS weeks (on average 30 days) to access the first level of legal (shareholder) ownership information using various sources, and often longer to get to the actual BO information as the sources might not be holding such information and further information requests are then required. These time periods might be too long for gathering evidence to advance some types of criminal investigation, particularly those involving tracing assets that might be dissipated. The situation is further compounded by a lack of knowledge amongst many LEA officers about complex corporate structures and how they can be abused to facilitate crime. These factors mean that access to adequate, accurate, and current BO information by LEAs often does not occur in a timely manner. The challenges seem to be consistent with the reports from the AIs which indicated that in most cases it was difficult for them to identify BO and obtain all required information through the CDD processes they conducted and to verify and confirm the information's accuracy (also see IO 4).

Accessing BO information from AIs through FIC

414. The FIC also assists LEAs during their investigations by requesting BO information from AIs (see c.24.6) and then providing LEAs the name of the FI, DNFBP, or VASP that the legal person or trust is a client of. LEAs can then apply for a subpoena to obtain any BO information held by the specific institution (c.24.6). SAPS said that this process was extremely useful and made it a lot easier to obtain evidence about ownership. It takes FIC about 7–10 days to receive the information from the requested AIs.

Access to basic information on legal arrangements held by the Master's Office

415. The Master's Office provides basic information on each trust such as the trust name, trust file number, names of trustees, domicile address, and the office where the trust was registered on its website. The Master's Office can, in addition, provide the trustee's South African identity number to LEAs upon being requested to do so through a subpoena. It takes about 10–15 days for the Master's Office to provide requested information. The basic information other than the trustee's identity is, however, not verified and is not always up to date. The Master's Office also does not obtain information on any other natural person who might be exercising ultimate effective control of a trust. The Master's Office does not gather or obtain information on the trust's purpose. The Master's Office signed a MOU with the SARS in June 2018 to facilitate information exchange; it has only been used once by the SARS to request a trust deed which was provided in about a month.

There is no other information available about how frequently other authorities seek information from the Master's Office nor about the timeliness of responses as such records are not kept.

Access to BO information on legal arrangements using subpoenas

416. LEAs have also requested BO information using subpoenas from professional trustees which are AIs and banks. They indicated that professional trustees had provided the information in less than 30 days when it was available but took more time where further information was requested on linked persons or accounts. However, this information is limited to the identity of their clients or persons either giving the instruction to create the trust, creating the trust, or being appointed as trustee. This does not include information on other natural persons who might be exercising ultimate effective control over the trust, agents, or service providers to the trust as this is not required by law (see c.25.1). BO information was not always available from banks, because banks have difficulties obtaining such information when establishing a business relationship with a trustee (see IO 4).

Effectiveness, Proportionality, and Dissuasiveness of Sanctions

417. The authorities could not provide any examples where requests for basic and BO information from AIs and other sources had not been complied with and had resulted in sanctions being applied. The obligation for AIs to identify BO and verify their identity information became enforceable recently in April 2019, and supervisors are yet to impose any sanctions for breaches of this obligation.

418. Overall, it cannot be said that effective, proportionate, and dissuasive sanctions have been applied against persons who failed to comply with information requirements. The CIPC shared information about investigations into noncompliance with the Companies Act, but these do not identify cases which related to noncompliance with information requirements. Where these investigations had resulted in the CIPC issuing compliance notices and the companies addressing the violations, the CIPC had closed the cases without imposing any fines or other penalties. Where a company had failed to file returns in two successive years, the CIPC moved to strike it from the register as an administrative measure. Failure to file annual returns was highlighted by the CIPC as a main compliance violation. Therefore, it does not look like deregistration alone is dissuasive enough and the period of two years prescribed by the law is rather too long to strike off delinquent companies.[73] The CIPC cannot impose administrative fines for Companies Act violations but must refer such cases to court which seems a cumbersome process.

C. Overall Conclusion on IO.5

419. There is a good range of public information about the types of legal persons and arrangements which can be created in South Africa and how to create them. Most competent

[73] Likewise, no cases taken by the CIPC to disqualify directors involved failure to comply with information requirements

authorities demonstrated a general understanding that legal persons created in South Africa are often abused for ML, but they have not properly identified and assessed the ML or TF vulnerabilities that the different types of legal persons have. South Africa has implemented some measures to prevent the misuse of legal persons and arrangements for ML/TF purposes, but the extent to which the measures are complied with varies, companies and trusts still feature prominently in ML schemes, and the extent of their abuse for TF is unknown. Competent authorities can obtain adequate, accurate, and current, basic information on legal persons and arrangements to some extent. However, and of great concern, is that they can access BO information only to a very limited extent or not at all. Access to such information is not timely. There is no evidence that any sanctions for failure to comply with information requirements have been imposed.

420. South Africa is rated as having a low level of effectiveness for IO.5.

INTERNATIONAL COOPERATION

A. Key Findings and Recommended Actions

Key Findings

- South Africa provides constructive MLA and extradition in response to international requests. The assistance provided is useful and has resulted in resolution of some criminal cases in other jurisdictions but is sometimes slow, and a significant proportion of requests are returned unexecuted for failure to comply with South African requirements. There is an absence of an effective case management system and overall responsibility for timely execution of the requests.

- Requests for international legal assistance have only been made in a very limited number of instances, which is inconsistent with South Africa's risk profile. The authorities have not adequately demonstrated that seeking international cooperation in the investigation of ML, associated predicate offenses, and TF is a priority and need major improvements to how they follow up on outgoing requests.

- The main competent authorities exchange information informally with foreign counterparts reasonably consistent with South Africa's risk profile. Most information is exchanged by the FIC.

- Some basic information on companies and trusts can be shared in a timely way as it is publicly available, but there are challenges with the timeliness for information about most companies registered before 2016 and sharing BO information.

Recommended Actions

- Actively seek formal and timely MLA for all ML, associated predicate offenses, and TF in a much greater proportion of the cases that have transnational aspects and actively follow up on such requests in a timely manner.

- Proactively pursue requests made to foreign jurisdictions in *"State capture"* cases through all available channels, including making direct contact with foreign agencies responsible for handling the requests and travelling to those places for case conferencing as appropriate.
- When requests fail to comply with South African requirements, the authorities should provide proactive assistance and guidance to requesting countries about how those requests could be resubmitted or supplemented successfully.
- Develop an overall case management system within the DoJ&CD (the Central Authority) to streamline and monitor the timely processing, prioritization, and execution of all incoming MLA and extradition requests by responsible agencies.
- Improve the overall capacity and turnaround time to share BO information with foreign counterparts, primarily by implementing the recommended actions for IO.5.
- Maintain adequate and accurate statistics on all international cooperation requests, especially turn-around time, to enhance monitoring of timely execution and internal review processes.

The relevant Immediate Outcome considered and assessed in this chapter is IO.2. The Recommendations relevant for the assessment of effectiveness under this section are R.36–40 and elements of R.9, 15, 24, 25, and 32.

B. Immediate Outcome 2 (International Cooperation)

421. South Africa is the most developed country in the southern Africa region and attracts a large volume of immigrants from sub-Saharan Africa. It is also a regional financial center. This increases the risk of potential involvement of persons in cross-border financial crimes, and hence the need for international cooperation in the region is high. The DoJ&CD is the central authority for MLA and extradition requests.

Providing Constructive and Timely MLA and Extradition

422. South Africa can render constructive MLA and extradition on the basis of its broad and permissive legal framework which allows for formal and informal international cooperation. It can also render constructive MLA and extradition on the basis of treaties and conventions. The requests for MLA that come through DIRCO are forwarded to the DoJ&CD where they are first analyzed and, if authorized for execution, distributed to the relevant agencies. The requests are referred to the NPA, SAPS (Interpol) and the Judiciary. A police officer will work with an NPA official to execute the request, and a magistrate may issue subpoenas to take evidence and require production of documents. An inquiry is held before the magistrate, and the evidence obtained sent to the requesting jurisdiction. While there are clear procedures in place to execute incoming MLA requests, in the assessors' view, the internal administrative procedures are overly formal, and each agency tends to work within a narrow focus, contributing to a lack of overall responsibility and proactive case management by any one agency including the Central Authority. It was evident

during the onsite that each agency worked on the request at the exclusion of others, and the authorities do not have an effective overall case management system to facilitate the handling incoming MLA and extradition requests in a timely manner (see c.37.2).

423. South Africa receives and handles on average eight incoming ML/TF related MLA requests each year with about 30 percent being returned for not meeting South Africa's legal requirements. Over the five-year period, 2015 to 2019, South Africa received 552 MLA requests. Of these incoming requests, 40 related to ML and one related to TF. Of these 41 requests, 29 were either executed by the authorities or were still in the process of being executed. Four of eight case studies provided by the authorities in which the MLA requests were accepted were from the United States, and the other four were from Denmark, the Netherlands, Ethiopia, and the Isle of Man. The information provided by the authorities for the 41 incoming requests shows that the shortest time taken to execute a request for MLA was two months and the longest time was two years and 1 month in a particularly complex case. On average, requests took at least one year to process. Although the authorities do not maintain records on feedback, they indicated that most of those assisted appreciated and found the assistance useful. This was confirmed from the cases provided by the authorities in which MLA was helpful and led to the arrest of suspects in some cases and recovery of proceeds in others. A total of 12 (or 30 percent) ML/TF-related requests were not executed due to noncompliance with South African requirements, which is concerning. The authorities did not sufficiently evidence what proactive assistance or detailed guidance they provided to requesting jurisdictions to enable them to meet their requirements, other than returning the request with a statement as to why it could not be executed.

424. South Africa received on average one ML/TF-related extradition request each year during the period under review. Two hundred and two extradition requests were received and processed over the five-year period 2015 to 2019. Only four of these requests related to ML and one related to TF. Three requests were returned for noncompliance with the legal basis for extradition requests, evidencing a return rate of 60 percent for ML/TF-related extradition requests. The request relating to TF was executed (the subject voluntarily agreed to return to the requesting country following arrest) and one request relating to ML has been under processing for 13 years. According to the authorities, some delays are probably due to the fugitives being litigious and contesting the extradition process, but they did not indicate that this had been the specific cause of all the delays.

425. The assistance provided is, to a large extent, useful and, in some instances, resulted in resolution of criminal cases in other jurisdictions and the recovery of proceeds of crime, but it could be executed in a more timely manner. The provision of MLA is at times slow, and this is consistent with feedback received on international cooperation from some jurisdictions. Two responding jurisdictions indicated a total silence in response to their requests. Only one jurisdiction responded that MLA was provided in a timely fashion.

426. The authorities indicated that the LEAs and the NPA have had resource challenges which may explain some delays in responding to requests. During the onsite, the government announced budget increases for the NPA and the LEAs which may help with speeding up the provision of MLA and extradition requested.

427. South Africa's NPA:AFU has offered effective and timely assistance in the recovery, restraint, and forfeiture of proceeds of crime in most cases. The case in Box 12 is a good example of the provision of effective AML/CFT-related MLA.

Box 12.1. Fraud Case Example

The NPA:AFU received a request from Denmark via the CARIN/ARINSA network. Investigations revealed that Nielsen fraudulently transferred a sum of R36 million ($2.4 million) over a period of 10 years to an FNB account, held in her and her son's name in South Africa.

There was a formal MLA from Danish authorities requesting the SAPS to arrest Nielsen and her son.

The NPA:AFU conducted a cash flow investigation and identified various assets purchased with the proceeds of the fraud in Denmark. On a Red Notice, Interpol arrested Nielsen and her son. They both agreed to voluntary extradition to Denmark, confirmed that their assets in South Africa were purchased with crime proceeds and that they would not oppose an application to freeze and forfeit the funds. To date the NPA:AFU has obtained five preservation orders.

428. Inwards MLA requests related to ML/TF are mainly coming from North America and Europe and, to a lesser extent, from neighboring African countries (e.g. Botswana and Eswatini). South Africa's risk profile suggests that it should be receiving and thus providing more cooperation within the African region. Incoming requests dominate, reinforcing that the authorities are often reactive rather than proactive for transnational ML/TF matters. Overall, South Africa provides MLA and extradition to a much greater extent than it requests.

Seeking Timely Legal Assistance to Pursue Domestic ML, Associated Predicates and TF Cases with Transnational Elements

429. South Africa has sought MLA from different jurisdictions to pursue domestic ML, associated predicate offenses and TF but needs to use it more often especially in relation to *"State capture"* cases. Over 2015–2019, the authorities made 50 outgoing MLA requests with 32 being made in 2018. Prior to 2018, outgoing requests averaged less than five each year. Of the 50 requests, 3 related to ML and 3 to terrorism. No MLA requests sought to freeze assets related to *"State capture"* cases. During the same period, the authorities made no outgoing ML or TF-related extradition requests. More cooperation should be occurring within Africa considering South Africa's role as a regional financial hub with porous borders and large migrant population which includes people from high risk jurisdictions on the continent. There also do not seem to be enough outgoing requests to the Middle East and South Asia reflective of those places being suspected destinations of outflows of proceeds related to *"State capture"* (see below).

430. The low volume of outgoing requests for MLA is not consistent with South Africa's risk profile. The delay to expeditiously investigate and speedily pursue recovery of the proceeds of crime relating to *"State capture"* cases which have transnational elements is a cause for concern. As it is, this means that the authorities have missed opportunities to obtain evidence and assistance from other jurisdictions at the earliest opportunity, and some proceeds may have dissipated. In October 2019, after the authorities started seeking assistance with investigating the *"State capture"* cases, the

United States added the three key suspects to the OFAC sanctions list.[74] The authorities indicated that they had sent out 16 requests for MLA to 10 countries relating to *"State capture"* cases in 2018, but were still waiting for the responses as of the onsite, 14 months after the requests were made. They also indicated that informal enquiries are often made through diplomatic channels prior to sending formal MLA requests. These informal enquiries are not tracked but the authorities said that often they do not get feedback on outcomes.

431. Box 13 provides a sanitized case that illustrates a degree of effectiveness in national cooperation in the making of an outgoing MLA request as well as concerns about the time it takes to pursue such matters.

Box 13.1. State v XYZ and Others

Investigations revealed that wide-scale corruption had siphoned large amounts from a number of SOEs, some of which was transferred through banks and other entities including to some institutions located in foreign jurisdictions. To finalize the investigations, institute criminal prosecutions, and pursue the money abroad through asset recovery processes, South Africa made MLA requests to, inter alia, Country A. The request to Country A was submitted by the DPP to the DoJ&CD on March 7, 2018 and delivered to the relevant authorities in Country A on April 24, 2018.

In September 2018, Country A acknowledged receipt of the MLA request. South Africa has not received any further feedback. From November 2018 onwards, numerous requests for feedback were made through diplomatic channels to no avail. More efforts to get feedback including in the margins of international events and other forms of informal contact were made but no assistance has been forthcoming. The undue delay or non-execution of the request has far-reaching effects on the case's investigation and prosecution as the requested evidence is material to the matter's successful conclusion.

432. The authorities expressed frustration with the slow pace at which responses to most of their requests for MLA are being attended especially in the *"State capture"* requests. The authorities received an initial response to 11 of 16 outgoing *"State capture"* MLA requests made to 10 different jurisdictions during the relevant period. In one case, where there was concerted follow-up, the authorities were assisted to their satisfaction. In instances where there has been no progress, the authorities do not appear to have made regular concerted effort to pursue the MLA requests after the initial response or lack thereof. The authorities are urged to proactively pursue all the outstanding requests and keep a record of action taken.

433. The Bobroff matter (see Box 14.1) is an example showing that the authorities can seek and also provide good quality international cooperation in some cases. This case involved receiving and sending out requests to the same foreign jurisdiction. The predicate offenses were fraud, theft, and tax evasion. The MLA process including asset forfeiture took almost two years, but in the end more than R100 million ($6.8 million) was forfeited. The criminal trial for the predicate offenses and ML is still pending in South Africa.

[74] www.federalregister.gov/documents/2019/10/31/2019-23785/notice-of-ofac-sanctions-actions

Box 14.1. Bobroff Matter

The accused were directors of a law firm that specialized in personal injury matters. They had entered into multiple fee agreements with their clients to disguise various frauds, thefts, and tax evasion. The accused invested the proceeds of these crimes along with a substantial amount of the firm's monies in an investment account which was opened under a disguised name with the aim to launder the proceeds. In 2017, both incoming and outgoing MLA requests were received and made, making this a complex matter. The MLA request received was to gather evidence. The NPA:AFU also obtained a preservation order over foreign bank accounts and made an MLA request to freeze those accounts abroad. The court extended the preservation order numerous times, each time for 180 days. On August 21, 2019 a final Forfeiture Order was obtained to the value of R103,648,756.66 ($7 million). The matter is under appeal.

Seeking other Forms of International Cooperation for AML/CFT Purposes

434. The competent authorities in South Africa do seek and exchange information informally with their foreign counterparts on a regular basis. The LEAs and the intelligence organizations are at the forefront of such information exchange. The NPA uses its membership of the Africa Prosecutors Association (APA) for the effective exchange of information with other prosecutors. The FIC is the most prolific seeker of international cooperation. The FIC made 306 requests for information from other jurisdictions during the period under review (see Table 8.1). Forty requests related to ML, 28 to TF, and 238 to predicate offenses. The FIC also made inquiries on behalf of the SAPS and the NPA:AFU. In the light of its risk profile, South Africa should be seeking other forms of cooperation at a higher level to be able to effectively deal with ML/TF.

Table 8.1. South Africa: Number of FIC Requests Sent to Other FIUs—Five Years ending March 31, 2018

Crime (Year Ending March 31)	2014	2015	2016	2017	2018	Total	Percent
Fraud	26	13	3	26	11	79	26%
Tax Crimes	22	12	16	13	12	75	25%
ML	2	3	11	7	17	40	13%
Corruption	9	2	-	6	14	31	10%
TF	3	0	13	6	6	28	9%
Narcotics	4	1	-	4	-	9	3%
Rhino Horn Smuggling	2	2	1	-	-	5	2%
Illicit Flow of Funds	-	-	-	5	-	5	2%
All Other	4	6	7	9	8	34	11%
Total	72	39	51	76	68	306	
Requests Granted	N/A	N/A	4	4	8	16	
Average Response Time (Months)	3-9	3-9	3-9	3-9	3-9	3-9	

435. The LEAs also share information and conduct joint investigations with their foreign counterparts. In one example, this type of cooperation led to the forfeiture of R63 million ($4.3 million) from a Ponzi scheme over a six-year period from 2009 till 2015 using the POCA, ch.6. This case involved over 10 countries and R13 billion ($884 million) in proceeds. The Ponzi scheme, which operated for around six years prior to the last South Africa ME, offered investors returns of over 200 percent annually related to trading in ingredients for pharmaceuticals. Some suspects in the case had to be extradited from Australia, Switzerland, and the United Kingdom.

436. The SARS seeks information from foreign counterparts on tax matters. The case of Ben Nevis (Holdings) Limited reflects the benefit South Africa has derived from international cooperation for tax purposes. They managed to pursue and collect revenue that they would otherwise have lost. The case involved both administrative and criminal matters. During the period under review, requests were made to foreign jurisdictions for the exchange of information on import and export data, verification of information, confirmation of declarations, verification of stamp impression, exchange of information on seizures and detentions and controlled deliveries, some of which are predicate offenses to ML. Tax offenses were identified as among the high risk offenses in South Africa, yet the authorities do not seek tax information from their foreign counterparts at a higher level. During the period under review, the SARS sent 84 requests for assistance, and 70 percent were granted while only 2 percent were turned down. The average turnaround time was estimated by the authorities to be 34 days per request.

437. The FSCA cooperates in a timely manner and exchanges information with its counterparts when requested or if needed. As a member of CISNA, it benefits from the exchange

of information and assists other jurisdictions with information relating to insurance issues, securities, and on non-bank financial businesses issues.

438. Overall, the informal requests for information made are broadly consistent with South Africa's risk profile. However, the assessment team would have expected more enquiries related to *"State capture"* cases to have been made, especially in earlier years.

Providing Other Forms of International Cooperation for AML/CFT Purposes

439. The authorities largely provide other forms of international cooperation and exchange financial intelligence with their foreign counterparts. However, in most instances, it is not spontaneous. The FIC and the SSA are the ones that regularly share information spontaneously.

440. The SAPS cooperates with other LEAs regionally and internationally in the fight against transnational crimes including terrorism, TF, and ML. Cooperation in SADC countries is via the Southern African Region Police Chiefs Cooperation Organization (SARPCCO). The SAPS shares information on threats related to ML and TF and related intelligence. This exchange of intelligence assisted in the arrest of two intending FTFs who were en route to a conflict zone. A kidnapping with links to TF was successfully investigated as a result of both international cooperation and in response to MLA.

441. The NPA:AFU handles requests directly from other AFUs and formal MLA requests. In the relevant period it dealt with 41 requests from foreign regional and international AFUs. As a member of ARINSA, South Africa cooperates effectively with other members as the representatives of the member countries can be contacted directly by telephone and can provide helpful information pending formal MLA processes.

442. The FIC dealt with 1,310 information requests related to ML, related predicates, and TF over the period 2014–2019 (see Table 8.2).

Table 8.2. South Africa: FIC Requests Received from Other FIUs Five Years ending March 31, 2018

(Year Ending March 31) Crime	2014	2015	2016	2017	2018	Total	Percentage
Tax Crimes	12	73	110	165	43	403	31%
Fraud	20	68	103	110	45	346	26%
ML	53	98	99	57	25	332	25%
TF	6	74	10	3	6	99	8%
Corruption	5	9	13	10	12	49	4%
Narcotics Related	6	3	9	7	4	29	2%
All Other	2	3	9	13	25	52	4%
TOTAL	104	328	353	365	160	1,310	100%
Requests Granted	104	328	350	142	162	1,086	83%
Requests Refused	0	0	0	0	0	0	0%
Requests Pending	0	0	3	223	-2	224	17%
Average Response Time (Days)	1-10	1-10	1-10	1-15	1-15	N/A	

443. In one example, the FIC cooperated with the Danish FIU in following fraud proceeds which had been sent to South Africa. The fraudster had fled to South Africa. To assist the Danish FIU, the FIC had to cooperate domestically with the NPA, NPA:AFU, SAPS, Interpol, and a private bank. These efforts resulted in the arrest of two Danish suspects in South Africa and the issuing of restraining orders against their properties.

444. The FIC in the relevant period received 99 requests for TF related information from foreign jurisdictions. The time taken to process and respond to the requests ranges between 1 to 12 days (see Table 8.2). However, according to FIC, the general turnaround time taken to respond to requests is less than 10 days. The authorities indicated that their counterparts appreciated the information that they shared.

445. The FIC also gave 101 spontaneous disclosures to other FIUs—see Table 8.3. Of those, 26 related to ML, four to TF, and 71 related to other predicate offenses. This is commendable and in line with the country's risk profile. Fifty-one percent of the disclosures related to crimes that are considered as posing the highest risk in South Africa.

Table 8.3. South Africa: FIC Spontaneous Disclosures to Other FIUs—5 Years ending March 31, 2018

Crime (Year Ending March 31)	2014	2015	2016	2017	2018	TOTAL	Percentage
ML	11	11	2	-	2	26	26%
Fraud	7	3	1	-	12	23	23%
Tax Crimes	12	3	3	2	2	22	22%
Illicit Flow of Funds	-	-	-	-	12	12	12%
Narcotics	5	2	-	-	2	9	9%
TF	0	4	0	-	-	4	4%
Corruption	-	4	-	-	-	4	4%
Theft	-	-	1	-	-	1	1%
TOTAL	35	27	7	2	30	101	100%

446. The SARS received 98 requests during the period under review, dealing with verification of certificates of origin, confirmation of documents for exports done, provision of declarations to authenticate the exports done, assistance in the investigation of illegal motor vehicles schemes, confirmation of authenticity of artworks, provision of profiles of traffickers dealing in ML and gold, special control delivery, spontaneous tracking of containers as well as assistance with valuation matters.

447. The SARB:PA exchanges AML/CFT relevant information and cooperates with other central banks and supervisory authorities to a large extent. This relates to both prudential and AML/CFT issues. During the period under consideration the SARB:PA handled 184 outgoing correspondence relating to fit and proper inquiries, AML/CFT inspections, licensing, and cross-border banking issues.

448. The FSCA's cooperates with foreign counterparts in a timely manner mostly in response to requests made. The FSCA between 2016 and 2018 received and processed 137 requests from other jurisdictions. The average turnaround time was 25 days. See Box 15.1 for an example of FSCA cooperation.

Box 15.1. Financial Supervisor Cooperation

On October 28, 2016, the FSCA received a letter from the central bank governor of a neighboring country, requesting assistance regarding "possible illegal investments in Mamepe Capital—South Africa". On March 27, 2017, the FSCA was advised by its counterpart in the other country of suspicious investments relating to the same matter and received a request for information. A bank in the neighboring country allegedly invested R208 million ($14.1 million) through Mamepe Capital (Pty) Ltd ("Mamepe"), a registered FSP in South Africa. The FSCA investigated the matter including to request information from its counterpart (on February 16, 2018) relating to the relationship and transactions between the foreign bank and Mamepe. The FSCA engaged the FIC on the matter on October 17, 2018 and on several occasions thereafter. The FSCA

Box 15. Financial Supervisor Cooperation (concluded)

established that the money was transferred by the foreign bank to Mamepe and various entities and that no investment was made.

On February 19, 2019, based on the findings of its investigation, the FSCA decided to (i) withdraw Mamepe's FSP license; (ii) debar its key individual; and (iii) direct them to repay the foreign bank R10 million ($680,000).

A core issue was that Mamepe provided the foreign bank with a product consignment note for R175 million ($11.9 million) reflecting as an investment on behalf of the foreign bank in commodities. However, that transaction was fictitious. It is in this context that the Financial Services Tribunal later found (when Mamepe unsuccessfully applied to have the FSCA's decision reconsidered) that Mamepe's actions were probably ML.

449. In general, the SARB:PA is active in making and responding to requests for international cooperation. Table 8.4 shows the number of enquiries received from foreign supervisors for information on the fitness and propriety of individuals during 2014–2018.

Table 8.4. South Africa: Foreign Information Requests Received by the SARB:PA—Five Years to December 31, 2018

	2014	2015	2016	2017	2018	Average
Requests received	10	15	13	8	15	12
Requests granted	10	15	13	8	15	12
Average Response Time (days)	>25.6	>22.0	>18.5	>30.9	>27.7	>24.4

450. Generally, the informal requests for information received are fairly consistent with South Africa's risk profile.

International Exchange of Basic and Beneficial Ownership Information of Legal Persons and Arrangements

451. South Africa provides basic information on legal persons to some extent (see generally chapter 7). The CIPC has a website from which anyone, including foreign counterparts, can obtain most basic information. Information online is from 2016, and any information on companies registered before that date has to be searched for manually. The information is, however, not always kept up to date. In addition, other authorities such as the SARS, the FIC, the SARB, and the SAPS share basic information to the extent that they hold it when requested. For example, the FIC shares information on legal persons and legal arrangements which it obtains from the CIPC or from the AIs.

452. South Africa's capacity to exchange BO information in a timely manner is more limited. The authorities do receive requests for BO information from foreign jurisdictions. However, the cases they provided did not clearly demonstrate that they were able to obtain and provide the information routinely. One case where they were able to do so is the Gregory case (see Box 16 below). As discussed in chapter 7, the CIPC does not always hold BO information, and the authorities rely more on obtaining such information from AIs. However, that information, to the extent it exists, may not be accurate as the AIs cannot verify it with the CIPC. The process to obtain BO information

is long as the banks will only release the information if they are served with a subpoena. This can take 7 to 10 days each time a subpoena is served, but if there are complex corporate structures, it can take SAPS a number of weeks to access the first level of legal (shareholder) ownership information using various sources, and then longer to get to the actual BO information. A number of repeated subpoena requests on banks may be required.

453. Most basic but not full BO information about trusts can be provided to foreign requesters. The Master's Office, which is responsible for the registration of trusts, obtains and maintains all basic information[75] (see section on Legal Persons and Arrangements). Most basic information, except names of trustees, is available on the Master's Office website. The Master's Office can provide details about trustees within 15 days when subpoenaed, but not for other persons who control or benefit from the trust (see Section on Legal Persons and Arrangements). Thus, a foreign request must be made in a way that results in a subpoena being served on the Master's Office by a domestic competent authority for the information to be availed. In the light of the limited information held by the Master's Office and the need for a subpoena, the competent authorities cannot provide foreign jurisdictions with full BO information when requested. Some BO information can be obtained from AIs and provided to foreign requesters, but the authorities did not demonstrate that this occurred or that it was timely.

Box 16.1. John Gregory Stouch: Incoming Request

An ML-related MLA request was received on August 16, 2016, which included obtaining bank statements and company records from the registrar of companies, including BO information. The appropriate information was obtained from the CIPC and a bank. The CIPC records were obtained using domestic cooperation and the bank records following the serving of a subpoena. The information was delivered to the requesting state during February 2018 (18 months after the request was made).

C. Overall conclusions on IO.2

454. The authorities demonstrated that they provide MLA and extradition to other jurisdictions to some extent but seek it to a much lesser extent. This imbalance is not consistent with South Africa's risk profile, especially in relation to *"State capture"* issues. They also did not demonstrate that they provide the assistance requested in a timely manner; the turnaround time averages over one year. Of concern is that a significant proportion of requests are returned unexecuted due to a failure to comply with South African requirements without the authorities giving proactive assistance on how those requests could be resubmitted or supplemented successfully. The authorities have increased the volume of ML/TF MLA requests that they make in recent times, but requests often suffer from delays in getting responses, especially relating to *"State capture"* and need major improvements to how they follow up such requests. Most authorities are reasonably good at exchanging information with their foreign counterparts on an informal basis consistent with the risk profile. South Africa provides some basic information for companies and

[75] The information obtained includes trust name, file number, names of the trustees and their South African identification number, and the office where the trust was registered.

trusts in a timely manner. The main challenge to providing BO information in a timely manner is that this information is not readily available.

455. South Africa is rated as having a moderate level of effectiveness for IO.2.

Annex I. Technical Compliance Annex

This section provides detailed analysis of the level of compliance with the FATF 40 Recommendations in their numerical order. It does not include descriptive text on the country situation or risks and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the MER.

Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the previous ME in 2009. This report is available at http://www.fatf-gafi.org/countries/#South%20Africa.

South Africa does not fully regulate and supervise for AML/CFT all of the financial activities and DNFBPs required under the FATF standard. These scope deficiencies are specifically identified in appropriate places throughout this section. In addition, there are many criteria rated "mostly met" where the only deficiency relates to scope. Where appropriate, these are notated with the phrase "Scope deficiency".

Recommendation 1 – Assessing Risks and Applying a Risk-Based Approach

This is a new Recommendation.

Criterion 1.1 – *(Partly met)* South Africa is in the process of carrying out its first coordinated assessment of ML/TF risks at the national level. The methodology used involves examining ML/TF/PF threats, vulnerabilities, and consequences. The approach taken is predominantly qualitative rather than quantitative, relying primarily on experts' judgement. Several SRAs conducted recently fed into the NRA with respect to sector vulnerabilities. These include banking, insurance, ADLAs (which are MVTS), securities firms, financial service providers and CIS managers. A document laying out the primary key findings of ML risks was concluded in June and revised in July 2019. A similar document on TF risks was completed subsequently. Apart from the NRA process, there are other exercises that are not focused on ML/TF risks but may inform the understanding of ML/TF risks. These include, for instance, ongoing work of the IFWG[1] to understand the evolving FinTech landscape and National Intelligence Estimate (NIE) that identifies national security threats related to ML such as illicit financial flows, organized crime, corruption and the illicit economy, etc., and the threat assessments conducted by the PCMC.

Criterion 1.2 – *(Met)* An IDC was established in November 2018 to coordinate on AML/CFT matters at the national level, under which the NRA WG, chaired by the FIC[2] was established in January 2019 to coordinate the NRA process.

[1] Members: the NT, the FSCA, the FIC, and the SARB.

[2] Members include all members of the IDC, the NICOC, and the SIU.

Criterion 1.3 – *(Partly Met)* The authorities indicated their commitment to keep the ML and TF NRA up to date, which has not been recorded in any official document.[3]At the agency level, the SARB:PA's policy is to conduct ML/TF risk assessment of the banking sector every two years. This however is not the case for other sectors.[4]

Criterion 1.4 – *(Partly met)* Various mechanisms are available to share the results of risk assessments when they are available. The NRA WG will coordinate the process of producing and delivery of the information on the results of the NRA process once completed. It is, however, not specified in the NRA WG's draft TOR which agencies or institutions the NRA will be shared with. At the sector level, there are mechanisms to share risk assessments among financial supervisors. MOUs have been signed under the Financial Sector Regulation (FSR) Act, ss. 76 and 77, between: (i) the SARB and the FSCA; (ii) the SARB:PA, SARB and FIC; (iii) the SARB:PA and the FSCA; (iv) the SARB:PA, SARB, and the National Credit Regulator; and (v) the SARB:PA and the SARB.[5] These MOUs contain provisions on information sharing, which can be used to facilitate sharing of ML/TF risk assessments, when they are available. Although the authorities either have shared risk assessments with some FIs or intend to do so with others, there are no specific arrangements for such purposes. Likewise, no mechanisms exist to enable sharing of risk assessment results among supervisors of DNFBPs as well as with the DNFBPs.

Criterion 1.5 – (Partly Met) The NRA WG is mandated to "coordinate the collaboration between departments and agencies in efforts to understand and mitigate identified ML and TF risks, including the identification of key priority areas". However, there is no evidence that resources have been allocated across the AML/CFT authorities based on risks. At the agency level, the SARB:PA adopted a RBA to AML/CFT supervision of banks in 2017 and recently began the application to supervision of insurance companies (see c.26.5). Only within the banking sector, ML/TF risks inform the frequency and intensity of supervision but only to a limited extent. There is also no evidence that allocation of supervisory resources at the sector level is oriented by ML/TF risks.

Criterion 1.6 – *(Not Met)* CFIs (which includes stokvels), credit providers other than money lenders against securities, FinTech companies (that offer financial services and are not VASPs or FSPs), DPMS that are not KRDs, accountants (for activities other than providing financial services), and CSPs other than attorneys are not AIs subject to AML/CFT obligations (except the general requirements to file suspicious transactions that apply to any person who carries on a business, is in charge of or manages a business, or is employed by a business and has a suspicion – see R.20) nor to supervision or monitoring. The exclusions are not based on proven low ML/TF risks.[6]

[3] The preliminary findings of the NRA indicate that the 2019 ML NRA findings will be "reviewed on an ongoing basis".

[4] The FSCA also intends to update the SRA of the securities sector every two years.

[5] See: www.resbank.co.za/PrudentialAuthority/FinancialSectorRegulation/Pages/Financial-Sector-Regulation-Act.aspx

[6] The authorities have initiated the process that aims to extend the AML/CFT obligations to cooperative banks, high-value goods dealers (including DPMS), accountants, and CSPs by notice issued by the NT.

Criterion 1.7 – *(Partly Met)* South Africa partially addresses higher risks through requiring AIs[7] to consider risk factors communicated by the authorities based on the authorities' understanding of ML/TF risks at a national or sector level in its risk assessment (FIC GN7, para. 41). Some FIs and DNFBPs are not AIs and are not subject to these requirements (see c.1.6). South Africa also brought MVDs, which are deemed high-risk, under the AML/CFT regime. Beyond preventive measures, South Africa gives a high priority to financial inclusion which could help bring people to the formal economy and mitigate the ML/TF risks arising from the informal sector.

Criterion 1.8 – *(Mostly Met)* AIs can apply simplified CDD (FIC Act, s.42(2)(m)) where they assess their ML/TF risks as lower (GN7, para. 56). An AI is must consider risk factors identified at a national or sector level in its risk assessment (see c.1.7). As such, the identification of lower-risk scenarios by an AI must be done consistent with the authorities' assessment of the ML/TF risks. Some FIs and DNFBPs are not subject to these requirements (see c.1.6).

Criterion 1.9 – *(Partly met)* AIs' implementation of the measures described under c.1.7, c.1.8, c.1.10, c.1.11 and c.1.12 are subject to supervision as described under c.26.1, c. 26.4, c.28.2 and c. 28.5 and suffer from the same deficiencies noted there. Some FIs and DNFBPs are not subject to these requirements thus are not supervised or monitored for compliance (see c.1.6).

Criterion 1.10 – (*Mostly Met)* An AI must develop, document, maintain and implement an AML/CFT RMCP, (FIC Act s.42(1)). The RMCP should allow the institution to identify, assess, monitor, mitigate, and manage ML/TF risks that the provision of products and services by the institution may give rise to (FIC Act, s.42(1)). AIs must identify and analyze their ML/TF risks to understand them (GN7, para. 43).

a) *(Mostly met)* An AI must document the methodology, procedures of risk assessment as well as the conclusion reached in its RMCP (GN7, para. 47)

b) *(Mostly met)* GN7 contains risk factors that AIs are expected to consider, including those related to products and services, delivery channels, geographical locations, and clients (GN7, para. 37-40). The application of risk management systems and controls must be commensurate with the extent of assessed risks (GN7, para. 27).

c) *(Mostly met)* An AI is expected to re-evaluate the relevance of risk factors and the appropriateness of risk-ratings from time to time and determine the intervals at which this will be done (GN7, para. 46).

[7] AI ("accountable institution"), as defined in the FIC Act, covers attorneys, TSPs, real estate agents, AUs of an exchange, banks, mutual banks, long-term (life) insurers, casinos, foreign exchange dealers, businesses of lending money against the security of securities, financial service providers (including financial advisors, which include insurance intermediaries, asset managers, and hedge fund managers), CIS managers, Postbank, Ithala, and money remitters.

d) *(Mostly Met)* An AI must make its RMCP, which includes risk assessments (see (a) above), available to FIC or a supervisory body (FIC Act, s.42(4)).

Scope deficiency: Some FIs and DNFBPs are not subject to these requirements (see c.1.6).

Criterion 1.11 – (*Mostly met).* All criteria have a scope deficiency (see c.1.6).

a) *(Mostly met)* An AI must develop, document, maintain, and implement a RMCP (FIC Act s.42(1)). The RMCP must be approved by the board of directors, senior management, or other person or group of persons exercising the highest level of authority (FIC Act, s.42(2B)).

b) *(Mostly met)* An AI must review its RMCP regularly to ensure that the RMCP remains relevant to the AI's operations (FIC Act, s.42(2)(c)). The board of directors or senior management must ensure that the AI's staff adhere to its policies, procedures and processes designed to limit and control ML and TF risks (GN7, para. 182).

c) *(Mostly met)* AIs must take enhanced measures, in terms of the range, degree, frequency or intensity of controls, when risks are higher (GN7, para. 55)

Criterion 1.12 – (*Partly met)* AIs can take simplified measures when the risks are assessed as lower (GN7 para. 56) but there are no requirements that such measures are not allowed when there is a suspicion of ML/TF or when the requirements under c.1.10 and c.1.11 are not met. These do not apply to some FIs and DNFBPs (see c.1.6).

Weighting and Conclusion

South Africa has started identifying and assessing its national ML/TF risks but is yet to conclude either exercise. Most AML/CFT authorities have not yet implemented a RBA. Risk assessment and mitigation obligations for the main FIs are relatively robust but do not apply to all FIs or DNFBPs.

Recommendation 1 is rated partially compliant.

Recommendation 2 – National Cooperation and Coordination

South Africa was rated compliant on national cooperation (former R.31) in the 2009 MER.

Criterion 2.1 – (*Partly met)* South Africa has not developed coordinated and holistic national AML/CFT policies informed by identified risks but existing policies address some of the risks identified, including those to promote financial inclusion, bring sectors deemed high-risk (e.g., MVDs) under the AML/CFT regime, and obligate CTRs (more details under section 2.2).

Criterion 2.2 – (*Mostly Met)* The IDC is mandated to: (i) identify gaps, assess the effectiveness of AML/CFT measures, and to make proposals to departments to improve the AML/CFT regime; and (ii) coordinate the collaboration between departments and agencies in their efforts to understand and mitigate identified ML/TF risks including the identification of key priority areas**.** It however excludes

supervisors of the DNFBP sectors covered by the regime[8] and the CIPC, the company registry. The FIC is mandated to review FIC Act implementation, a central piece of legislation in the country's AML/CFT legal framework, annually and report to the Minister of Finance (FIC Act. S. 4(e)).

Criterion 2.3 – (*Mostly met)* The IDC provides a forum for the FIC, LEAs, and financial supervisors to coordinate on policy. It however does not involve all stakeholders (see c.2.2).

MOUs are the main mechanisms for operational cooperation and coordination. MOUs have been signed: (i) between the FIC and the financial regulators; (ii) among financial supervisors; (see c.1.4); (iii) between the FIC and LEAs; (iv) and among the SSA and the SARS. Mechanisms established at the operational level for purposes other than AML, such as the IFFTT, established to facilitate the investigation and prosecution of priority cases that involve illicit financial flows, and the ACTT to prioritize investigation and prosecution of corruption cases could potentially facilitate coordination on some ML cases.

TF is not addressed as the part of the discussion on terrorism at the policy level. The CTFC, chaired by the SSA, facilitates coordination on counter terrorism at the operational level, which also reviews the TF aspects in each terrorism cases. The DIRCO convenes the IDWG-CT, which is responsible for coordinating and overseeing the implementation of South Africa's international obligations associated with TF arising from the UNSCRs as well as keep implementing agencies apprised of developments on this matter in the international arena. Its members however do not include regulators responsible for overseeing implementation of the UNSCRs by FIs and DNFBPs.

Criterion 2.4 – (*Not Met)* There are no mechanisms to allow cooperation and coordination to combat the financing of proliferation of weapons of mass destruction.

Criterion 2.5 – (*Not Met)* There is no evidence of cooperation and coordination between relevant authorities to ensure the compatibility of AML/CFT requirements with Data Protection and Privacy rules and other similar provisions.

Weighting and Conclusion

South Africa has designated the IDC to coordinate policy making on AML/CFT but is yet to develop national policies on AML/CFT informed by risks identified. Various mechanisms exist to enable inter-agency cooperation at both policy and operational levels albeit some gaps.

Recommendation 2 is rated partially compliant.

Recommendation 3 - Money Laundering Offense

[8] The real estate sector, casinos; attorneys, and the accounting profession.

In its previous MER, South Africa was rated largely compliant with the former R.1. The identified defect was the POCA, s.6 (Acquisition, possession or use of proceeds of unlawful activities) did not extend to the perpetrator of the predicate offense.

Criterion 3.1 – (*Met)* ML is criminalized in line with the relevant articles of the Vienna and Palermo Conventions. Under s. 4 POCA, it is an offense for any person who knows or ought reasonably to have known the property represents the proceeds of unlawful activities to enter into an agreement or arrangement or transaction in connection with the property, or performs any other act in respect of the property, which has the effect or is likely to have the effect of concealing or disguising the nature, source, location, disposition, or movement of the property or ownership thereof, or of enabling any person who has committed the offense to avoid prosecution. Under s.5 POCA, it is an offense to assist another person to benefit from proceeds of unlawful activities by retention or control of the proceeds on behalf of the other person or by making available the proceeds to the other person for his benefit. Under s.6 POCA it is an offense for a person to acquire, use or possess property which s/he knows or ought reasonably to have known represents proceeds of unlawful activities of another person. Ancillary offenses are available: see c.3.11.

Criterion 3.2 – (*Met)* South Africa adopts an "all crimes" approach for predicate offenses. Predicate offenses include a range of offenses in each of the designated categories offenses.

Criterion 3.3 – (*NA)* South Africa does not apply a threshold approach for predicate offenses.

Criterion 3.4 – (*Met) "Property"* is broadly defined to include property of any type, regardless of value; this includes VAs (POCA, s.1). "Proceeds of unlawful activities" means any property or service, advantage, benefit or reward derived, received or retained directly or indirectly in South Africa or elsewhere in connection with unlawful activities and includes any property representing property so derived (POCA, s.1).

Criterion 3.5 – (*Met)* There is no requirement to obtain a conviction for the predicate offense, nor to allege or prove a specific offense from which the property is derived: *S v Imador* 2014 (2) SACR 411 (WCC).

Criterion 3.6 – (*Met)* The definition of "proceeds of unlawful activity" and "unlawful activity" extends to conduct occurring in South Africa or elsewhere. "Unlawful activity" is defined in the POCA to mean any conduct which constitutes a crime, or which contravenes any law whether such conduct occurred in South Africa or elsewhere. This includes proceeds from offenses committed in other jurisdictions.

Criterion 3.7 – (*Mostly met)* Sections 5 POCA (Assisting another to benefit from proceeds of unlawful activity) and 6 POCA (Acquisition, possession or use of proceeds of unlawful activities) do not apply to the perpetrator of the predicate offense. Although s.4 POCA (ML – by entering an agreement, arrangement or transaction or performing any other act in connection with the property with the effect of concealing or disguising property or assisting a person to avoid prosecution or to remove or diminish property) can cover self-laundering, this provision does not necessarily extend

to all cases e.g. when the transaction or arrangement does not or is not likely to have the effect of concealing or disguising the source of the proceeds or its location or ownership, or enabling someone to avoid prosecution or remove or diminish those proceeds; see *S v Van Der Linde* [2016] 3 All SA 898.

Criterion 3.8 – (*Met)* The ML offenses in the POCA, ss. 4 to 6, apply to any person who "knows" or "ought reasonably to have known" that the property is or forms part of the proceeds of unlawful activity:s.1(2)&(3) POCA for the mental element of the offense. South African law permits intent to be inferred from direct facts as well as circumstantial or other indirect evidence: *S v Imador* 2014 (2) SACR 411 (WCC); *De Vries v the State*, High Court of South Africa, Case No. 67/2005 [2011] ZASCA 162

Criterion 3.9 – (*Met)* Proportionate and dissuasive criminal sanctions apply to the ML offenses in the POCA, ss. 4 to 6. Offenses are punishable with a fine not exceeding R100 million ($6.8 million) or imprisonment for a period not exceeding 30 years (POCA, s.8).

Criterion 3.10 – (*Met)* The CPA, s.332 allows for prosecution of corporate bodies in respect of any offense. A criminal prosecution does not preclude civil liability (e.g. for damages) or administrative proceedings (which may be used under regulatory supervision). Such action is without prejudice to the criminal liability of natural persons. The sanction for the ML offense committed by a corporate body is proportionate and dissuasive being a fine not exceeding R100 million ($6.8 million)

Criterion 3.11 – (*Met)* South African law recognizes the concept of ancillary offenses including conspiracy, incitement, and attempts applicable to the ML offenses under the POCA, ss. 4 to 6 (s. 18 Riotous Assemblies Act).

Weighting and Conclusion

South Africa meets all criteria except that a minor shortfall exists for self-laundering (acquisition, possession or use of proceeds does not extend to the perpetrator of the predicate offense).

Recommendation 3 is rated largely compliant.

Recommendation 4 - Confiscation and Provisional Measures

In its previous MER, South Africa was rated compliant with the former R.3.

Criterion 4.1 – (Mostly Met)

a) *(Met)* The POCA provides for criminal (conviction based) confiscation and civil (non-conviction based) forfeiture under the POCA, chs.5&6, respectively. Ch.5 allows for post-conviction confiscation of proceeds of offenses and related criminal activity, including ML, predicate offenses and TF, or property of corresponding value (ss.12 to 36, in particular s.18). "Property is broadly defined (POCA, s.1 – see c.3.4 and ch.6 allows for non-conviction-based forfeiture of instrumentalities of an offense listed in the POCA, sch.1 (including ML and

specified offenses under the POCDATARA), the proceeds of unlawful activities, and property associated with terrorist and related activities (ss.37 to 62, in particular s.50). The non-conviction-based forfeiture procedure is an *in rem* procedure targeting specific tainted property.

b) *(Mostly Met)* Any *"proceeds of unlawful activities"* may *be* confiscated following a conviction for ML or a predicate offense. This means any property or part thereof or any service, advantage, benefit or reward which was derived, received or retained, directly or indirectly, in connection with or as a result of any unlawful activity carried out by any person whether in South Africa or elsewhere. The non-conviction-based forfeiture provisions allow for confiscation of instrumentalities used in ML and predicate offenses. The CPA, s.35 generally provides for the forfeiture and disposal of property used in the commission of an offense following conviction. However, there is no specific provision for confiscation of instrumentalities intended for use in ML or predicate offenses in all circumstances.

c) *(Mostly Met)* "Proceeds of unlawful activities" includes property which is the proceeds of TF and such property may be confiscated following a conviction for the TF offense. The non-conviction-based forfeiture provisions allow for confiscation of instrumentalities used in offenses under the POCDATARA as well as property associated with terrorist and related activity. However, there is no specific provision for confiscation of instrumentalities intended for use in TF in all circumstances e.g. when there has been no commission of a TF offense.

d) *(Met)* Confiscation orders under the POCA, ch.5, are money judgments based on the corresponding value of benefits derived from the defendant's offending. Any realizable property (including legitimately obtained and untainted property) of the defendant may be realized to satisfy the order.

Criterion 4.2 – (Met)

a) *(Met)* A DPP may subpoena persons to appear before a court and to supply information in connection with any criminal offense (CPA, s.205). The POCA empowers the National DPP to request Government Departments to furnish information relevant to investigations under the POCA (POCA, s.71) and to direct that a DPP institute an investigation in terms of the NPA Act, ch.5 (POCA, s.72). Courts are empowered, when making a restraint order, to order the discovery of facts relating to property under the defendant's control and the location of such property (POCA, s.26). The FIC receives financial information reports made to it (FIC Act, s.29) and it can obtain additional information relating to those reports (FIC Act, s.32). The FIC also has additional powers to monitor financial activity (FIC Act, s.35) and the information obtained can be shared with LEAs to assist them in discharging their investigative functions including for confiscation purposes.

b) *(Met)* Authorities investigating ML and TF may apply for search warrants to seize articles (CPA, ss. 20-21). Articles may also be seized without a warrant in defined circumstances (CPA, s.22). A restraint order may be obtained over property that may be realized to satisfy a

confiscation order under the POCA, ch.5 (POCA, s.26). For non-conviction-based confiscation under the POCA, ch.6, a preservation order can be obtained over property that may be tainted and therefore subject to forfeiture (POCA, s.38). The FIC may issue directives to freeze bank accounts for up to 10 working days if there are reasonable grounds to link a transaction or proposed transaction to unlawful activities or TF related activities (FIC Act, s.34). The SARS may obtain a preservation order if it is satisfied on reasonable grounds a tax collection may be frustrated because assets are or will be disposed of or removed (Tax Administration Act, s.163).

c) *(Met)* Offense provisions exist relating to the misuse of information, failure to comply with court orders and hindering persons in the performance of their functions to ensure property subject to confiscation will not be dissipated (POCA, s.75).

d) *(Met)* There are a range of investigative measures to support the confiscation powers under the POCA and the POCDATARA: see c.31.1-31.4.

Criterion 4.3 – (*Met)* Confiscation orders under the POCA, ch.5, are made against the defendant's property. The interests of third parties such as creditors are protected in this process (POCA, ss. 20, 30 and 31). For confiscation orders under the POCA, ch.6, the court may exclude the interests of a third party who can show that he or she did not receive property as a gift and did not have reasonable grounds to suspect that was the proceeds of unlawful activity (POCA, s. 52). Common law can also protect the rights of third parties.

Criterion 4.4 – (*Met)* The NPA:AFU processes provide for the appointment of a Curator Bonis to safeguard, maintain and manage assets the subject of a restraint or preservation order. This process includes liquidation of the assets once a confiscation or forfeiture order is made. The funds realized are paid into the CARA (POCA, ch.7) or to the victim depending upon the court order. Monies paid to the CARA may be utilized for allocation to LEAs, to organizations which render assistance to victims or crime, and for administration of the account (POCA, s.69A). Curators can also be appointed to trace, recover, and safeguard cash pending the outcome of the criminal trial (POCA, s.28) or the forfeiture application (POCA, s.42). Mechanisms exist to manage property seized under search warrant or without a warrant under s.20-22 CPA pending confiscation or forfeiture.

Weighting and Conclusion

South Africa meets all the criteria except there is a minor gap for confiscation of instrumentalities intended for use in ML, predicate, and TF offenses.

Recommendation 4 is rated largely compliant.

Recommendation 5 – Terrorist Financing Offense

South Africa was rated largely compliant with the former SR. II because of the inability to assess effectiveness as South Africa had not had a TF prosecution at the time of the evaluation.

Criterion 5.1 – (Partly Met) The Protection of Constitutional Democracy Against Terrorist and Related Activities Act No. 33 Of 2004 (POCDATARA) came into effect on 20 May 2005 and it contains several offenses related to TF (s.4). Generally, the criminalization of TF in South Africa is broadly consistent[9] with most of the TF Convention. The POCDATARA, however, does exclude from the definition of terrorist activity certain acts committed during an armed struggle.[10] This exemption therefore narrows the scope of the TF Convention. Article 6 of the TF Convention states that 'Each State Party shall adopt such measures as may be necessary, including, where appropriate, domestic legislation, to ensure that criminal acts within the scope of this Convention are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature'.

Criterion 5.2 – (*Met)* The TF offenses ***include*** acquiring, collecting, using, possessing or owning property while that person intends that the property, financial or other service or economic support be used, or while that person knows or ought reasonably to have known or suspected that the property, etc. will be used to commit or facilitate the commission of a specified offense,[11] (POCDATARA, s.4). It further indicates that the property, financial or other service or economic support cannot be provided for the benefit of, or on behalf of, or at the direction of, or under the control of an entity which commits or attempts to commit or facilitates the commission of a specified offense. An 'entity' includes a terrorist organization and individual terrorists. The TF offense therefore extends to any person who willfully provides or collects funds or other assets by any

[9] There are some shortcomings with respect to the criminalization of TF as follows:

- Hague Convention offenses related to aircraft - this is dealt with by the offenses related to hijacking an aircraft in the POCDATARA, s.9, but that section is more restrictive than the convention as it contains additional *mens rea* elements;
- UN Convention on Internationally Protected Persons - the convention distinguishes between attacks on persons or property as, with the former, only an attack is required, whereas with the latter a violent attack is required. However, the offense in the POCDATARA, s.8, is more restrictive as it requires the attack to be violent in both cases;
- Offenses under Montreal Convention and Protocol (relating to civil aviation) and offenses under Vienna Convention on Protection of Nuclear Material - these offenses are not covered in the POCDATARA.

[10] …any act committed during a struggle waged by peoples, including any action during an armed struggle, in the exercise or furtherance of their legitimate right to national liberation, self-determination and independence against colonialism, or occupation or aggression or domination by alien or foreign forces, in accordance with the principles of international law, especially international humanitarian law, including the purposes and principles of the Charter of the United Nations and the Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the said Charter, shall not, for any reason, including for purposes of prosecution or extradition, be considered as a terrorist activity…

[11] A *'specified offence'* is defined in the POCDATARA as the following:

(a) the offence of terrorism referred to in section 2, an offence associated or connected with terrorist activities referred to in section 3, a Convention offence, or an offence referred to in section 13 or 14 (in so far as it relates to the aforementioned sections); or (b) any activity outside the Republic which constitutes an offence under the law of another state and which would have constituted an offence referred to in para. (a), had that activity taken place in the Republic.

Broadly speaking, a *"Convention offence"* refers to those created in fulfillment of the South Africa's international obligations in terms of instruments dealing with terrorist and related activities.

means, directly or indirectly, with the unlawful intention that they should be used, or in the knowledge that they are to be used, in full or in part: (a) to carry out a terrorist act(s); or (b) by a terrorist organization or by an individual terrorist. There is no requirement for a link to a specific terrorist act or acts.

Criterion 5.2 *Bis* – (*Met)* The travel by individuals to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training is criminalized (POCDATARA, s.3).

Criterion 5.3 – (*Met)* 'Property' means money or any other movable, immovable, corporeal or incorporeal thing, and includes any rights, privileges, claims and securities and any interest therein and all proceeds thereof (POCDATARA, s.1). This would include funds or other assets whether from legitimate or illegitimate sources. It would also include Vas.

Criterion 5.4 – (*Met)* The TF offense is not dependent on whether the funds were used to carry out or attempt a terrorist act(s); or that they be linked to a specific terrorist act(s) (POCDATARA, s.17).

Criterion 5.5 – (*Met)* The *mens rea* required for TF offenses includes both intent and negligence. Under South African law the intentional element of the offense can be inferred from objective factual circumstances.

Criterion 5.6 – (*Mostly Met)* The maximum sanction that can be imposed for a TF offense is a fine not exceeding R100 million ($6.8 million) or imprisonment for a period not exceeding 15 years (POCDATARA, s.18). While the maximum sanctions are potentially dissuasive, they are not proportionate compared to the ML offense (maximum 30 years imprisonment) and the terrorism offense (maximum life imprisonment).

Criterion 5.7 – (*Met)* Criminal liability and sanctions for TF extends to legal persons (Interpretation Act No. 33 of 1957). Under South African law, criminal liability does not preclude the possibility of parallel criminal, civil or administrative proceedings where more than one form of liability is available (Criminal Procedure Act 51 of 1977, ss.81-82).

Criterion 5.8 – (*Met)* Any person who threatens, attempts, conspires, aids, abets, induces, incites, instigates, or commands, counsels, or procures the commission of a *POCDATARA* offense has also committed an offense (POCDATARA, s.14).

Criterion 5.9 – (*Met)* South Africa has an all crimes approach; therefore, TF offenses are predicate offenses for ML. Moreover, laundering property linked to terrorist activities is criminalized by providing that a person who becomes concerned in an arrangement which in any way:

- facilitates the retention or control of such property by:
- an entity which commits, attempts to commit, or facilitates the commission of a terrorist related offense; or

- a specific entity identified in a notice (containing the names of individuals and entities listed pursuant to a United Nations Security Council Resolution on terrorism) issued by the President;
- converts such property;
- conceals or disguises the nature, source, location, disposition, or movement of such property; the
- ownership thereof or any interest anyone may have therein;
- removes such property from a jurisdiction; or
- transfers such property to a nominee;
- is guilty of an offense (POCDATARA, s.4).

Criterion 5.10 – *(Met)* The *POCDATARA, s.4* relates to offenses concerning `terrorist activity' which includes TF. The *POCDATARA* defines 'terrorist activity' as acts committed inside or outside South Africa, having effects or causing harm inside or outside South Africa and/or influencing persons etc. inside or outside South Africa.

Weighting and Conclusion

While South Africa meets most requirements for the recommendation there are some minor deficiencies and a major exemption identified with respect to the criminalization of TF as per the TF Convention. The exemption significantly narrows the scope of TF offense in South Africa compared to the TF Convention. There is also a concern with respect to the proportionality of the sanctions for TF in comparison to the sanctions for ML.

Recommendation 5 is rated partially compliant.

Recommendation 6 – Targeted Financial Sanctions Related to Terrorism and Terrorist Financing

In its 2009 MER, South Africa was rated partially compliant on SR.III (former R.6). Deficiencies were the lack of mechanism to communicate effectively actions pursuant to UNSCR 1373 and of guidance to Ais, as well as the lack of mechanism for bringing delisting requests to the UNSC and for notifying and obtaining the approval of the Al-Qaida and Taliban Sanctions Committee for granting access to frozen assets as is required by S/RES/1452(2004).

Criterion 6.1 – *(Not met)* There are no mechanisms establishing a domestic process for identifying targets or for procedures to be followed when making a designation proposal.

a) (*Not met*) There is no provision identifying a competent authority or a court as having responsibility for proposing persons or entities for designation. South Africa implements UNSCRs 1267, 1989 and 1988 sanctions regimes through the process described in the

POCDATARA (s.25). However, this Act simply gives the President responsibility for notifying – through proclamation in the Gazette – when the UNSC has identified a person or entity under these UNSCRs.

b) *(Not met)* There is no mechanism for identifying targets for designation.

c) *(Not met)* South Africa did not demonstrate they apply an evidentiary standard of proof or "reasonable grounds" or "reasonable basis" when deciding whether or not to make a proposal for designation. There is no provision establishing that proposals would have to be conditional upon the existence of a criminal proceeding.

d) *(NA)* Not applicable, to date, South Africa has proposed no names. And has not had to put into practice the procedures and standard forms for listing adopted by the relevant UN committees.

e) *(NA)* Not applicable – to date, South Africa has proposed no names.

Criterion 6.2 – **(***Partly met)* For UNSCR 1373, South Africa relies on the freezing mechanism of the POCDATARA, s.23(1). As per the non-conviction-based procedure described in c.4.1, the procedure in s.23 is an *in rem* action. This means that a freezing order only focusses on specific property identified at the time of the order rather than on any asset of a designated person in South Africa at any point in time. This is not consistent with a designation for TFS under UNSCR 1373.

a) *(Partly Met)* The competent authority having the responsibility for designating persons or entities that meet the UNSCR 1373 criteria for designations is the High Court. It may order a freezing based on an *ex parte* application by the National DPP to a judge (POCDATARA, s.23). When a request to freeze is received from another country, the NPA, as the main authority authorized to bring the application, will assess the nature of the request and notify all the relevant agencies (FIC, Police, security services) that would provide it advise for deciding to submit or not an *ex parte* application. However, when receiving a request from another country authorities cannot proceed with a freezing order under s.23 unless property of the designated person is located in South Africa.

b) *(Not met)* The mechanism to identify targets for designation is the freezing mechanism in the POCDATARA, s.23. This *in rem* procedure is, however, not consistent with a proper designation under this UNSCR as it does not amount to a general freezing order. In addition, the lack of property of a designated person in South Africa when the request is made limits the identification of targets.

c) *(Mostly Met)* The threshold of "reasonable grounds to believe" applies whether the designation is put forward by the national authorities or at the request of a foreign country (POCDATARA, s.23). There is nothing in rules or procedures to indicate that the NPA must make a "prompt determination" to apply to the Court for an *ex parte* decision.

d) *(Met)* An evidentiary standard of proof of "reasonable ground to believe" applies (POCDATARA, s.23). This is not conditional upon the existence of a criminal proceeding as the case is put before the High Court *ex parte*.

e) *(NA)* Not applicable, as no names have been proposed by South Africa to date.

Criterion 6.3 – (Met):

a) *(Met)* Competent authorities have legal authorities and procedures to collect or solicit information to identify property of persons or entities that meet the criteria for designation. Those are entailed within legal powers governing the functioning of relevant authorities to gather relevant information in line with their statutory mandates (FIC Act for the FIC, CPA, s. 205 for LEAs).

b) *(Met)* The application from the DPP is *ex parte* (POCDATARA, s.23).

Criterion 6.4 – (*Partly met)* Authorities do not implement TFS without delay for UNSCRs 1267, 1989 and 1988. There is no provision requiring authorities to do so and the process can take months. UNSCR designations are implemented through Presidential notification which leads to freezing obligations on all persons (POCDATARA, ss.4 and 25). As regards UNSCRs 1267, 1989 and 1988, South Africa receives immediate email notifications from the UN and a SAPS official monitors the UN website daily. If a UNSCR list changes, the official prepares a draft proclamation to be signed by the National Commissioner before being sent to the Minister of Police for approval. Once approved, the Proclamation is forwarded to the President's office for signature. An acting President (s.9(1) of the Constitution) can sign on the President's behalf if the President is unavailable. As soon as the Proclamation is signed, it is published in a special urgent *Gazette* that can be issued at any time. TFS obligations come into effect at publication (POCDATARA, s.4). This process can take up to a few months. There is no provision requiring the authorities to implement "without delay". Implementation of TFS under UNSCR 1373 is without delay as the obligation to act without delay is triggered by a freezing order under the POCDATARA (s.23) which is concomitant with the designating decision. As explained in c.6.2, this freezing order does not amount to a proper designation as it only focusses on property identified rather than on any asset of a designated person.

Criterion 6.5 – (Partly met):

a) (Partly met) The POCDATARA, s.4(2) prohibits any person from "dealing with, entering into or facilitating any transaction or performing any other act, providing financial or other services in respect of property which that person knows or ought reasonably to have known or suspected to have been acquired, collected used, possessed, owned or provided **for the benefit of a specific entity** identified in a notice issued by the President" under the POCDATARA s.25 to implement a designation under UNSCRs 1267, 1989 and 1988 and subsequent resolutions (see c.6.1). This prohibition is consistent with the FATF definition of freeze and covers transfer, conversion, disposition or movement of funds or other assets.

Once the prohibition is in force, the freezing is immediate and "without prior notice". However, the provision on which South Africa rely to implement UNSCR 1373 designations (POCDATARA, s.23(1)) would prohibit any person to deal with assets identified in the court order rather than any asset of a designated person (see c.6.2).

b) (Partly Met)

i. *(Partly Met)* There is no requirement that the funds were used to carry out or attempt a terrorist act or that the funds are linked to a specific act. (POCDATARA, s.17).

ii. *(Met)* The prohibition under the POCDATARA, s.4 extends to all funds and other assets that are owned or controlled by a designated entity under UNSCRs 1267, 1989 and 1988 and subsequent resolutions, and not just those that can be tied to a particular terrorist act. However, as explained in c.6.2, the freezing order under s.23 which would implement a designation based on UNSCR 1373 is an *in rem* action, i.e. the order only focusses on specific property identified in the order rather than on any asset of a designated person.

iii. *(Met)* Property is defined widely (POCDATARA, s.1 and POCA, s.1)(see c.5.3 and c.3.4) This includes proceeds, and therefore "funds and assets derived or generated" as required by sub criterion (iii).

iv. *(Not Met)* The prohibition does not cover funds or other assets of persons and entities *"acting on behalf or, or at the direction, of a designated person"*.

c) *(Partly met)* The prohibition under the POCDATARA, s.4 applies to both nationals and any person or entity in South Africa jurisdiction (POCDATARA, s. 15(1)(b)). However, deficiencies identified in c.6.5(b) also apply for this sub criterion.

d) *(Partly met)* For designations pursuant to UNSCR 1267, 1989 and 1988, the mechanism for communicating designations is the publication of the Presidential proclamation in the *Gazette* and notices published on the websites of the SAPS and the FIC. However, it is not clear if the notice contains clear guidance for Fis, DNFBPs, and other persons or entities as regards their specific obligations. There is no mechanism for UNSCR 1373.

e) *(Partly met)* Every AI which has in its possession or under its control property owned or controlled by on behalf of, or at the direction any entity that has committed or attempted to commit a specified offense (including TF offense), or any entity identified under the POCDATARA, s.25, must report that fact to the FIC (FIC Act s.28A). This would not cover attempted transactions when the assets are not in the AI's possession or control. In addition, there are no reporting obligations for assets frozen or actions taken under UNSCR 1373.

f) *(Met)* Any person having an interest, which may be affected by a decision on an ex parte application (such as a freezing of a designated persons assets), may apply to a court for relief (Supreme Court Act, s.6(4)(b)).

Criterion 6.6 – (Partly met)

a) *(Not met)* There is no publicly known procedure through which South Africa can bring delisting requests to the attention of the UNSC for consideration.

b) *(Not Met)* There are no delisting procedures in relation to freezing actions taken pursuant to UNSCR 1373.

c) *(Met)* Any person having an interest that may be affected by decision on an *ex parte* application (such as freezing order under the POCDATARA, s.23) may apply for a court for relief (Supreme Court Act, s.6(4)(b)).

d) *(Not met)* There is no procedure to facilitate review by the 1988 Committee.

e) *(Not met)* There is no procedure for informing designated persons and entities of the availability of the UN Office of the Ombudsperson to accept delisting petitions.

f) *(Met)* The Uniform Rules of Court set out procedures whereby a person affected by a freezing order can seek relief. In case of false positive, any person may apply to a court for a declaratory order that the President's Proclamation does not apply to him/her.

g) *(Partly met)* For designations pursuant to UNSCR 1267, 1989 and 1988, the President is the authority in charge of issuing a notice by proclamation and such notices cover de-listing and unfreezing. However, the notice does not contain clear guidance for Fis and DNFBPs. There is no mechanism for UNSCR 1373.

Criterion 6.7 – (*Partly met)* For freezing orders under s.23 related to UNSCR 1373, an affected person would have to apply to a court for expenses, and the state would have to argue that it should be done in the spirit of the appropriate UN resolutions. However, there is no provision authorizing use of funds or other assets that were frozen as provided for in UNSCR 1452.

Weighting and Conclusion

South Africa has major shortcomings for this recommendation. There are delays in the implementation of TFS for UNSCRs 1267, 1989 and 1998, and no domestic process for making proposals nor identifying targets for designation under these resolutions. For UNSCR 1373, South Africa relies on a freezing mechanism that does not amount to proper designations for TFS as it focuses on identification of property rather than on designated entities.

Recommendation 6 is rated non-compliant.

Recommendation 7 – Targeted Financial Sanctions Related to Proliferation

These obligations were added during the revision of the FATF Recommendations in 2012 and were thus not considered during the previous ME. The amendment to the FIC Act that put in place the freezing regime to implement TFS related to PF came into force in April 2019.

Criterion 7.1 – (Partly met) When the UNSC adopts a new Resolution with PF-related TFS, the Minister must announce its adoption in the Gazette (FIC Act, s.26A). Publication in the Gazette – which makes the obligation enter into force, is done in a matter of days. Once publication occurs, designations that result from subsequent listings or amendments by the UNSC of existing UNSCRs, are done without relying on further notices by the Minister and the FIC can notify the changes to the list on the FIC website. In those cases, the entry into force of the modification to the list is the FIC's notice publication. This system does not allow for implementation without delay in all instances as the publication of the Minister's notice in the Gazette is done within a matter of days after the adoption of a UNSCR. The FIC has issued such notifications in most cases within 24 hours. The process is however longer on weekends and took up to 3-5 days in a few cases.

Criterion 7.2 – (Mostly met) The Minister of Finance and the FIC are responsible for implementing TFS. The framework is not fully consistent with what is required by c.7.2.

a) (Mostly met) The FIC Act, s.26B(2), "prohibits any natural or legal person to, directly or indirectly, in whole or in part, and by any means or method to deal with, enter into or facilitate any transaction or perform any other act in connection with property which such person knows or ought reasonably to have known or suspected to have been acquired, collected, used, possessed, owned or provided for the benefit of, or on behalf of, or at the direction of, or under the control of a person or an entity identified pursuant to a UNSCR contemplated in a notice issued by the Minister under s.26A of the FIC". GN7 specifies that the "FIC Act requires …[AIs]… to freeze property and transactions". The prohibition is consistent with the FATF definition of freeze and covers transfer, conversion, disposition or movement of funds or other assets. The prohibition enters into force immediately once the designated person has been identified, either through a ministerial notice or directly through a FIC notice, which is not "without delay" in all instances (see c.7.1). The obligation to freeze is "without prior notice".

b) (Mostly Met) The definition of property under the FIC Act is wide and consistent with the FATF definition of freeze (see c.3.4 and c.5.3).

   i. (Met) The FIC Act extends to all funds and other assets that are owned or controlled by a designated entity, and not just those that can be tied to a particular threat of proliferation.

   ii. (Met) S.26B(2) covers funds and other assets that have been acquired, collected, used possessed, owned or provided "for the benefit of, or on behalf of, or at the direction of, or under the control" of a natural or legal designated person. This covers "funds and

other assets owned or controlled, directly or indirectly" and there is no provision precluding the freeze of "jointly owned" funds.

iii. (Met) It includes proceeds, and therefore "funds and assets derived or generated".

iv. (Not Met) It does not extend to funds and other assets of persons acting on behalf of, or at the direction of a designated person or entity. S.26B(2) only covers property that has been acquired, collected, used, possessed, owned, or provided for the benefit of, on behalf of, or at the direction of, or under the control of a designated person. This excludes property of a non-designated person that would be acting for a designated person and that would have not been acquired for the benefit of a designated person.

a) (Mostly met) The prohibition applies to both nationals and any person or entity inSouth Africa jurisdiction. The prohibition does not apply if the person or entity gets a license from the Minister to engage in such activity (FIC Act, s.26C). However, deficiencies identified in c.7.2(b) also exist for this sub criterion.

b) (Mostly met) The Minister must announce, "upon adoption" of the resolution by notice in the Gazette (FIC Act, s.26A). The Notice is also published on the FIC's website. Any person can subscribe to the List and receive email notification of any additions or amendments to the List. Guidelines (GN7) have been issued on the FIC Act's obligation in relation to TFS for R.7. However, they provide general guidance and only limited materials and sector specific details to guide in practice entities with implementation.

c) (Met) An AI must report to the FIC any funds in its possession or under its control related to s.26A (FIC Act s.28A(c)). All FIs and DNFBPs (including those not referred as AIs in the FIC Act) must report to the FIC regarding assets frozen or actions taken pursuant to TFS including for attempted transactions (FIC Act, s.29).

d) (Met) Third parties can rely on the common law bona fide defense. In addition, no criminal or civil action lies against any person complying in good faith with a provision related to implementation of obligations under R.7 (FIC Act, s38(1)).

Criterion 7.3 – (Mostly met) There are measures for monitoring and ensuring compliance for most FIs and DNFBPs with the requirements of R.7 (see c.26.1, c.28.2, and c.28.3 regarding those not subject to FIC Act supervision). Every supervisory body is responsible for supervising and enforcing compliance with the FIC Act and can impose administrative sanctions for compliance failures or institute court proceedings (FIC Act, ss. 45, 45C, and 45F). Thus, any person not complying with obligations set out in s.26B can be sanctioned.

Criterion 7.4 – (Partly met)

a) (Not met) There are no provisions nor publicly known procedures enabling or informing listed persons and entities to petition a request for de-listing at the Focal point established pursuant to UNSCR 1730.

b) (Met) The Uniform Rules of Court set out procedures whereby a person affected by a freezing order can seek relief from the Court. In case of false positive, any natural or legal person may apply to a court for a declaratory order that the President's Proclamation does not apply to him/her and order the unfreezing.

c) (Mostly Met) The Minister can authorize access to funds or other assets for basic expenses and to satisfy certain judgments or arbitral liens (FIC Act, s.26C). The provision requires that the Minister's permission is to be given in accordance with the UNSCR. However, these provisions do not cover "extraordinary expenses". The FIC website sets out how a person can apply for permitted financial services.

d) (Mostly met) The Director must give notice of a decision of the UNSCR to delist under an existing UNSCR (FIC Act, s.26A) and does this by publishing a notice on the FIC website. In addition, the Minister may revoke a UNSCR notice if the related sanctions have been withdrawn by the UNSC (FIC Act, s.26A(4)). In addition, any person can receive emails from the FIC on updates relating to the listing, amendments or delisting of persons and entities. Guidelines (GN7) have been issued on TFS for R.7. However, those do not clarify precisely FIs', DNFBPs', and other persons' or entities' obligations to respect a de-listing or unfreezing action.

Criterion 7.5 – (Mostly Met)

a) (Mostly Met) There are provisions allowing authorities to permit addition to any account frozen of interests or other earnings due. The FIC Act, s.26C(d), provides that the Minister "may permit" a person to conduct financial services or deal with property if it is necessary to accrue interest or other earnings due on accounts. Once accrued, such interests, earnings and payments continue to be subject to the prohibition obligation provisions or are frozen. However, this permission is not limited to interests or other earning or payments that arose prior to the date on those became subject to the provisions of the UNSCR.

b) (Met) The Minister "may permit" a person to conduct financial services or deal with property if it is necessary to make a payment to a third party which is due under a contract, agreement or other obligation made before the date on which the person or entity was identified by the UNSC (FIC Act, s.26C(c)). The provision requires that the Minister's permission is to be given in accordance with the UNSCR", covering conditions (i), (ii), and (iii) of c.7.5(b).

Weighting and Conclusion

South Africa has moderate shortcomings as there are some delays in the implementation of TFS. In addition, the prohibition does not extend to funds and other assets of persons acting on behalf of, or at the direction of a designated person or entity, guidance does not provide enough sector specific details for all AIs and RIs for AIs, and there are no provisions nor publicly known procedures enabling or informing listed persons and entities to petition a request for de-listing. There are

measures for monitoring and ensuring compliance for most FIs and DNFBPs with the requirements of R.7.

Recommendation 7 is rated partially compliant.

Recommendation 8 – Non-Profit Organizations

South Africa was rated partially compliant with the former SR. VIII. The primary concerns were: there was no assessment of the potential TF risks posed within South Africa's NPO sector; no outreach program had been undertaken to protect the sector from TF abuse; registration of NPOs was only voluntary; the NPO Directorate had no power to sanction office bearers of defaulting NPOs or to impose fines or to freeze accounts of NPOs for violation of oversight measures; there was no prescribed retention period that applied to the record keeping requirement of NPOs; there was no specific requirement for NPOs to maintain for a period of five years information on the identity of person(s) who own, control or direct their activities, and there were no formal gateways for the Directorate to exchange non-public information. Since the third round the recommendation has changed significantly.

Criterion 8.1 – (Not Met):

a) *(Not Met)* South Africa has the Nonprofit Organization Act No. 71 of 1997 (NPO Act) that regulates NPOs in South Africa and defines an NPO as a trust, company or other association of persons that is established for a public purpose and whose income and property is not distributed to its members or officers. In March 2012, South Africa published a Strategic Risk assessment of its broader NPO sector outlining issues in respect of registration, outreach, supervision, and international cooperation. The risk assessment concluded with a list of policy recommendations to improve the countries oversight of its broader NPO sector. No information however was provided to the assessment team on any progress made against those recommendations. South Africa has also failed to demonstrate that any analysis of this broader NPO sector identified a subset of organizations that, based on their activities or characteristics, are likely to be at risk of TF abuse.

b) *(Partly Met)* South Africa indicates that no assessment has ever been undertaken to identify the nature of threats posed by terrorist entities to the NPOs which are at risk as well as how terrorist actors abuse those NPOs, however the March 2012 Strategic Risk Assessment does acknowledge some internationally recognized inherent risks of how terrorist entities in general can abuse the NPO sector.

c) *(Not Met)* Through the March 2012 Risk Assessment, South Africa did review its laws and regulations that relate to NPOs generally, however the strategy stopped short of identifying the subset of NPOs that may be abused for TF support and did not identify specific measures required to be able to take proportionate and effective actions to address TF risks. A similar review of the sector took place in 2019. However, it had the same shortcomings.

d) *(Partly Met)* South Africa publishes an Annual Report on the State of NPOs in South Africa, detailing their income and expenditures. South Africa failed to demonstrate that it has followed up on the policy recommendations stemming from the March 2012 Risk Assessment or periodically reassesses the sector by reviewing new information on the sector's potential vulnerabilities to terrorist activities. The Preliminary Findings document of the TF NRA, however, contains a detailed description of the vulnerabilities in South Africa's oversight of NPOs pertaining to the risk of TF abuse.

Criterion 8.2 – (Partly Met):

a) *(Partly Met)* The NPO Act has clear policies promoting accountability, integrity and public confidence in the administration and management of all NPOs in South Africa. Such measures include: the keeping of books and records in accordance with accounting principles; the annual reporting of its activities and financial statements in prescribed form; and, the right of public access to any document of a registered NPO that the registrar of NPOs collects. Given that the registration of NPOs in South Africa is voluntary, these policies would not necessarily apply to all NPOs relevant to R.8.

b) *(Partly Met)* The NPO Act, ch.2, outlines at a very high level the obligations of the organs of state to implement its policies and measures in a manner designed to promote, support and enhance the capacity of non-profit organizations to perform their functions. In July 2019, FIC and DSD began holding joint outreach sessions with NPOs to create awareness on the vulnerability of the sector on TF. However, no plans to educate the donor community to raise awareness of vulnerabilities faced by NPOs to TF abuse and TF risks were shared with assessors.

c) *(Not Met)* The NPO Act, ch.2, articulates the objective to encourage NPOs to maintain adequate standards of governance, transparency and accountability and to approve those standards and South Africa has indicated that the NPO Directorate periodically conducts workshops and outreach programs on how NPO boards should consider the processes they have in place and decide if there are sufficient controls and compliance mechanisms in place to comply with the intent of NPO Act as well as their own core values. As indicated in c.8.2(b), South Africa has begun holding outreach sessions with NPOs. It is unclear, however, if these sessions include discussions on developing and refining best practices to address TF risk and vulnerabilities.

d) *(Partly Met)* The constitution of all NPOs that intend to register must provide that the organization's financial transactions be conducted by means of a banking account (NPO Act, s.12.(2)(k)). Again, given that NPO registration in South Africa is voluntary, these policies would not necessarily apply to all NPOs relevant to R.8.

Criterion 8.3 – (*Not Met)* The Director of NPOs has authority to cause any document or a narrative, financial or other report that is submitted to the Director to be scrutinized, or, by means of a notice, require a registered NPO to submit any information or document reasonably required in order to

enable the director to determine whether the organization is complying with the material provisions of an organizations constitution or its obligations under the NPO Act (NPO Act, s.18(2)). South Africa however has failed to provide any information to suggest that it takes steps to promote effective supervision or monitoring such that South Africa is able to demonstrate that risk-based measures apply to NPOs at risk of TF abuse.

Criterion 8.4 – (Not Met):

a) *(Not Met)* All registered NPOs must file proscribed financial statements with the Director of NPOs (NPO Act, s.17). However, this obligation does not demonstrate that South Africa monitors the compliance of NPOs with the requirements of this Recommendation, including the risk-based measures being applied to them under c.8.3.

b) *(Not Met)* A person convicted of an offense **in** terms of the NPO Act is liable to a fine or to imprisonment or to both (NPO Act, s.30). The amount of the fine and the length of imprisonment are not however specified in the NPO Act and South Africa has failed to provide any further information with respect to sanctions for violations by NPOs or persons acting on their behalf.

Criterion 8.5 – (Not Met):

a) *(Met)* The NPO Directorate is responsible for liaising with other organs of state and interested parties (NPO Act, s.5). The Directorate, via the DSD, is a standing member of the IDC on AML/CFT. The Directorate has recently begun joint outreach sessions for NPOs with the FIC and has begun information exchanges with the FIC where they routinely send data to FIC for verification on directors of applicant NPOs. The NPO Directorate also chairs the newly formed NPOTT mandated to address R.8 and IO.10 core issue 10.2.

b) *(Not Met)* South Africa provided no information to show it complies with these criteria.

Criterion 8.6 – (*Not Met)* South Africa has not indicated that they have identified a point or points of contact nor developed procedures to respond to international requests for information regarding NPOs suspected of TF or involvement in other forms of terrorist support.

Weighting and Conclusion

South Africa has not yet done an assessment of their broader NPO sector to identify those organizations, based on their characteristics or activities, that put them at risk of TF abuse. South Africa also has no capacity to monitor or investigate NPOs identified to be at risk of TF abuse.

Recommendation 8 is rated non-compliant.

Recommendation 9 – Financial Institution Secrecy Laws

In its previous MER, South Africa was rated compliant with the former R.4.

Criterion 9.1 – *(Mostly Met)* According to the Protection of Personal Information Act (POPI Act) processing of personal information of clients of FIs may only be done within the confines of the POPI Act. The sharing of information between FIs where this is required by R.13, 16 or 17 is within the confines of the POPI Act if it is *"processing in order to comply with obligations imposed by law"* (s.11(1)(*c*)). Further processing of information by FIs carrying out its functions both in terms of the FIC Act and banking laws is explicitly allowed under the POPI Act (s.15(3)(*c*)(*ii*)). The authorities have not demonstrated the Regulations relating to Banks or FIC GNs are within the confines of this Act. Therefore, the POPI Act may form a legal obstacle for FIs to share information where this is required by mentioned Recommendations.

Competent authorities may process information if necessary for the proper performance of their public law duty, and therefore processing for the purposes of the FIC Act is allowed (ss. 11, 12, 15 and 18), including sharing of information with other competent authorities as the definition of 'processing' in the POPI Act is very broad to include sharing and having access to (s.1). The POPI Act explicitly includes the processing of information with foreign authorities under specific conditions not constituting unreasonable obstacles (s.72).

Weighting and Conclusion

Competent authorities can access information they require to properly perform their AML/CFT functions without the POPI Act being an obstacle. However, information sharing between FIs – where required by R.13, 16 or 17 – is only allowed under the POPI Act if it can be considered to be processing in order to comply with obligations imposed by law. This may cause a legal issue as essential AML/CFT and related obligations are imposed by secondary legislation (e.g. Regulations and Directives) and therefore not being within the confines of the POPI Act.

Recommendation 9 is rated largely compliant.

Overview of Preventive Measures

Requirements to implement preventive measures are primarily covered by the FIC Act, addressing *AIs*, which do not cover all FIs and DNFBPs (see c.1.6), and VASPs. This act implemented a RBA in 2017 to preventive measures, enforceable from April 2019. Furthermore, GN7 provides for guidance to AIs on implementation of the FIC Act. GN7 is enforceable means under the FATF Recommendations as it requires each AI to follow the guidance, or otherwise to be able to demonstrate that the AI achieves an equal level of compliance with the relevant provisions in the FIC Act. Furthermore, enforcement action may emanate for non-compliance with the FIC Act where it is found that an AI has not followed GN7. The guidance has been issued by the FIC, in collaboration with the NT, the SARB and the predecessor to the FSCA. The **Regulations relating to Banks** were issued by the Minister of Finance in 2012 and are enforceable (Banks Act, s.90). Particularly Regulation 36(17)(page 776) is of importance regarding CBRs, covering all *"banks and controlling companies in respect of a bank"*, as defined by the Banks Act (s.1).

The SARB issued EFT Directive 1, in 2015 for conduct within the NPS in respect of the FATF Recommendations and in 2017 published an Interpretation Note for EFT Directive 1. The Directive and its Interpretation Note (IN) are enforceable means in accordance with the FATF Methodology as they set out clearly stated requirements for R.16, which are sanctionable for non-compliance under the NPS Act.

Recommendation 10 – Customer Due Diligence

South Africa was rated partially compliant with the former R.5., based on shortcomings primarily regarding identification of beneficial owners and legal persons, ongoing due diligence, enhanced due diligence, and unjustified exemptions.

Due to incomplete scoping of FIs under the FIC Act, all R.10 criteria have a scope deficiency.

Criterion 10.1 – *(Mostly Met)* The FIC Act prohibits AIs to establish a business relationship or conclude a single transaction with an anonymous client or a client with an apparent false or fictitious name (s.20A), and existing accounts had to be reviewed in this respect at introduction of the provision in the FIC Act in 2001.

Criterion 10.2 – (Partly Met).

a) *(Mostly Met)* AIs must identify and verify the identity of the client, a representative of the client (if any), and of the beneficial owner when establishing a business relationship (FIC Act, s.21). Furthermore, AIs must obtain information on the nature and intended purpose of the relationship, and the source of funds the prospective client expects to use in concluding transactions (FIC Act, s.21A). In addition, GN7 includes the understanding of the risk profile of the prospective client (para. 123).

b) *(Mostly Met)* The measures to identify and verify the identity of the client, a representative of the client (if any), and of the beneficial owner are also required when entering into a single transaction (not less than R5,000; $340)(FIC Act, s.21). GN7 confirms that the full scope of CDD measures is to be performed in respect of clients conducting single transactions above the threshold (para. 81). However, the concept of a single transaction does not include situations where the transaction is carried out in several operations that appear to be linked (para. 79).

c) *(Mostly Met)* SARB's *EFT Directive 1* (s.3) and its IN (ss. 6.1.1.3, 6.1.2.1, and 6.3.1) confirm CDD measures required under the FIC Act must be undertaken when carrying out occasional transactions that are wire transfers under R.16.

d) *(Partly Met)* AIs must provide in their RMCP for the manner in which and the processes by which the institution will perform CDD requirements when, during the course of a business relationship, the institution suspects that a transaction or activity is suspicious or unusual (FIC Act, ss. 42, 21 – 21C). It's not clear if and how far such requirement directs AIs to

undertake CDD measures when there is a ML/TF suspicion regardless of any exemption or thresholds that are referred to elsewhere under the Recommendations.

e) *(Mostly Met)* When the AI has doubts about the veracity or adequacy of previously obtained customer information, it must repeat the steps taken to identify and to verify client's identity, its representative and beneficial owner (FIC Act, ss.21 and 21D).

Criterion 10.3 – *(Mostly Met)* AIs must identify the client - being a natural person or legal person, partnership, trust–or similar arrangement - when entering into a single transaction or establishing a business relationship, and to verify its identity (FIC Act, ss.21 and 21B). Reference to the use of reliable, independent source documents, data or information has been included in GN7. AIs should, as far as practicable, use government issued or controlled sources as the means of verification when verifying basic identity attributes. There's an exemption in the GN which is not compliant–with the criterion, as–- in exceptional cases - information could be used from sources other than the original source of the information and this should only be done in cases where AIs are confident that they can adequately manage ML/TF risks.

Criterion 10.4 – *(Mostly Met)* An AI must establish and verify the identity of the person representing the client, as well as that other person's authority to act on behalf of the client (FIC Act, s.21).

Criterion 10.5 – *(Partly Met)* "Beneficial owner", in respect of a legal person, means a natural person who, independently or together with another person, directly or indirectly owns the legal person or exercises effective control of the legal person (FIC Act, s.1). The definition of "beneficial owner" does not extend to the situation where the beneficial owner exercises effective control of the client who is a natural person. Section 21B deals with situations when a client is a legal person or a natural person acting on behalf of a partnership, trust, or similar arrangement between natural persons. The AI in such situations must identify the beneficial owners, natural persons controlling a partnership, and the beneficiaries of a trust or - if beneficiaries are not referred to by name in the trust deed or other founding instrument in terms of which the trust is created - the particulars of how the beneficiaries of the trust are determined. Furthermore, it must take reasonable steps to verify the identity of these persons, so that the AI is satisfied that it knows who these persons are.

Criterion 10.6 – *(Mostly Met)* AIs must obtain information to reasonably understand the nature of the business relationship concerned and the intended purpose of such (FIC Act, s.21A).

Criterion 10.7 – (Mostly Met)

a) *(Mostly Met)* - Ongoing due diligence needs to be conducted on the business relationship, including monitoring of transactions and source of funds to ensure that transactions are in line with the client's business and risk profile (FIC Act, s.21C). Source of funds is not defined but believed to include VAs.(e.g. GN7, para. 145).

b) *(Mostly Met)* CDD information obtained must be kept up to date (FIC Act, s.21C), while GN7 requires AIs to ensure that the information it has about a client is still accurate and relevant

(para. 127). This can only be reached by undertaking reviews of existing records, while ongoing due diligence is undertaken based on the client's ML/TF risk in accordance with its RMCP (FIC Act, s.42(*g*)).

Criterion 10.8 – *(Mostly Met)* The definition of "legal person" in the FIC Act means any person, other than a natural person, that establishes a business relationship or enters into a single transaction, with an AI and includes a person incorporated as a company, close corporation, foreign company or any other form of corporate arrangement or association, excludes a trust, partnership or sole proprietor. If a client contemplated in s.21 is a legal person or a natural person acting on behalf of a partnership, trust or similar arrangement between natural persons, an AI must, in addition to the steps required under ss.21 and 21A and in accordance with its RMCP establish: (a) the nature of the client's business; and (b) the ownership and control structure of the client (FIC Act, s.21B).

Criterion 10.9 – *(Mostly Met)* AIs must provide in their RMCP the way and the processes by which the AI conducts additional due diligence measures in respect of legal persons, trusts and partnerships (FIC Act, s.42(2)(f)). GN7 includes references to the collection of information regarding name, legal form and proof of existence of the legal person or arrangement; information regarding powers that regulate and bind the person or arrangement and names of senior managers, and its registered office's address or principal place of business.

Criterion 10.10 – *(Mostly Met)* Regarding c.10.5, the FIC Act refers to beneficial owners of a legal person, as those natural persons who, independently or together with another person, directly or indirectly owns the legal person; or exercises effective control of the legal person. AIs must establish the identity of the beneficial owners of the client (FIC Act, s.21B) by:

a) *(Mostly met)* determining the identity of each natural person who, independently or together with another person, has a controlling ownership interest in the legal person; or

b) *(Mostly met)* if in doubt whether such a natural person is the beneficial owner or no natural person has a controlling ownership interest in the legal person, by determining the identity of each natural person who exercises control through other means; or

c) *(Mostly met)* if such a natural person is not identified, by determining the identity of each natural person who exercises control over the management of the legal person, including in his or her capacity as executive officer, nonexecutive director, independent nonexecutive director, director or manager. No threshold is given regarding a 'controlling ownership interest'.

Criterion 10.11 – *(Partly Met)* The identity of the settlor, trustee(s), and beneficiaries or class of beneficiaries of trusts must be established, and reasonable steps must be taken to verify these identities (FIC Act, s.21B(4)). The protector (if any) is not mentioned, but the concept of a protector is foreign to South African trust law. The law doesn't contain a requirement to ensure that any other natural person exercising ultimate effective control over the trust (including through a chain of

control or ownership) must be identified and their identity verified. GN7 doesn't provide any further clarification either.

Criteria 10.12 and 10.13 – *(Not Met)* There are no additional CDD measures – in addition to the normal CDD measures – to be applied on the beneficiary of life insurance and other investment related insurance policies, nor with regard to the requirement to include such beneficiary as a relevant risk factor in determining whether enhanced measures are applicable.

Criterion 10.14 – *(Mostly Met)* AIs must in all circumstances refrain from establishing the business relationship or to conclude a single transaction with a client, if it's unable to establish or verify the identity of a client or the beneficial owner (FIC Act, s.21E).

Criterion 10.15 – *(NA)* See c.10.14. It's under no circumstance allowed for a customer to utilize the business relationship prior to verification.

Criterion 10.16 – *(Mostly Met)* South-Africa has chosen to implement a stricter requirement than the standard by requiring AIs to perform CDD not only on new (prospective) clients, but as well on all clients it engaged with before the FIC Act took effect (FIC Act, s.21(2).

Criteria 10.17 & 10.18 – *(Partly Met)* An AI must develop, maintain and implement a RMCP to assess, manage and mitigate its ML/TF risks, and in particular to provide for the manner in which and the processes by which EDD is conducted for higher risk business relationships and when simplified CDD might be permitted (s.42(2)(m). However, this requirement does not entail higher risk occasional transactions, and the application of simplified measures when there is a suspicion of ML/TF or specific higher risk scenarios apply, is not explicitly excluded. GN7 provides guidance for AIs in how to set up a risk assessment of their business, including a risk assessment of clients, and addressing resulting higher risks situations through EDD measures and lower risks through simplified measures. The guidance sufficiently includes relevant risk factors to be included in the risk assessment and promotes the use of a risk matrix.

Criterion 10.19 – *(Mostly Met)* AIs cannot establish the business relationship or conclude a transaction when they are not able to perform identification and verification measures (see c.10.14). The same is true regarding other CDD measures in the FIC Act, and existing business relationships with a client need to be terminated (FIC Act s.21E). In such cases, the institutions are explicitly required to consider filing a report to the FIC.

Criterion 10.20 – *(Not Met)* Neither the FIC Act nor GN7 contain a provision regulating the situation in which an AI is permitted not to pursue the CDD process, and instead be required to file a report to the FIC, when it forms a suspicion of ML/TF and it reasonably believes that performing the CDD process will tip-off the client. A requirement to file a report is included in the FIC Act when such suspicion is formed, but an AI should be explicitly permitted to stop performing ongoing due diligence measures it must perform under c.10.7.

Weighting and Conclusion

South Africa has to a large extent implemented CDD requirements in line with R.10. Shortcomings are particularly related to:

- the FIC Act not covering all FIs (see c.1.6);
- the definition of "beneficial owner" does not extend to the situation where the beneficial owner (a natural person) exercises effective control of the client who is a natural person;
- no requirement to ensure that any other natural person exercising ultimate effective control over a trust (including through a chain of control or ownership) must be identified and their identity verified;
- the absence of particular CDD requirements regarding the beneficiary of life insurance and other investment related insurance policies;
- the requirement to apply enhanced measures does not entail higher risk occasional transactions, and the application of simplified measures when there is a suspicion of ML/TF or specific higher risk scenarios apply, is not explicitly excluded;
- regulating the situation in which an AI is permitted not to pursue the CDD process, when it reasonably believes that performing the CDD process will tip-off the client.

Recommendation 10 is rated partially compliant.

Recommendation 11 – Record-Keeping

South Africa was rated partially compliant with the former R.10, based on shortcomings related to requirements to include the date of the transactions or address of the customer, and to maintain account files or business correspondence. Outside of the banking sector, there was no general obligation to keep transaction records sufficient to permit the reconstruction of account activity. Furthermore, effective application of the record keeping obligations was eroded by some exemptions, while uncovered FIs were not subject to the record keeping obligations. All – except for the last finding – were found to be addressed by South Africa (FATF 14th FUR, November 2017).

Due to incomplete scoping of FIs under the FIC Act, all R.11 criteria have a scope deficiency.

Criterion 11.1 – *(Mostly Met)* All necessary records of every transaction must be maintained by AIs for at least five years following conclusion of the transaction (FIC Act, ss.22A and 23).

Criterion 11.2 – *(Mostly Met)* Records relating to the establishment of a business relationship with a client or prospective client[12] and all information collected through all applicable CDD measures must be kept for at least five years from the date on which the business relationship is terminated (FIC

[12] A client is *'a person who has entered into a business relationship or a single transaction with an AI'* (FIC Act, s.1).

Act, s.23). South Africa has not demonstrated that this set of information covers analysis undertaken during CDD.

Criterion 11.3 – *(Mostly Met)* The FIC Act, s.22A(2), lists all relevant aspects of a transaction to be recorded: amount and currency involved, conclusion date of the transaction, parties and nature of the transaction, and business correspondence. Transaction records must be sufficient to enable the transaction to be reconstructed (GN7,para.167).

Criterion 11.4 – *(Mostly Met)* AIs must ensure that the records be readily available to the FIC and the relevant supervisory authorities when required (GN7, para. 170). There is however no explicit requirement for the records to be readily available to law enforcement agencies. Law enforcement agencies can access the records of an AI using coercive measures (e.g., subpoena under the CPA, s.205).

Weighting and Conclusion

South Africa's legal framework provides for all criterion under R.11. However, there is a minor deficiency due to the requirements not applying to all FIs (see c.1.6).

Recommendation 11 is rated largely compliant.

Recommendation 12 – Politically Exposed Persons

South Africa was rated non-compliant with the former R.6 because there was no enforceable obligation for AIs to identify PEPs or take other such as measures as indicated in former R. 6.

Due to incomplete scoping of FIs under the FIC Act, all R.12 criteria have a scope deficiency.

Criterion 12.1 – *(Partly Met)* The definition of foreign prominent public official (FIC Act, sch.3B) is limited to "*an individual who holds, or has held at any time in the preceding 12 months…"*, hence excludes officials who held such functions only in the period prior to this. This is contrary to R.12 and the definition of foreign PEP in the Glossary. AIs must include in their RMCP rules a process to identify whether a prospective client or the beneficial owner is a foreign PEP (FIC Act, s.21F). Consequently, senior management approval is required before establishing a business relationship, and reasonable measures are to be taken to establish the source of wealth and the source of funds, and to conduct enhanced ongoing due diligence on the relationship. However, there's no requirement to include in their RMCP a process to identify existing customers becoming a PEP, and to consequently obtain senior approval for continuing the relationship with such existing customers of the institution when it becomes clear they're foreign PEPs. GN7 only advises AIs "*to bear in mind that although a client might not initially (at the commencement of the business relationship) meet the definition of a prominent person (or immediate family member or known close associate), this position might change over time.*" (para. 159).

Criterion 12.2 – *(Partly Met)* The definition of a 'domestic prominent influential person' used includes a broad range of prominent public functions (sch.3A),applying a limited definition of senior

politician.[13] The second part of the definition consists of board members of companies delivering goods, services, or both to an organ of state, above a certain annual transaction value as determined by government. Thirdly, heads or other executives directly accountable to that head of an international organization based in South Africa. The third part of the definition is more limited than the FATF definition requires, as the latter doesn't exclude the international organization to be based in the country itself but extends to all international organizations wherever based. For domestic prominent influential persons, there are also limitations of time: *"in an acting position for a period exceeding six months or has held at any time in the preceding twelve months"*. If an AI determines that a prospective client (or its beneficial owner) is a domestic prominent influential person and that the prospective business relationship needs to be regarded as a higher risk, following its RMCP, the institution must apply the same measures as for foreign PEPs (s. 21G). Like under c.12.1, there is no provision dealing with the situation in which an existing client turns out to be a domestic PEP.

Criterion 12.3 – *(Partly Met)* The requirements for foreign and domestic PEPs apply to immediate family members and known close associates of such persons, under the same limitations of time and scope (s. 21H).

Criterion 12.4 – *(Not Met)* No specific requirements, other than those mentioned under 12.1 to 12.3, have been included regarding PEP beneficiaries of life insurance policies.

Weighting and Conclusion

Major shortcomings are found in South Africa's implementation of R.12, where it concerns the definition of a PEP and regarding dealing with existing customers becoming a PEP. The definition of a PEP is limited in time and the inclusion of persons with functions in international organizations is limited to organizations based in South Africa. These limitations apply to family members and close associates of all types of PEPs. These limitations strongly undermine South Africa's legal framework to mitigate ML/TF risks related to persons holding public functions. In addition, the lack of clear requirements for AIs to include in their RMCP a process to identify existing customers becoming a PEP, and to subsequently obtain senior approval for continuing the relationship with such customers when it becomes clear they're PEPs, weakens the South African AML/CFT system to an important extent. In addition, the requirements are not applied to all FIs (see c.1.6).

Recommendation 12 is rated non-compliant.

Recommendation 13 – Correspondent Banking

[13] Included are: (Deputy) President of the Republic; government (deputy) minister; Premier of a province; member of the Executive Council of a province; executive mayor of a municipality; leader of a political party (see as well GN7, para. 147); member of a royal family or senior traditional leader; head, accounting officer or CFO of a national or provincial department or government component; municipal manager or municipal CFO; chairperson of the controlling body, CEO, accounting authority, CFO, CIO of a public entity; chairperson of the controlling body, CEO, CFO, CIO of a municipal entity; constitutional court judge and other judges as defined; an ambassador or high commissioner or other senior representative of a foreign government based in South Africa; and, military officials above a certain rank.

South Africa was rated non-compliant with the former R.7. There was no specific obligation in law or regulation for AIs to conduct enhanced due diligence on CBRs.

Due to incomplete scoping of FIs under the FIC Act, all R.13 criteria have a scope deficiency.

Criterion 13.1 – *(Mostly Met)* Regulation 36(17)(b)(iii) of the Regulations relating to Banks (page 776) which are the only South African FIs that can have correspondent relationships requires enhanced measures to be implemented for CBRs, including:

a) ***and (b)*** *(Mostly met)* the collection of sufficient information to understand a respondent's business, to determine its reputation, and quality of supervision and its AML/CFT controls;

b) *(Mostly met)* senior management's approval needs to be obtained before establishing new CBRs;

c) *(Partly met)* documenting the respective responsibilities of each institution, which is less strict than the criterion demanding to clearly understand the AML/CFT responsibilities of each institution.

Criterion 13.2 – *(Met)* With respect to any payable-through accounts a bank needs to be satisfied that the respondent has duly verified the identity of, and performed ongoing due diligence on any customer that has direct access to accounts of the correspondent, and that it is able to provide relevant customer identification data upon request by the correspondent (Regulation 36(17)(b)(iii)(F) of the Regulations relating to Banks).

Criterion 13.3 – *(Met)* Banks must not enter into or continue a CBR with a shell bank located in a foreign jurisdiction (Regulations relating to Banks, Reg.36(17)(b)(i)(C)). Furthermore, banks must ensure that each respondent institution does not permit its accounts to be used by a shell bank (Reg. 36(17)(b)(iii)(B)). A shell bank is defined in the Regulations as being a bank without physical presence in the country in which it is authorized to conduct banking business, and not being subject to adequate supervision.

Weighting and Conclusion

Most requirements exist; scope limitations.

Recommendation 13 is rated largely compliant.

Recommendation 14 – Money or Value Transfer Services

South Africa was rated as partially compliant under former Special R.VI as it was found that those MVTS entities conducting operations within South Africa (i.e. domestic activity) did not have to be licensed or registered. MVTS were not subject to all applicable FATF Recommendations and the system in place to monitor and ensure compliance for banks was inadequate. Sanctions applicable to MVTS operators if they failed to adequately comply with the provisions of the FIC Act were not

effective, proportionate, or dissuasive. Finally, South Africa was found to not have taken steps to address the informal sector.

Criterion 14.1 *– (Mostly Met)* The following are authorized to engage in MVTS businesses in foreign currencies (i.e., remit cross border):

- Banks and mutual banks that are Authorized Dealers (ADs);
- Postbank is authorized to carry out banking businesses including transfers under the South African Postbank Limited Act 2010, ss. 2 and 4. In 2013, the SARB:FinSurv authorized the SAPO to perform person to person outward international money transfers not exceeding R5,000 ($340) per applicant per month within an overall limit of R60,000 ($4,080) per year. There is no limit on inward transfers.
- ADLAs authorized to deal in foreign exchange, including remittance, for the sole purpose of facilitating travel related transactions (ECR, Reg.3(1) and (2)).
- In practice, the authorization of ADs and ADLAs is conducted by the SARB:FinSurv.
- No registration or licensing requirements apply to any persons who conduct purely domestic money or value transfer business except banks.

Criterion 14.2 *(Partly Met)* Any person who breaches the ECR commits a criminal offense and may be liable, on conviction, to a fine of the value of foreign currency involved or R250,000 ($17,000), whichever sum is greater, or to imprisonment for a period up to five years or both (ECR, Reg.22). The authorities recognize there are active informal networks of MVTSs operating in the country. When the SARB:FinSurv receives information on unauthorized activity involving foreign exchange only, it will follow up and reports incidents to the relevant law enforcement agencies. However, the authorities have not demonstrated that any of these actions have resulted in proportionate and dissuasive sanctions being imposed.

Criterion 14.3 *(Met)* Banks and mutual banks are subject to AML/CFT supervision by the SARB:PA (see R.26). ADLAs are subject to the SARB:FinSurv's monitoring of compliance with the AML/CFT requirements in the FIC Act (FIC Act, s.45, sch.2, para.2).[14] MVTSs providing pure domestic services, though not subject to licensing or registration, are subject to AML/CFT requirements and monitoring of compliance by the FIC (FIC Act, s. 4(g), Sch 1, para. 19), as is Postbank.

Criterion 14.4 *– (Partly Met)* Banks that are ADs are not required to maintain a list of agents. There are also no requirements for these agents to be licensed or registered. ADLAs may also operate through agents for cross-border transfers but only if the SARB:FinSurv approves them through the formal channels (ADLA Manual, s B.2(B)). The SARB:FinSurv maintains a list of all agents of ADLAs. These do not extend to domestic MVTS.

[14] www.fic.gov.za/Documents/K-14619%20FIC%20AR%202017-2018_Web.pdf

Criterion 14.5 – (*Partly Met)* It is a precondition for authorization of agents that ADLAs must provide a description of the internal controls mechanisms that will be used by the agent in order for them to be compliant with the FIC Act (ADLA Manual, s. B.2 (B)(i)(b)). Banks have partnered with ADLAs (Category III and IV) and both sides conduct due diligence on the other before entering into the business contract. neither banks that are ADs nor ADLAs must include agents in their AML/CFT program.

Weighting and Conclusion

Businesses that engage in travel related transactions in foreign exchange including transfers must be licensed or registered. Domestic MVTS are not subject to licensing or registration. The authorities have not demonstrated that they have taken actions against unlicensed MVTS, which is an important gap considering the significant informal sector in South Africa. There are limited circumstances where agents are registered and MVTS need not include agents in their AML/CFT program.

Recommendation 14 is rated partially compliant.

Recommendation 15 – New Technologies

South Africa was rated partially compliant with the former R.8. There were no specific legal or regulatory requirements for AIs to have policies in place to address the potential abuse of new technological developments for ML/FT. However, some guidance was given (mainly) regarding identification and verification issues related to non-face-to-face business and cell-phone banking products.

The new R.15 focuses on assessing risks related to the use of new technologies, in general, and imposes a comprehensive set of requirements in relation to virtual asset service providers (VASPs). The FATF revised R.15 in October 2018 and its interpretive note in June 2019 to require countries to apply preventive and other measures to virtual assets and VASPs. In October 2019 (just before the assessment team's onsite to South Africa), FATF agreed the corresponding revisions to its assessment Methodology and began assessing countries for compliance with these requirements immediately.

Criterion 15.1 – *(Partly Met)* Different initiatives regarding financial sector trends and risks for new technologies are employed by the authorities, predominantly in FinTech. However, these initiatives fail to sufficiently identify and assess ML/TF risks and focus on general aspects related to policy and regulatory implications, financial inclusion, financial market stability, efficient functioning of financial markets, and protecting the rights and interests of consumers. The SARB:PA considers the types of products offered by institutions and feeds this into the risk-based tool that the AML/CFT team uses but has to update the tool to catch up with new products and services developed since 2016.

Regarding AIs, GN7 mentions the risk indicators that need to be considered when assessing ML/TF risks. AIs should satisfy themselves that their ML/FT risk management systems and controls remain adequate in view of changing circumstances relating to *inter alia* emerging threats and

vulnerabilities, product innovations, and new target markets. Risk factors related to the type of clients, products and services, delivery channels, et cetera should be considered. Institutions may, but are not required to, have a new product approval process in place, whereby relevant risk considerations are required (para. 38).

Criterion 15.2 – *(Partly Met)* There's no specific provision requiring AIs to undertake ML/TF risk assessments prior to the launch or use of new products, business practices and technologies, and to take appropriate measures to manage and mitigate the risks. In more general wording the FIC Act, s.42, requires the RMCP of AIs to identify, assess, monitor, mitigate and manage the potential risk that the provision of products or services offered may involve or facilitate ML activities or TF, and related activities.

Virtual Assets and Virtual Asset Service Providers

Criterion 15.3 – *(Not Met)* South Africa cannot show it has identified and assessed the ML and TF risks emerging from VA activities (crypto asset activities) and the activities or operations of VASPs (CASPs) and has taken measures to mitigate such risks. However, it does have a certain appreciation of the risks of the VASP sector, based on a mapping exercise of the current landscape of VASPs in South Africa, and the voluntarily involvement of the major market participants under the AML/CFT regime. Furthermore, attention is given to VASPs in the ML NRA as far as they constitute threats in the banking sector. As of the onsite, VASPs were not subject to the AML/CFT regime (beyond the reporting obligation, see c.15.8) and therefore, had no obligations to identify, assess, manage, and mitigate their ML and TF risks. Certain VASPs mitigate some of their ML/TF risks by voluntarily applying the principles of the FIC Act to their client base.

Criterion 15.4 – ***15.6*** *(Not Met)* There are no requirements for VASPs to be licensed or registered and they are not subject to AML/CFT supervision.

Criterion 15.7 *(Not Met)* While VASPs have a general obligation to report (see c.15.8), the general reporting guidelines may assist the VASPs to a certain extent, but no reporting guidelines dedicated to their obligation have been issued. The FIC has visited one VASP with to raise general awareness of the FIC Act and to update the entity of its future regulatory obligations if it becomes an AI.

Criterion 15.8 – *(Partly Met)* VASPs are subject to the same general obligation to report suspicious and unusual transactions to the FIC (FIC Act, s.29 – see R.20) and the same sanctions for failure to report or for tipping off as other businesses (see R.35).

Criterion 15.9 *(Not Met)* VASPs are only required to apply the reporting (see R.20) and tipping-off provisions (see R.21), as mentioned above.

Criterion 15.10 – *(Partly Met)* VASPs are subject to the same TF and PF TFS obligations as any other person (see R.6 and R.7 and specifically cc.6.5(d), 6.5(e), 6.6(g), 7.2(d), 7.2(e), and 7.4(d)). VASPs can be subject to sanctions for failure to comply with PF TFS obligations (see c.7.3) but there are no measures in place yet for monitoring and ensuring compliance.

Criterion 15.11 – *(Partly Met)* There is no bar providing MLA (including for freezing and confiscation), extradition, or international cooperation related ML, predicate offenses, and TF involving VAs. However, no supervisory authority for VASPs exists to exchange information with foreign counterparts.

Weighting and Conclusion

ML/TF risks relating to new technologies are identified only to a limited extent, as initiatives focus on general policy aspects and regulatory implications, financial inclusion, financial market stability, efficient functioning of financial markets, and protecting the rights and interests of consumers. There's no specific provision requiring AIs to undertake ML/TF risk assessments prior to the launch or use of new products, business practices and technologies, and to take appropriate measures to manage and mitigate the risks. Regarding VAs and VASPs South Africa has taken its first steps in setting up a risk mapping exercise, but is not adequately identifying, assessing, and understanding risks yet. Therefore, no risk-based measures are taken, VASPs are not required to take AML/CFT measures beyond the reporting obligation (which is addressed to all businesses), and are not subject to licensing or registration, nor supervised. These are major deficiencies.

Recommendation 15 is rated non-compliant.

Recommendation 16 – Wire Transfers

South Africa was rated partially compliant with the former SR.VII, as there were *inter alia* no legal requirements for all wire transfers to be accompanied by full originator information, to ensure intermediary FIs to transmit all originator information with the transfer, and to ensure beneficiary FIs to consider restricting or terminating the business relationship with FIs that fail to meet the wire transfer requirements. South Africa addressed (most of) these deficiencies by issuing the SARB *EFT Directive 1* and its IN.

Criterion 16.1 – *(Met)* All banks and clearing system participants must ensure that any wire transfers - commonly known as EFT in South Africa - meet the requirements of R.16 (*EFT Directive 1*, cl. 1.3.4). An ADLA can only effect EFTs via a bank; thus, all EFTs are processed by banks. The IN explicitly points out the required information to be present, in line with c.16.1. FIs must include a unique transaction reference number in the EFT which would permit traceability of the transaction if there is no account number (IN, para. 6.1).

Criterion 16.2 – *(Mostly Met)* Batched cross border transitions must include the originator's account number or a unique reference number to remain with the EFT transfer through the payments chain, provided the batch file containing all the required originator and beneficiary information is traceable and made available upon request (IN, para. 5.4.4). However, there's no requirement, such as to verify the information, to ensure that it is accurate.

Criteria 16.3 & 16.4 – *(NA)* In South Africa there is no *de minimus* threshold for cross-border EFTs. All cross-border EFTs are regarded as qualifying EFT transactions, and all required originator and beneficiary information must be present in the message (IN, para. 5.4.2).

Criterion 16.5 – *(Met)* It's generally required that for all EFT transactions the required information must be present. This includes domestic MVTS as the Directive covers non-banks participating in the EFT environment (1.3.7).

Criterion 16.6 – *(Met)* If required information cannot be included in a domestic EFT, this information should be maintained and made available to the beneficiary FI and appropriate authorities by other means within three business days of receiving a request (IN, par 5.3). The ordering FI must include the number of the account from which the transaction is funded or a unique transaction reference number in the message, provided that this number will permit the transaction to be traced back to the originator or the beneficiary. Law enforcement should be able to compel immediate production for such information.

Criterion 16.7 – *(Partly Met)* An ordering FI is an AI and must adhere to the record keeping requirements in the FIC Act, s.22-23, and therefore must record all information necessary to reconstruct a transaction, and in particular information on the parties of the transaction. This is too broad to include the specific originator information as included under c.16.1(a)(iii); in particular the address or national identity number or date and place of birth.

Criterion 16.8 – *(Met)* For all EFTs the ordering FI must not execute any transaction which lacks required and accurate originator and required beneficiary information (IN, 6.1.3.1).

Criterion 16.9 – *(Met)* For cross-border EFTs, FIs that process an intermediary element of such chains of an EFT should ensure that all originator and beneficiary information that accompanies the EFT is retained with it (para. 6.2.1).

Criterion 16.10 – *(Partly Met)* An intermediary FI must maintain all transaction related information for at least five years (FIC Act, ss.22-23). However, the requirement is too broadly formulated to include the specific originator (who may not be its customer and not subject to its CDD measures) information (see c.16.7),

Criterion 16.11 – *(Met)* Intermediary FIs are must take reasonable measures to identify cross-border EFTs that lack required originator information or required beneficiary information (IN, para. 6.2).

Criterion 16.12 – *(Met)* An intermediary FI must use its discretion to determine when to execute, reject or suspend an EFT lacking required information, and take appropriate follow-up action (IN, para. 6.2.3). Any bank or clearing system participant that facilitates or originates EFTs resulting in funds flowing from one person or institution to another, must ensure that the requirements of the Recommendation are implemented and maintained (*EFT Directive 1*, para. 1.3.4).

Criterion 16.13 – *(Met)* Beneficiary FIs must take reasonable measures to identify cross-border EFTs that lack required information on originator or beneficiary (IN, para. 6.3.3).

Criterion 16.14 – *(Met)* All cross-border EFTs are regarded as qualifying EFTs, and all the required information must be present and verified. Beneficiary FIs must conduct CDD as provided for in the FIC Act in respect of its customer (the beneficiary)(IN, 6.3). Such information needs to be recorded and retained in accordance with the FIC Act.

Criterion 16.15 – *(Met)* The beneficiary FI must use its discretion based on its risk-based policies and procedures to determine when to execute, reject or suspend an EFT lacking required originator or beneficiary information, and appropriate follow-up action (IN, 6.3.4).

Criterion 16.16 – *(Not Met)* With reference to R.14, R26, and c.16.1, the *EFT Directive 1* is applicable to FIs participating in the EFT environment (IN, para. 4.1.1) including the MVTS providers as referred to under c.14.1. They therefore must comply with all relevant requirements as addressed under cc. 16.1 – 16.15. It was not established that these FIs must apply these requirements in whatever country they operate, directly or through their agents.

Criterion 16.17 – *(Not Met)* South Africa has not shown it has implemented the requirements included under c.16.17, particularly the requirement to file an STR in any country affected.

Criterion 16.18 – *(Partly Met)* There are two limitations to the screening of wire transfers, contrary to this criterion. First, beneficiary FIs are explicitly excluded from the requirement to screen incoming EFTs and the originator of these transactions against sanctions lists (IN, 6.3.5). Secondly, according to the IN (6.2.1 b. and c.) the intermediary FI is only required to screen cross-border EFTs. Screening of domestic EFTs against UN sanction lists is explicitly excluded, but the intermediary IN here has a duty to satisfy itself that the originator FI has appropriate controls in place to perform such screening. The originating FI must screen both originator and beneficiary.

Weighting and Conclusion

South Africa has overall a largely sufficient legal structure to implement R.16. Shortcomings concern the requirement to verify originator information with regard to batched wire transfers, record keeping obligations potentially being too broad to include specific originator information, absence of a clear specific obligation requiring AIs to have a RMCP such that they know when to execute, reject or suspend an EFT lacking required information, and to take appropriate follow-up action, and limitations to the screening of wire transfers to comply with international sanctions (while individual FIs in the chain of processing transfers are obliged to screen their respective clients).

Recommendation 16 is rated largely compliant.

Recommendation 17 – Reliance on Third Parties

South Africa was rated non-compliant with the former R.9, based on the absence of requirements for the institution relying on third-party verification/identification to immediately obtain the relevant CDD information; to satisfy itself that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the other institution "without delay"; to explicitly satisfy itself of the adequacy of applicable AML/CFT measures applicable to the foreign FI;

too broad exemptions from verification requirements regarding customers from FATF membership countries, and uncovered FIs not being subject to the CDD obligations of the FIC Act.

Due to incomplete scoping of FIs under the FIC Act, all R.17 criteria have a scope deficiency.

Criterion 17.1 – *(Partly Met)* The FIC Act does not prohibit institutions from relying on third parties to perform CDD, and AIs must include such reliance in their RMCPs (FIC Act, s.42(2)(d)). The *Public Compliance Communication No. 12 (Pcc12) Outsourcing of Compliance Activities to Third Parties*, which is enforceable, indicates that AIs remain responsible for compliance with their obligations in terms of the FIC Act regardless of their internal arrangements relating to how those obligations are met. However, there are no explicit requirements for the AI relying on a third party to obtain immediately information concerning outsourced CDD measures, to satisfy itself that copies of relevant data will be made available upon request, and to satisfy itself that the third party is regulated, supervised and has measures in place for compliance with CDD and record keeping requirements.

Criterion 17.2 – *(Partly Met)* South Africa provides general information to AIs on considerations on (the level of) country risk as periodically advised by the FATF. This doesn't particularly refer to the determination in which countries the third party that meets the conditions to rely on for CDD measures, can be based.

Criterion 17.3 – *(NA)* No use has been made of the consideration for countries to include requirements for FIs that rely on a third party that is part of the same financial group.

Weighting and Conclusion

Major shortcomings are identified, particularly where there are no explicit requirements instructing the AI relying on a third party to obtain immediately the necessary information concerning outsourced CDD measures, to satisfy itself that copies of relevant data will be made available upon request, to satisfy itself that the third party is regulated, supervised and has measures in place for compliance with CDD and record keeping requirements. Furthermore, no reference is made to determining in which countries the third party can be based, considering information available on the level of country risk, beside more general reference to public warnings on FATF's call for countermeasures against countries with strategic deficiencies.

Recommendation 17 is rated non-compliant.

Recommendation 18 – Internal Controls and Foreign Branches and Subsidiaries

South Africa was rated partially compliant with the former R.15 and non-compliant with former R.22 as there were no requirements to have a compliance officer or independent audit function for FIs other than banks. There were also no requirements for FIs to put have screening procedures when hiring staff nor to conduct ongoing training. For former R.22, there was no direct requirement to ensure that foreign branches and subsidiaries observe AML/CFT measures consistent with home country requirements and the FATF Recommendations to the extent that the host country's laws and

regulations permit. Nor was there a requirement to apply the higher of the requirements if South African and host country requirements differ.

Due to incomplete scoping of FIs under the FIC Act, all R.18 criteria have a scope deficiency.

Criterion 18.1 *(Mostly Met)* –AIs must develop, document, maintain and implement a RMCP, commensurate with the size and complexity of the institution and the nature of its business (FIC Act., s.42).

a) *(Mostly met)* AIs must include compliance management arrangements and must have a compliance function and assign a person with sufficient competence and seniority to ensure the function's effectiveness (FIC Act, s.42A, and GN7).

b) *(Not met) No* procedures regarding screening of employees are included in the FIC Act, or the GN.

c) *(Mostly met)* The FIC Act, s.42A, and the GN7 provide for the appropriate ongoing training of employees.

d) *(Mostly met)* Although an independent audit function is not explicitly mentioned in the FIC Act or the GNs, specific and comprehensive requirements for internal audit are to be found in some of the sector legislation covering core FIs.[15] Similar general requirements to establish an audit function apply to FSPs,(Financial Advisory and Intermediary Services (FAIS) Act, s. 19), and long-term life insurers must appoint auditors who submit an annual audit report to the FSCA, including a report on AML/CFT compliance (Insurance Act, s.32). Non-core FIs are not required to have an independent audit function.

Criterion 18.2 – *(Not Met)* AIs operating in groups of companies may implement group-wide RMCPs, while ensuring the elements of those RMCPs are appropriate for the different entities within the group and adequately tailored where needed (GN7). There is no requirement in the FIC Act or in the GN for financial groups to implement group-wide programs including the measures set out in c.18.1 and 18.2.(a)-(c).

Criterion 18.3 – *(Partly Met)* AIs situated in South Africa and operating in foreign jurisdictions should also be aware of local AML/CFT obligations in all jurisdictions where they operate (GN7, page 64). This should be reflected in the AI's RMCP, and procedures should be in place to meet local AML/CFT obligations in each jurisdiction where an AI operates. If there are conflicts between South African and local AML/CFT requirements and meeting local requirements would result in a lower standard than in South Africa the AI must implement measures which meet the South African

[15] For example, banks "shall establish an independent and objective internal audit function that … establishes and maintains… appropriate methods in order to monitor the bank's compliance with laws, regulations, and supervisory and internal policies" (Regulations Relating to Banks, Reg 48).

requirements. No reference has been made to the situation in which the host country doesn't permit the proper implementation of AML/CFT measures consistent with the home country requirements.

Furthermore, every relevant foreign branch, subsidiary or operation of a bank or controlling company must implement and apply: a) AML/CFT measures consistent with the relevant FATF Recommendations issued from time to time; and b) the higher of AML/CFT standards issued in the Republic of South Africa or the relevant host country (Regulations relating to Banks Reg. 36(17)(b)(ii)).

Weighting and Conclusion

Important elements of this Recommendation are in place – compliance management arrangements; ongoing training of employees; independent audit functions for core FIs; and ensuring application of appropriate AML/CFT requirements by foreign branches and subsidiaries – but other elements are not. The following major to moderate shortcomings exist: no requirement for financial groups to implement group-wide programs; procedures to screen staff are not required; non-core FIs are not required to have an independent audit function, and additional mitigating measures where the host country does not permit proper implementation are not required. In addition, the requirements are not applied to all FIs (see c.1.6).

Recommendation 18 is rated partially compliant.

Recommendation 19 – Higher-Risk Countries

South Africa was rated non-compliant with the former R.21, based on the absence of a specific requirement for FIs to give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations, while efforts to inform the financial sector about the risks of certain jurisdictions were directed only to banks, and there were no requirements to apply counter-measures in situations where countries do not sufficiently apply the FATF Recommendations.

Due to incomplete scoping of FIs under the FIC Act, all R.19 criteria have a scope deficiency.

Criterion 19.1 – *(Mostly Met)* The RMCP must provide for the manner and the process by which enhanced due diligence is conducted for higher risk business relationships (s.42(2)(m)), while geographic location such as a high-risk jurisdiction must be an indicator when considering such higher risk business relationships. Reference is made to international body, a domestic regulator, supervisory body, or other credible source expressing their concern in relation to a geographic location (GN7, p. 18).

Criterion 19.2 – *(Mostly Met)* The FIC and supervisory bodies may issue directives to AIs which reasonably may be required to give effect to the FIC's objectives (FIC Act, s.43A). The power is broad and would include instances to apply countermeasures proportionate to the risks when called upon to do so by the FATF and independently of any call by FATF to do so.

Criterion 19.3 – *(Mostly Met)* The FIC regularly publishes on its website advisories following FATF plenary meetings.

Weighting and Conclusion

All the requirements are in place, but there is a minor deficiency as they do not apply to all FIs (see c.1.6).

Recommendation 19 is rated largely compliant.

Recommendation 20 – Reporting of Suspicious Transaction

South Africa was rated largely compliant with the former R.13 and SR.IV in the last MER. The system fell short in that leasing and financing companies had not yet implemented the reporting obligations.

Criterion 20.1 – *(Partly Met)* The requirement to report a suspicious or unusual transaction - as– defined by this criterion - to the FIC is addressed to a very wide category of persons and institutions, including any person who carries on a business; is in charge of a business; manages a business; or is employed by a business" (FIC Act, s.29). The term "business" is not defined in the FIC Act. The ordinary meaning of the term, within the context of the FIC Act, is that of a commercial activity or institution, as opposed to a charitable undertaking or public sector institution. This means that any person associated with a commercial undertaking as an owner, manager or employee of that undertaking, is subject to the obligation to report suspicious or unusual transactions and activities to the FIC, including AIs and RIs as listed in the FIC Act, Schs. 1 and 3, respectively. See also GN4B on Reporting of Suspicious and Unusual Transactions and Activities.

For the period it may take to report, the FIC Act includes a reference to 'the prescribed period after the knowledge was acquired or the suspicion arose' (s. 29(1)). The prescribed period is "as soon as possible but not later than fifteen days after a natural person or any of his or her employees, or any of the employees or officers of a legal person or other entity, has become aware of a fact concerning a transaction on the basis of which knowledge or a suspicion concerning the transaction must be reported." (FIC Act, Reg. 24(3)). The wording used in Reg. 24(3) creates an ambiguity that could undermine the requirement to report as soon as possible when a suspicion is formed, where emphasis could be placed on the 15 business days period as an absolute term instead of on the promptness of the reporting requirement.

Criterion 20.2 – *(Met)* The FIC Act, s.29(1) includes attempted transactions, and no thresholds. are in use.

Weighting and Conclusion

The scope of who must report is formulated very broadly in the FIC Act, covering all FIs and going beyond the mere concept of the entity or institution itself, and the primary obligation is for FIs to make a suspicious report as soon as possible with an outer limit of 15 business days after a

suspicion is formed. However, South Africa's legislation is not sufficiently clear on that point, which creates a minor deficiency.

Recommendation 20 is rated largely compliant.

Recommendation 21 – Tipping-Off and Confidentiality

South Africa was rated compliant with the former R.14.

Criterion 21.1 – *(met)* the FIC Act protects AIs, RIs, and their directors, officers and employees from criminal and civil liability when reporting suspicions in good faith to the FIU in accordance with this Act (s. 38).

Criterion 21.2 – *(Met)* Tipping-off is prohibited (FIC Act, s. 29(3) and (4)). These provisions are not intended to inhibit information sharing under R.18.

Weighting and Conclusion

Recommendation 21 is rated compliant.

Recommendation 22 – DNFBPs: Customer Due Diligence

South Africa was rated non-compliant with the former R.12, as deficiencies identified in former R.5, 6, and 8-11 that applied to FIs also applied to all DNFBPs, and scope issues further reduce the application of the requirements of former R.5 and R.8-11. Casinos were permitted to apply reduced CDD in all cases, not based on demonstrated low risk. Attorneys were exempted from all CDD requirements and many record keeping requirements. The full range of preventative measures as required by R.9 did not apply to non-face-to-face transactions in the real estate sector, and only very limited information on transactions was recorded.

DPMS (other than KRDs covered as RIs), accountants (for activities beyond providing financial services), and CSPs other than attorneys[16] are not covered by the FIC Act.[17]

Criterion 22.1 – *(Partly Met)* The FIC Act, sch.1, lists the following institutions as AIs, which must comply with the CDD requirements as described under R.10:

- *Casinos* - businesses of making available a gambling activity, including casinos without any threshold (National Gambling Act, 2004 (Act 7 of 2004), s.3);

[16] CSPs not being attorneys are not covered; so, this counts for all CSP related activities performed not by an attorney.

[17] A proposed amendment is said to include these services or activities. In addition, the FIC Act is proposed to be amended to include dealers in goods above the value of R100 000 ($6 800), but no timelines for implementation are available.

- *Real estate agents* – when involved in transactions for a client buying and selling of real estate (Estate Agency Affairs Act, 1976 (Act No. 112 of 1976));

- *Lawyers, notaries etc*. –practitioners, including attorneys, notaries (being specialist attorneys) and independent legal professionals (Legal Practice Act, 2014 (LPA), ss. 1, 24 and 30, replacing the Attorneys Act[18]) and may be in a position to carry out any of the listed activities.

- *Trust service providers* –any person that …as a business… invests, keeps in safe custody, controls, or administers trust property within the meaning of the Trust Property Control Act, 1988 is included. However, this does not cover all services as included in the Glossary: providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement are not included.

- *Accountants* – to the extent their activities are "financial services", i.e., managing financial products or financial instruments (FSR Act, s.3(1)), under the FSR Act, they must be registered as FSPs. They are not covered for other activities.

Criterion 22.2 – *(Partly Met)* Covered DNFBPs must comply with the record-keeping requirements as mentioned under R.11.

Criterion 22.3 – *(Not Met)* Covered DNFBPs must comply with the PEPs requirements as mentioned under R.12 above, which have major shortcomings.

Criterion 22.4 – *(Not Met)* Covered DNFBPs must comply with the new technologies requirements as mentioned under R.15 above.

Criterion 22.5 – *(Not Met)* Covered DNFBPs must comply with the reliance on third-parties' requirements as mentioned under R.17 above, which have major shortcomings.

Weighting and Conclusion

Not all DNFBPs are included under the FIC Act: CSPs other than attorneys; accountants (for activities beyond provision of financial services), and DPMS other than KRDs as RIs. All these businesses and professions are relevant to the risk profile of the country (see section on ML/TF Risks and Context). Covered DNFBPs must comply with the requirements regarding CDD, record keeping, PEPs, new technologies, and reliance on third parties, notwithstanding the respective shortcomings as

[18] The Attorneys Act, 1979 was repealed by the LPA, s.119, with effect from 1 November 2018. The LPA, s.118: "Subject to the provisions of this Act, a reference in any other law to: (a) an advocate, a counsel or an attorney, must be construed as a reference to a legal practitioner in this Act." The effect of the LPA, s.119(3), is that the admission of an attorney who practiced under the Attorneys Act remains valid and is deemed to have been done under ss.24 and 30 of the LPA. By the same reasoning the reference in the FIC Act, Sch 1, to a practitioner continues to refer to a person who is admitted under the LPA, ss.24 and 30. The above provisions, read together with the Interpretation Act, 1957 (No. 33 of 1957), s.12, demonstrates that Item 1 of Sch 1 and the reference to the Attorneys Act still includes a practitioner to mean any attorney, notary or conveyancer.

mentioned under R.10; R.11; R.12; R.15, and R.17. The shortcomings under R.12, R.15 and R.17 are regarded as major.

Recommendation 22 is rated partially compliant.

Recommendation 23 – DNFBPs: Other Measures

South Africa was rated partially compliant with the former R.16. The main shortcomings are: in applying former R.13 and SR.IV for attorneys, there is a lack of clarity on how to interpret legal privilege in the context of meeting the reporting obligations pursuant to the FIC Act; in applying former R.15 and R.21: the deficiencies identified in former R.15 that apply to the financial sector also apply to all DNFBPs.

Criterion 23.1 – *(Partly Met)* All DNFBPs must comply with the reporting requirements of R.20 above, as these apply to all businesses in South Africa, while reference is made to the minor deficiency under R.20 regarding the requirement to report promptly.

Legal professional privilege is respected, as the FIC Act excludes the requirement to report if the relevant information was obtained through communications between an attorney and the client made in confidence for the purposes of legal advice or litigation which is pending or contemplated or which has commenced; or a third party and an attorney for the purposes of litigation which is pending or contemplated or has commenced (s.37(2)).

Criterion 23.2 – *(Partly Met)* Covered DNFBPs must comply with the internal controls requirements as mentioned under R.18 above.

Criterion 23.3 – *(Partly Met)* Covered DNFBPs must comply with the higher-risk countries requirements as mentioned under R.19 above.

Criterion 23.4 – *(Partly Met)* Covered DNFBPs must comply with the tipping-off and confidentiality requirements set out under R.21 above.

Weighting and Conclusion

CSPs other than attorneys, accountants (for activities beyond provision of financial services), and DPMS are not covered except for reporting obligations. For all sectors, the reporting obligations suffer from the same issue on "timeliness" as mentioned under R.20. These combined result in major shortcomings.

Recommendation 23 is rated partially compliant.

Recommendation24 – Transparency and Beneficial Ownership of Legal Persons

In its previous MER, South Africa was rated NC with this requirement. The major deficiencies were that there were limited measures to ensure adequate, accurate and timely information on beneficial

ownership and control of legal persons which could be accessed in a timely way by competent authorities. Since then, a new Companies Act has come into force – see section on ML/TF Risks and Context.

Criterion 24.1 – *(Mostly met)* South Africa has mechanisms that identify and describe the different types, forms and basic features of legal persons formed and created in South Africa (Companies Act No 71 of 2008, s.8). The kind of documents and information they must file with the CIPC is described in s.13 and Reg.14 of the Regulations to the Act. The Act also provides a process for foreign companies to transfer their registration from a foreign jurisdiction to be incorporated in South Africa (s. 13(5), (6)). This information is also publicly available on the website of the CIPC (www.cipc.co.za/index.php/access/disclosures). However, information which can be obtained at the CIPC offices and on its website on processes of creating legal persons only covers basic information and no processes for obtaining and recording of BO information are covered.

Criterion 24.2 – (*Not met)* South Africa has not assessed the ML/TF risks that all types of legal persons created in the country are exposed to. The nearest exercise was focused on transparency of BO and it did not consider ML/TF risks.[19]

Criterion 24.3 – (Met) Legal persons created in South Africa must be registered with CIPC (Companies Act, ss.13 and 14). The form to incorporate each type of company requires who incorporated it, the company name, the number of directors, the number of authorized shares, and the objects and powers (Companies Act Regulation, Reg.15). Full details of the directors are required (s.13(1) as read with. Reg.14, Form CoR 14.1). The CIPC assigns the company a registration number; enters information about the company from the incorporation forms in the companies register (s.14(1)); and issues the company a registration certificate. Companies must maintain an office in South Africa, provide the address of the registered office to the CIPC, and notify the CIPC about any changes of the registered address (s.23(3)(b) as read with Reg.21). All the information entered in the companies register is publicly available at the CIPC and on its website (http://www.cipc.co.za/index.php/access/disclosures).

Criterion 24.4 – *(Met)* Companies must maintain the information required by this criterion (ss.24, 36, 37 and 50) within South Africa and must notify the CIPC of the location where the information is maintained or can be accessed, if not at the company's registered office (s.25).

Criterion 24.5 – *(Partly Met)* There are some mechanisms to ensure that some of the information referred to in c. 24.3 and c.24.4 is accurate and up to date. Companies must file annual returns at the CIPC confirming the status of the information previously provided (s.33). They must also file notices with the CIPC when: the registered office changes (s.23(3)(b)(ii)) as read with s. 23(4)(a-b)); directors change (s.70(6) as read with Reg.39); there are changes to the class of shares the company can issue (s.36(4) as read with Reg. 15(3)); and changes in the location of where the company's records are accessible (s.25(2)(b)). However, there is no time limit for filing the latter. Securities registers on

[19] *NRA for BO Transparency in SA*. A report prepared for the Government's Inter – Departmental Committee on BO Transparency, May 2018

shareholding must also be maintained although there is no requirement for these to be kept up to date (s.50(1)(b) as read with Reg. 32). The CIPC is not obliged to verify for accuracy any of the information submitted to it but uses the DHA database (which it can access directly) to verify the ID information of company officials at the time of registration.

Criterion 24.6 – *(Partly met)* South Africa addresses the requirements under this criterion through option (c) (FIC Act, s.21B). Refer to c.10.10 and c.22.1 for detailed analysis. In addition, the FIC can obtain information from AIs (FIC Act s.27A) subject to the limitations to the scope of AIs (see Recs 10 and 22). Further, the FIC can request any person with a reporting obligation to provide information, including on BO information (FIC Act, s.27). The FIC then uses this information to determine with which FI, DNFBP, or VASP a legal person is a client and provides the information to LEAs who then can apply for a subpoena to compel provision of any BO information held (CPA, s.205). Not all persons with reporting obligations are AIs (including VASPs) and thus must obtain and maintain BO information. The above processes do not guarantee timely access to BO information by LEAs.

Criterion 24.7 – *(Partly met)* South Africa does not have a comprehensive mechanism to ensure that all legal persons keep accurate and up-to-date information on BO, including the CIPC. Other mechanisms, like keeping accurate and updated BO information through a BO register are also not available. Although**,** BO information obtained by AIs must be kept up-to-date and accurate (FIC Act, ss. 21C(b) and 21D), these do not cover all FIs and DNFBPs (see c.1.6). Where BO information can be obtained through share registers, any amendments to shareholding are supposed to be entered in the share register within ten days (s.36.4 as read with Reg.15(3)).

Criterion 24.8 – *(Partly met)* Companies created in South Africa must have directors (s. 66) whose obligations to the company include having to comply with any lawful requests to provide basic and shareholder information from the securities register which in some cases could include BO information. *Prescribed officers* (essentially those with executive control) must also provide this information (Companies Act Reg. 38). However, nothing requires directors or prescribed officers to be resident in South Africa. Furthermore, the scope of BO information obtained would be very limited as companies are not required to collect and maintain BO information in their securities register; only information on legal ownership (Companies Act, s.50). DNFBPs providing such services, other than attorneys are not regulated for AML/CFT, therefore their cooperation with competent authorities might be limited. No other comparable measures are identified by the authorities.

Criterion 24.9 – *(Partly met)* AIs holding basic or BO information about companies must keep records for at least five years from the date of termination of the business relationship or from the date on which the transaction is concluded (FIC Act, s.23). There are no other requirements obliging either the CIPC or the companies to maintain records of a company for any period after it has been dissolved. While companies are obliged to keep records for at least seven years (Companies Act, s.24), the timeline does not apply to the period after the company was dissolved or otherwise ceased to exist.

Criterion 24.10 – (*Partly met)* Competent authorities, including LEAs have powers to obtain access to basic and, in theory, BO information. Basic information on legal persons is publicly available

through the CIPC website (see c.24.3) meaning it can be accessed in a timely manner. Powers to obtain BO information through a company's securities register can only work to the extent that such information is available (see c.24.8). Shareholder information requests can be lodged with the CIPC Disclosure Unit which may dispatch the documents electronically or if certified copies are requested, send the documents by mail, or physically. The CPA, NPA Act, and the POCA empower different competent authorities, including LEAs to compel production of information which may be relevant to an inquiry, or investigation (see details under R.31). These powers can be used to obtain both basic and BO information, in a fairly timely manner according to the authorities to the extent that such information exists. A summons pursuant to the NPA, s.28, specifies the date and time for the person's appearance and the process and procedure is determined by the DPP. A subpoena is generally granted immediately upon application. Once served, the served party is given a period specified in the subpoena to provide the information requested under oath or appear at a particular place on a specified date and time. Timelines for obtaining information using a subpoena vary from seven to ten days and in some cases, are longer and may need to be repeated several times to get to BO information. Therefore, timely access to such information is not always assured.

Criterion 24.11 – *(NA)* This is non-applicable as bearer shares or bearer share warrants are not recognized under the Companies Act.

Criterion 24.12 – *(Mostly met)* A company's issued securities may be held by and registered in the name of one person for the beneficial interest of another person (Companies Act, s.56). Measures consistent with c.24.12(a) mitigate the risk of possible abuse of this type of security. These include: requiring the registered holder to disclose to the company the identity of the person on whose behalf a security is held; the identity of each person with a beneficial interest in the securities; number and class of securities held for each of the persons with beneficial interest and the extent of such beneficial interest (s.56(3)). This information must be disclosed in writing within five business days after the end of every month where a change has occurred in the identity information (s.56(4)(a)). Companies must keep a record of changes relating to identity of each person with a beneficial interest in the securities held in a register (ss.56(4)(a) and 56(7)(a)). Violations of these measures are an offense (see c.24.13). However, there is no requirement for the information to be filed with the registry. Nominee directors are recognized in South Africa and must comply with the requirements for directors under the Companies Act (ss. 66, 76, 77) and the common law practice of South Africa.

Criterion 24.13 – *(Mostly met)* A range of proportionate and dissuasive administrative and criminal sanctions is provided for persons that fail to comply with the requirements under c.24.3, c.24.4, c.24.6, c.24.9 and c.24.12. These include sanctions under the Companies Act as well as the CPA and NPA Acts (for failing to provide requested information to competent authorities). Fines of up to R1,000,000 ($68,000) can be imposed as well as prison terms of up to 15 years, or both (Companies Act ss. 28(4), 171(1),(2), and (7), 175(1)(b), (2), and (5), 216; NPA Act, s.41, CPA s.189). AIs that fail to fulfill their obligations under c.24.6 and c.24.9 are subject to sanctions discussed under R.35. There are no sanctions for failure by a company to keep information at least for five years after it has dissolved (c. 24.9).

Criterion 24.14 – (Partly met)

a) *(Partly met)* Basic information is available to foreign competent authorities through the CIPC website (see c.24.4). Where information is required by a foreign country, a formal request by way of a subpoena issued through a Magistrates Court has to be made to the CIPC Disclosure Unit. It normally takes about ten working days to provide the information; longer if the file and documents related to the request are not readily available. Thus, providing the information is not always predictable and timely. The Disclosure Unit does not have a formal MOU with any entity in respect of disclosures. and thus, this type of might not always be done in an efficient and timely manner (see Recs 37 – 40).

b) *(Mostly met)* State disclosures for information relating to shareholding are requested electronically with a formal letter of request on the entity's letterhead attached or receipt of a subpoena in respect of a specific disclosure. Procedures of attending to international requests described in (a) above also apply to exchanging information on shareholding.

c) *(Partly met)* The FIU and FSR can obtain BO information on behalf of foreign counterparts (see R.40). The DPP and an Investigating Director, respectively, can summon anyone for information at a place, date and time specified by them (CP Act, s.205 and NPA Act, s.28) but these powers are only useful to the extent that the subject person possesses BO information and as already discussed the powers may not ensure that the information is provided rapidly.

Criterion 24.15 – *(Partly met)* South Africa does not have a clear mechanism for monitoring the quality of assistance received from other countries in response to requests for basic and BO information. The authorities consider factors such as whether the correct information was provided, whether it was adequate in terms of content and substance, and reliance on public information provided by some other jurisdictions to verify and validate information provided. However, this is not done in all cases as the authorities do not always have the requisite powers to share information (see R.40).

Weighting and Conclusion

South Africa meets some of the requirements but there are moderate deficiencies which remain. The ML/TF risks associated with the different types of legal persons have not been fully assessed and identified. BO information is not always timely available to competent authorities and there is still limited access to such information as not all FIs, DNFBPs and VASPs are subject to requirement to identify BO, and the BO information that AIs must hold suffers from limitations described in R.10. Some powers available to access BO information cannot obtain such information as the information is not required to be kept.

Recommendation 24 is rated partially compliant.

Recommendation 25 – Transparency and Beneficial Ownership of Legal Arrangements

In the third Round of MEs, South Africa was rated NC with this requirement. The major deficiencies were that where a legal person was a founder, trustee or beneficiary, there was no obligation to obtain beneficial ownership information of the legal person and identification information on the founder and beneficiary was not verified by the trust register.

Criterion 25.1 – (Partly Met) Both inter-vivos and testamentary trusts exist in South Africa and are mostly administered under the Trust Property Control Act, 1988 (TPC Act).

a) [Partly Met) Inter-vivos trusts which have property present in South Africa must be registered with the Master (TPC Act, s. 4). However, none of the provisions in TPC Act give specific details as to who must be identified in the trust instrument and the kind of information which must be obtained by the trustee or must be part of the instrument at the time of lodging it for registration. Such duties can only be inferred based on the trustee's fiduciary duties under common law and statutory law in South Africa. Trustees designated as AIs (professional trustees[20] or TSPs, FIC Act, sch.1) must comply with all due diligence measures intended to establish and verify the identity of the client or person either giving the instruction to create the trust, creating the trust or being appointed as trustee (FIC Act, s.21). Further, the requirement to keep the information current is not met.

b) (Not Met) There are no requirements on any trustees to hold information on agents and service providers to the trust.

c) (Partly Met) Professional trustees, who are AIs must maintain information for at least five years from the date that their involvement with the trust ceases (FIC Act, s.23, also see c.11.1 and c.11.2). However, the information would not cover other natural persons who might be exercising ultimate effective control over the trust, nor information on agents and service providers to the trust.

Criterion 25.2 – (Partly Met) Professional trustees who are AIs (see c.25.1(b)) must keep information which they obtain up to date and accurate (FIC Act, s.21D). However, this obligation does not extend to other trustees.

Criterion 25.3 – (Partly Met) There are no explicit measures to ensure that trustees disclose their status to FIs and DNFBPs when forming a business relationship or carrying out an occasional transaction above the threshold. However, on the basis that trustees must deposit money they receive as trustees into a trust account in a bank (TPC Act, s.10), they must disclose their status to the bank when they open the trust account. The requirement does not apply to other FIs, DNFBPs, or VASPs.

Criterion 25.4 – (Met) There are no legal restrictions to prevent trustees from providing competent authorities with any information relating to a trust; or from providing FIs, DNFBPs, and VASPs, upon

[20] Any person that, […as a business…], invests, keeps in safe custody, controls or administers trust property.

request, with information on the beneficial ownership and assets of the trust to be held or managed under the terms of the business relationship.

Criterion 25.5 – (Partly Met) Competent authorities, in particular, LEAs have powers to obtain access to any information on trusts held by professional trustees and other AIs. However, the processes available to LEAs to access BO information do not always ensure timely access to such information. Trustees, who are not AIs, are not required to collect BO information (see c.25.1). The information available from other AIs having trusts or trustees as clients, is subject to the deficiencies identified under c.10.11. A FIC authorized representative can also access records kept by an AI to obtain further information to a report made to the FIC. Other powers to obtain timely access to information held by trustees, and other parties on the beneficial ownership and control of trusts exist under the FIC Act, the CPA, the NPA Act, and the POCA (see c.24.10). VASPs are not AIs and are not required to obtain and hold BO information.

Criterion 25.6 – (Partly met) South Africa has mechanisms to provide international cooperation for information on trusts but these mechanisms do not guarantee rapid provision of the information:

a) (Partly met) South Africa has mechanisms to provide international cooperation for basic information on trusts. Some information on trusts can also be obtained on the Master's website. However, not all basic information is collected and maintained by the High Court. Information on trusts can be formally requested and obtained through MLA from the DoJ&CD, which is the central authority for such requests, but the information is not always provided rapidly (see R.37 & 40).

b) (Mostly met) Information can be exchanged by financial sector regulators, or designated authorities using mechanisms described in R.37 and R.40. Information on trusts can also be obtained through counterpart to counterpart requests: foreign FIU to FIC which may obtain information from AIs (FIC Act, s.40(1)(b),).

c) (Partly met) The SAPS can use its investigative powers under domestic law to obtain, on behalf of foreign counterparts, BO information on trusts, to the extent it is available, using the mechanisms described under R.37 and R.40. But this may not always result in rapid provision of the information.

Criterion 25.7 – (Partly met) Professional trustees that are TSPs are subject to sanctions under the FIC Act for non-compliance with requirements discussed under c.25.1(a) and (c), (see R.35). No administrative or criminal sanctions are applicable to other trustees.

Criterion 25.8 – (Partly met) Sanctions described in c.24.13 also apply for failure to grant competent authorities timely access to trust information described in c.25.1 However, not all trustees must obtain and hold information required under c.25.1 and not all information required under the same criterion is covered. The process followed by LEAs in obtaining information (c.24.6), which would also apply to a trust, does not in itself confirm LEAs having timely access to the information, particularly on BO. Most of the sanctions provided in the FIC Act, NPA Act and CPA only apply for

failure to provide information (NPA Act, s.41, CP Act, s.205) not failure to grant LEAs timely access to information (see c.24.13).

Weighting and Conclusion

There are to a moderate extent, deficiencies relating to professional trustees being required to obtain full information on BO when they are creating trusts and AIs not being required to obtain BO information of any other natural person exercising ultimate effective control over a trust. Absence of such a requirement affects almost all criteria to this Recommendation. There are limitations on sanctions applicable to non-professional trustees.

Recommendation 25 is rated partially complaint.

Recommendation 26 – Regulation and Supervision of Financial Institutions

South Africa was rated partially compliant with the former R.23 and R.29. There were deficiencies in market entry controls. Registration and licensing did not apply to MVTS, financial leasing, and finance companies. Several FIs were not subject to AML/CFT supervision and some supervisors lacked adequate powers, and there were concerns about supervisory effectiveness.

Criterion 26.1 – (*Mostly Met)* The FIC Act, sch.2, as amended, including via the Interpretation Act, s.12,[21] lists the following supervisory bodies but without providing details as to which sector(s) each body covers:

- **The FSCA** became responsible for AML/CFT supervision under the FAIS Act, the Collective Investment Schemes Control Act, the Long Term Insurance Act and the Financial Markets Act (FM Act), collectively referred to as "sector legislation", all effected through a transition clause inserted by the FSR in the sector legislation stating that the sector legislation should be read as a referring to the FSCA, an independent body created by the FSR Act.

- **The SARB:PA** became responsible for AML/CFT supervision when it replaced "The Registrar" *as defined the Banks Act 1990, ss.3 and 4, –* s.3 has been repealed while s. 4 was significantly amended to set out the functions of the SARB:PA (sch.2, para.2).

- **The SARB:FinSurv** *in terms of Regulation 22E of the ECR, 1961* –is thus authorized to supervise ADLAs for compliance with the FIC Act.

- **The SARB:NPSD** is as supervisory body under the FIC Act as it organizes the payment clearing system (SARB Act, s.10(1)(c)). It is responsible for ensuring compliance by participants of the payment system (including banks, mutual banks, Postbank, and SAPO) with the *EFT Directive 1* for wire transfers. In practice, the SARB:NPSD relies on the SARB:PA to conduct onsite

[21] This provision provides that "…[w]here a law repeals and reenacts with or without modifications, any provision of a former law, references in any other law to the provision so repealed shall, unless the contrary intention appears, be construed as references to the provision so reenacted"

inspections for banks and mutual banks. The SARB:NPSD and the FIC coordinate to oversee Postbank's and SAPO's compliance with the *EFT Directive 1*.

The FIC is the designated AML/CFT supervisor for Postbank, Development Bank of South Africa, Land Bank South Africa, Ithala, ISOC, and money lenders against securities.

The FSCA has delegated AML/CFT supervisory responsivities of life insurers to the SARB:PA. For AUs, conduct of onsite inspections has been delegated to the JSE and four other exchanges.[22]

The following types of FI do not have a designated AML/CFT supervisor: CFIs, credit providers other than money lenders against securities, and FinTech companies offering financial services other than as FSPs.

Criterion 26.2 – *(Mostly Met)* The following FIs must be authorized by the FSCA or the SARB:PA to perform services in South Africa:

By the FSCA: FSPs including insurance intermediaries ((FSR Act, s.111(1)), Financial Advisors and Intermediaries Act, s 7), CIS managers (registration only), Collective Investment Schemes Control Act, s.5), AUs of exchanges (Financial Markets Act, s.4).

By the SARB:PA: banks[23] (Banks Act, s.11), mutual banks (Mutual Banks Act, s.9), co-operative banks and co-operative financial institutions (Co-operative Banks Act, ss.6 & 40A), insurers (Insurance Act, s. 5).

As mentioned under R.14, ADLAs involved in transferring or dealing in foreign currencies are subject to licensing by the SARB:FinSurv. MVTSs providing pure domestic services are not subject to any licensing or registration requirements.

Postbank and ISOC operate as deposit-taking entities without a banking license under a Banking Act exemption.[24] A few public entities, including Development Bank of South Africa, Land Bank South Africa, the PIC, are established by laws and engage in securities-related services as AUs of the JSE. The PIC is also authorized by the FSCA as an FSP.

Stand-alone credit providers other than money lenders against securities, and FinTech companies offering financial services that are not FSPs are not subject to market entry controls. Information required during the process for approving applications for registration as a bank prohibit the establishment or operation of a shell bank in South Africa (Banks Act, s.16)

Criterion 26.3 – (*Partly Met)* For all core FIs, fitness and propriety of directors, executives, senior managers, and significant owners must be assessed when licenses are applied for (FSR Act, ss.1(1)

[22] These are: A2X, 4AX, ZAR X, and Equity Express.

[23] Includes bank controlling companies and branches of foreign institutions

[24] As of the onsite, Postbank's application for a banking license, permitted after enactment of the Financial Matters Amendment Act, was under review.

and115(c)). Significant owners are persons that directly or indirectly have the right to appoint, or the consent is required to appoint, 15 percent of the members of a governing body of the FI or persons that own qualifying stakes in an FI (FSR Act, 157). The SARB:PA or the FSCA may remove a person from a specified position or function if the person no longer complies with the fit and proper requirements (FSR Act, s. 145(d)). They can also debar a natural person if the person contravened a financial sector law in a material way (FSR Act, s.153). A person may not become significant owner without prior written approval of the SARB:PA or the FSCA (FSR Act, s. 158 (2)), while the latter may not grant approval unless satisfied the person is fit and proper (FSR Act, s.158(7)). The FSR Act further authorizes the SARB:PA and the FSCA to make standards for fit and proper including for personal character qualities of honesty and integrity (FSR Act, s. 108). However, for some sectors the fit and proper standards established by the regulators do not extend to significant owners or beneficial owners. Specifically:

- **Banks** - Persons convicted of the offense of fraud or any other offense of which dishonesty, or the commission of violence, was an element or contravened the provisions of any law designed for protecting members of the public cannot hold the position of directors or executive officers (Banks Act, s.1(1A)). Appointment of these positions are subject to the SARB:PA's approval and may be rejected if fit and proper requirements are not met (Banks Act, ss. 60(5)(c) and 60(6)). The fit and proper standards do not apply to significant owners or beneficial owners, though s.37(4)(a) requires that significant shareholders not be contrary to the public interest.

- **Mutual banks** - Directors and executive officers are subject to the same fit and proper criteria as banks (Mutual Bank Act, 37). A director may be disqualified when s/he no longer meets the fit and proper standards (Mutual Bank Act, 38) but this does not apply to executives or managers. The fit and proper standards do not apply to significant owners or beneficial owners.

- **Cooperative banks** - Directors, managing directors and executive officers are subject to fit and proper standards which trace back 10 years preceding the application (Cooperative Banks Act, s.9). The fit and proper standards do not apply to significant owners or beneficial owners.

- **CFIs** – no integrity-related requirements or criteria are in place.

- **Life insurers** -Directors, senior managers, and significant owners (as defined under the FSR Act) are subject to fit and proper requirements (Insurance Act, s.13). The standards are set out in Prudential standards GOI 4 which contain similar standards to those for banks. However, appointment of senior managers is not subject to the SARB:PA's approval. The SARB:PA may only approve changes in control of an insurer or controlling company when it is satisfied that the directors, senior managers, and significant owners are fit and proper (Insurance Act, s.17).

- **FSP**s **(including insurance intermediaries)** - Persons with managerial functions including compliance officers, other persons who oversee an FSP's operations, and its representatives must always be fit and proper (FAIS Act, ss.1, 6A(a)(iii), 8A, and 13(2)(a)(1)). Board Notice 194 sets out incidents indicating when persons are not honest, or lack integrity or good standing, which include having been found guilty of offenses that involve dishonesty, breach of fiduciary duty,

dishonorable or unprofessional conduct (s.9). The Notice also extends the fit and proper requirements to persons who "control or govern" an FSP including its directors, members, trustees, or partners. It cannot be established that these capture beneficial owners. The FSCA may suspend or withdraw authorization when the licensee or any of its senior managers does not meet or no longer meets the fit and proper requirements (s.9). These however do not extend to significant owners or beneficial owners.

- **CIS managers** - A director must be a person who is honest and has integrity (Notice 910, s.4(a)). The FSCA may terminate the appointment of a director or officer of a CIS manager if s/he is not fit and proper (CIS Control Act, s. 43) but appointment of such persons is not subject to its approval. The criteria for fit and proper, like those for banks, only trace back 5 years preceding the date of application (Notice 910, s.4(c)). These do not extend to significant owners or beneficial owners.

- **AUs of the JSE** - The exchange rules must provide for equitable criteria for authorization to ensure high business integrity (FM Act, s. 17). JSE Equity Rules set out fit and proper requirements that are like those for banks (s. 4.10). Directors, natural persons who directly or indirectly hold more than 10 percent of the issued shares of the applicant or member and compliance officers are subject to these requirements.

In addition to the fit and proper standards established by sector regulators, all supervisory bodies (see details under c. 26.1), in making a determination as to whether a person is fit and proper to hold office in an AI, take into account any involvement by that person in any noncompliance with this FIC Act or any order, determination or directive made in terms of it, ML or TF activities (FIC Act, 45(1B)(f)).

Fitness and properness of shareholders or directors is part of the prerequisites set out in the ADLA Manual for an application for ADLA to be approved (s. A.3(C)). This does not extend to managers or beneficial owners. Furthermore, the SARB:FinSurv does not have powers to appoint or remove any individuals.

There are no measures to prevent criminals from owning, controlling, or managing CFIs, credit providers other than money lenders against securities, FinTech companies offering financial services that are not FSPs, and public FIs (for the managing aspect).

Criterion 26.4 – (Partly Met)

a) *(Partly Met)* Most core principles institutions are subject to AML/CFT supervision, but not in line with the core principles as consolidated group supervision for AML/CFT purposes is not in place. The new supervisory framework is yet to be assessed against the Core Principles. South Africa is expected to have its IMF review under the Financial Sector Assessment Program completed during 2020. The SARB:PA must undertake risk-based supervision and can designate members of a group of companies as a financial conglomerate (FCR Act, s.160(1)) and set prudential standards for them (s.164) it is yet to start conglomerate

supervision for banks, mutual banks, and insurance. For AUs only the JSE is undertaking AML/CFT supervision. No consolidated AML/CFT supervision of financial groups is carried out by either the SARB:PA or the FSCA at the group level. FIC's AML/CFT monitoring of Postbank does not fully accord with the core principles.

b) *(Partly Met)* ADLAs are subject to the SARB:FinSurv's monitoring of compliance with requirements flowing from the FIC Act and the ECR (FIC Act, s.45, sch.2, para. 2; ECR Act, Reg 2, 3 &22). Cooperative banks and public FIs, who also engage in money transfer services are not subject to authorization but are covered as AIs and supervised by the FIC. Credit providers other than money lenders against securities, and FinTech companies offering financial services that are not FSPs are not subject to supervision.

Criterion 26.5 – *(Mostly Met)*The frequency and intensity of AML/CFT supervision is informed to some degree by ML/TF risks. The SARB:PA must apply a RBA (see c.26.4) and has developed a RBA framework to AML/CFT supervision to measure, identify, assess, and understand ML/TF risks of banks. The framework considers factors related to each bank's regulatory history, inspection findings, etc. and several inherent ML risk factors but does not consider ML/TF risks in the country or the characteristics of banks or groups. The SARB:PA has two conflicting versions of the cycle in two in-force documents: the Inspection Manual and Risk-Based Supervisory Framework. The cycle outlined under the Table below is that included in the Inspection Manual (in force July 2019), which is more recent than the Framework (April 2018). Neither cycle is followed by the SARB:PA in practice.

Table 1. SARB:PA AML/CFT Supervisory Cycle Plan

Risk ranking	No.	Supervisory action cycle	Meetings	Reporting
Large banks/Very high risk	4	Every 12 to 18 months Detailed inspection, 4-6 weeks; large samples Focus on highest risk areas	3 x AML/CTF meetings	Monthly updates – compliance and audit reporting
High Risk	3	Every 24 months Detailed inspection, 3-4 weeks; large samples Focus on identified high and medium risk areas	1 x AML/CTF meeting	Quarterly updates
Medium Risk	30	Every 36 months	Attend SARB:PA workshops	Bi-annual updates
Low Risk	N/A	Every 49 months	Attend SARB:PA workshops	Annual update
Very Low Risk	N/A	Every 49 months	Attend SARB:PA workshops	18-month update

The SARB:PA took over supervision of and commenced inspections of life insurers in February 2019.[25] Its inspections are informed by the size of institutions and prudential regulatory data without considering ML/TF risks. The SARB:PA has conducted an ML/TF risk assessment of the insurance sector which will inform future supervisory activities but is not yet assessing individual institution's or group's ML/TF risk profiles.

The frequency and intensity of the FSCA's AML/CFT inspections of FSPs and CIS managers is determined by each institution's size and a general risk rating in which AML/CFT control constitute a three percent weighting. For each AU of the JSE, frequency and intensity is determined using a risk rating of 50-50 ML/TF factors and market risk.

The SARB:FinSurv's framework to assess ADLAs' ML/TF risks considers several risk factors that cover aspects of each ADLA's AML/CFT controls as well as certain inherent risks (such as customer base, location, etc.). The framework also considers characteristics of the ADLA (such as category and size) and will consider findings of the ML and TF NRAs when they become available. Regardless of the risk assessment, all ADLAs head offices are inspected once a year while the branches are selected based on ML/TF risk ratings.

[25] Previous AML/CFT supervision of the life insurance was conducted without having regard to ML/TF risks.

The FIC conducts onsite inspections of KRDs based on a risk tool (that focuses primarily on reporting patterns) but this is not the case for TSPs. Postbank and Ithala are, due to their perceived high ML/TF risk status, visited annually.

Criterion 26.6 – (*Partly Met)* The SARB:PA's policy is to conduct formal ML/TF risk assessments of each bank and mutual bank every two years, but in practice the matrix generated the first set of ratings in 2016 and has been updated only once in 2019.

The FSCA's general risk rating of each supervised entity is assessed at entry and updated when new information is provided by the entity, a complaint is received, and upon major regulatory events (e.g., investigations, debarment of representatives) including any related to AML/CFT.

The SARB:FinSurv updates risk ratings of ADLAs after its yearly onsite inspections.

There is no evidence that the FIC has undertaken risk assessments of domestic MVTSs, public FIs except Postbank, credit providers other than money lenders against securities, and FinTech companies offering financial services.

Weighting and Conclusion

South Africa has undergone legislative reforms in the last three years. Although technically a supervisory body has been designated to a large majority of FIs, a few sectors are only subject to reporting requirements and are not monitored for AML.CFT compliance. Gaps exist for market entry of certain non-core sectors. The fit and proper requirements are inconsistent and often not extended to beneficial owners including for core FIs. Supervision is carried out across most main FIs but the application of an RBA for AML/CFT supervision is either at an early stage or does not exist.

Recommendation 26 is rated partially compliant.

Recommendation 27 – Powers of Supervisors

In its previous MER, South Africa was rated partially compliant with former R.29. The main deficiency was the lack of clear authority for the securities supervisor to inspect for compliance, conduct onsite visits, and obtain information to determine compliance.

There is a scope limitation – some FIs have no AML/CFT obligations or compliance oversight (see c1.6). The analysis below does not apply to these sectors.

Criterion 27.1 – *(Mostly Met)* The FIC Act, s.45(1B), sets out powers supervisory bodies listed in sch.2 (see details under c.26.1) have to supervise or monitor compliance with AML/CFT obligations by AIs under their purview. In addition, the FSCA and the SARB:PA have powers to issue directives to entities and key persons (generally includes directors and senior management) under their purview if, among other areas, they are in contravention of the FIC Act or involved in, or likely to be involved in financial crime (FSRA, s.143, ss.(1)-(3)). "Financial crime" includes failure to report (see c.27.4 below). Moreover, the FIC is empowered to supervise and enforce the FIC Act AML/CFT obligations

of AIs, RIs (see c.1.7 on which sectors fall under RIs) and other persons if these are not regulated or supervised by a supervisory body and or if a supervisory body fails to enforce compliance (FIC Act, s4(g)).

Criterion 27.2 – (*Met)* The director or the head of a supervisory body (see c.26.1) is empowered to appoint inspectors to determine level of compliance of an AI or RI with the FIC Act. Appointed inspectors may enter the premises of the AI or RI for these purposes. (FIC Act, ss. 45A & 45B).

Criterion 27.3 – (*Met)* The FIC or a supervisory body may issue directives to AIs, RIs, or any other persons to provide a wide range of information (FIC Act, s. 43A(3)). An inspector (FIC Act, s.45A), in conducting an inspection, may order any person who has or had any document in his, her or its possession or under his, her or its control relating to the affairs of the AI, RI or person to produce that document or to provide the inspector with information in respect of that document (FIC Act, s.45B(2)(b)(ii)).

Criterion 27.4 – (*Partly Met)* The FIC and supervisory bodies have powers to impose a range of administrative sanctions on any AI, RI or other person when satisfied that there has been failure to comply or non-compliance with their respective obligations (which for non-AIs are very limited) in the FIC Act (FIC Act, s.45C). In addition, the SARB:PA and the FSCA also have powers to issue directives to AIs under their purview if the AI or its directors or senior managers are "involved or likely to be involved in financial crime" (FSR Act, ss. 143 & 144). The SARB:PA and the FSCA may remove a person from a specified position or function when the person has been involved in financial crime (FSR Act, s. 145). Failure to report a suspicious or unusual transaction, or property associated with terrorist or financial sanctions pursuant to UNSCRs constitutes a financial crime (FSR Act, s.1; FIC Act, ss. 50, 51A & 52). When a licensee has contravened a directive issued by the SARB:PA or the FSCA, the relevant regulator may suspend or revoke the license (FSR Act, ss. 120(1)(c)(iii) and 121(1)(b)). These measures do not apply to breaches of the FIC Act in aspects other than those mentioned above.

Weighting and Conclusion

Supervisors have powers to supervise and ensure compliance, conduct inspections, compel production of records and information, and impose a range of administrative sanctions. However, gaps remain in the ability to suspend or withdraw licenses. Some FIs are not subject to AML/CFT obligations or oversight for compliance (see c.1.6)

Recommendation 27 is rated as partially compliant.

Recommendation 28 – Regulation and Supervision of DNFBPs

In its previous MER, South Africa was rated partially compliant for former R.24 (and R.25). The FIC Act only provided for criminal sanctions, none of which had been applied and their applicability was not uniform across all supervisors. South Africa had not extended its regulatory regime to encompass FATF's DNFBPs population with many high-risk areas including DPMS and CSPs that are

not attorneys or accountants, were found to be outside of the regulatory regime. Guidance was also found to have not been issued for most sectors.

Criterion 28.1 – (Mostly Met)

a) *(Met)* No person may operate a casino (including an internet casino) without being issued with an appropriate license (National Gambling Act, ss. 8 and 11). There are nine provincial licensing authorities (PLA) responsible for issuing gambling licenses and supervising the casinos within their respective provinces. Each PLA must ensure that casinos which operate in its province are licensed to do so (National Gambling Act, s.3)

b) *(Mostly Met)* A person cannot hold a casino license if they fail to meet fit and proper tests (National Gambling Act, s.50). PLAs are authorized to investigate and consider license applications (s.30). Each PLA has legislative basis to prevent criminals from entering the sector and each PLA has its own rules on the criteria of fitness and propriety (underpinned by the legislation) but they are inconsistent as to who must be fit and proper and the criteria for fitness and propriety. It therefore cannot be established that they are adequate to prevent criminals or their associates from owning or managing casinos.

c) *(Met)* The NGB and PLAs are authorized to monitor casinos' compliance with the FIC Act (FIC Act, s.45 and Sch 2 and National Gambling Act, s.31(1)(e)).

Criteria 28.2 and 28.3 – (*Partly Met)* The FIC Act designates the following as the AML/CFT supervisory bodies for other DNFBPs (FIC Act, s.4(g) and sch.2):

- Estate Agents – the EAAB
- Attorneys (including notaries and independent legal professionals) – the LPC
- TSPs and any other person that, as a business, invests, keeps in safe custody, controls, or administers trust property – the FIC
- Auditors (for activities beyond providing financial services) – the Intendent Regulatory Board for Auditors
- Motor vehicle dealers (RI) – the FIC
- Krugerrand Dealers (KRDs -RI) – the FIC

The FIC has a system to monitor KRDs and TSPs. Estate agents are subject to monitoring by the EAAB. Attorneys are not "subject to" AML/CFT monitoring for compliance with the FIC Act; the authorities have not demonstrated that the LPC has systems in place to carry out such monitoring and, to date, the LPC has not carried out any such activity. DPMS that are not KRDs, accountants (for activities other than managing financial assets), and CSPs that are not attorneys have only reporting obligations under the FIC Act and are not subject to monitoring for compliance.

Criterion 28.4 – (Partly Met)

a) *(Partly Met)* Supervisory bodies listed above can supervise or monitor AIs and RIs compliance with the FIC Act using the same powers discussed in R.27, which do not include power to suspend or withdraw licenses for AML/CFT non-compliance.

b) (Partly Met)

- **Attorneys** are admitted by the High Court as legal practitioners if they are fit and proper (the LPA, s.24(2)(c)). The criteria applied are unclear and the authorities could not demonstrate that they are adequate to prevent criminals or their associates from being professionally accredited.

- **Trust Service Providers** must be authorized by the Master only when they act as a trustee, if the Master is satisfied of the applicant's "due and faithful performance" (TPC Act, s.6). The criteria applied in assessing this however are unclear, thus it is impossible to establish they are adequate to prevent criminals or their associates from owning or managing the TSPs.

- **Estate Agents** must obtain a fidelity fund and a registration certificate from the EAAB to practice (Estate Agency Affairs Act, s. 16). An applicant will be rejected if he/she has at any time been convicted of an offense involving an element of dishonesty (Estate Agency Affairs Act, s. 27(a)(ii)). A certificate issued will be withdrawn under the same circumstances.

- For DPMS, accountants (for activities beyond provision of financial services), and CSPs other than attorneys, there are no measures to prevent criminals from owning, controlling, or managing the entity or being professionally accredited.

c) *(Partly Met)* The supervisors mentioned under c.28.2 have the same sanctioning powers as discussed under R.27, which suffer from the same deficiencies mentioned there.

Criterion 28.5 – (Partly Met)

a) *(Partly Met)* The FIC uses a risk-based supervisory tool for monitoring KRDs to ensure compliance with the FIC Act. This tool uses selected inherent risks and mitigants to determines a risk rating for an institution, which then determines whether the entity requires an inspection. FIC does not use a risk-based system for TSPs. The authorities have not demonstrated the frequency and intensity of supervision of other DNFBPs is driven by ML/TF risks.

b) *(Partly Met*) For supervised DNFBPs (TSPs, KRDs, estate agents, and casinos) or there is no evidence that this criterion is being implemented. Attorneys are not subject to monitoring (see c.28.3). DPMS that are not KRDs, accountants (for activities other than provision of

financial services), and CSPs other than attorneys have only reporting obligations under the FIC Act and are not subject to monitoring for compliance.

Weighting and Conclusion

Supervisors have been designated for casinos, estate agents, attorneys, and TSPs and KRDs (as RIs). These sectors (except attorneys) are subject to some limited supervision, but it is not, for the most part, risk sensitive. DPMS that are not KRDs, accountants (for activities other than provision of financial services), and CSPs that are not attorneys have only reporting obligations under the FIC Act and are not subject to monitoring for compliance with preventive measures. For all sectors and professions, it cannot be established that adequate controls are in place to prevent criminality from operating.

Recommendation 28 is rated as partially compliant.

Recommendation 29 - Financial Intelligence Units

South Africa was rated largely compliant with the former R.26. The deficiency noted was that there had been no annual reports concerning AML/CFT cases, typologies and trends analysis that had been issued or published.

Criterion 29.1 – (*Met)* South Africa's FIU, the FIC, was established as the national center for receiving, analyzing and disseminating information on the suspicion of ML and TF following the passage of the *FIC Act No. 38 of 2001* and has been operational since 2003. The FIC's primary objective is the identification of the proceeds of unlawful acts and the combatting of ML activities, FT, and related activities (FIC Act, s.3). The FIC is to make information collected by it available to various law enforcement, prosecution, and intelligence services. The FIC is to process, analyze and interpret information disclosed to it and where appropriate, initiate analysis based on information in its possession (FIC Act, s.4). In addition, the FIC is to inform, advise and cooperate with law enforcement, prosecution, and intelligence services.

Criterion 29.2 – (Met)

a) *(Met)* Any person who carries on a business, manages, or is employed by such business must report to the FIC suspicious and unusual transactions concerning ML and TF (FIC Act, s.29).

b) *(Met)* AIs and RIs (see on c.1.7 for definitions") must report to the FIC any cash transactions above R24,999.99 ($1,700.)[26] (FIC Act, s.28; FIC Act, Reg. 22B). AIs must report to the FIC any property associated with terrorist and related activities and TFS pursuant to UNSCRs (FIC Act, s.28A).

[26] Including an aggregate of smaller amounts which combine to come to that amount if it appears to the AI or RI concerned that the transactions involving the smaller amounts are linked or considered fractions of one transaction.

Criterion 29.3 – (Met)

a) *(Met)* Persons subject to reporting obligations to the FIC must provide additional information, upon request of the FIC, relating to transactional activity and supporting documentation, concerning the report filed by them and the grounds for the report as the FIC may reasonably require for the performance by it of its functions (FIC Act, s.32). In addition, persons subject to reporting obligations to the FIC must provide information to the FIC upon request regarding whether certain persons are clients and the type and status of their business relationship with such clients (FIC Act, s.27). The FIC may also obtain whatever information, from an AI, that can be reasonably established to assist the FIC *'to identify the proceeds of unlawful activities or to combat ML activities or FT and related activities'* by way of a warrant issued by a judge, magistrate or regional magistrate which is a restrictive process compared to the standard's expectation of FIUs being able to request additional information directly from entities other than the one that filed the initial report. (FIC Act, s.27A).

b) *(Met)* The FIC has both direct and indirect access to a wide range of non-publicly available databases. Examples include:

- The FIC has direct access to information in databases maintained by other government departments (e.g. the population register maintained by the DHA and cross-border movement information on the DHA movement control system).
- The FIC has indirect access to information held by the SAPS related to the cross-border movement and criminal record of individuals; the Exchange Control Division of the SARB; and the SARS related to tax.

The FIC has further direct access to commercial databases containing information pertaining to registered legal entities and the composition of their governing structures, credit histories of individual and entities, ownership of property and lists related to PEPs. The FIC also makes use of open source information via the internet such as such as media and other paid subscriptions. Other methods to access information include MOUs and information shared via the ESW.

Criterion 29.4 – (Mostly Met)

a) *(Met)* The FIC conducts operational analysis related to specific targets proactively and upon request by competent authorities. For details on the number of operational analysis disclosures made by the FIC, please refer to the statistics provided in IO.6.

b) *(Partly Met)* The FIC also produces output it classifies as strategic analysis products, but these are not designed to support the operational needs of competent authorities but rather to raise awareness within REs and the general public (see details in IO.6).

Criterion 29.5 – (*Met)* The FIC must make information reported to it, obtained by and generated by its analysis available to relevant competent authorities at the initiative of the FIC or at the request of the competent authority (FIC Act, s.40). Any information exchange shall be made pursuant to written

agreements (FIC Act, s.40 (4)). The FIC must ensure that appropriate measures are taken to prevent loss and unlawful access to its information. It must continuously identify risks and establish, maintain, and update appropriate safeguards against such risks (FIC Act, s.41). In practice the FIC has MOUs in place to govern the sharing of information with competent authorities. All information is approved before dissemination and secure mechanisms are used to disseminate the information to competent authorities. The FIC utilizes the ESW to disseminate information to other jurisdictions (FIUs) who are members of Egmont. For non-Egmont members and domestic competent authorities, the FIC uses the goAML encrypted email application, Secure File Transfer Protocol (SFTP) solution as well as a dedicated email mailbox, which is PKI encrypted to disseminate information. The three mechanisms/applications are accessed through authentication protocols.

Criterion 29.6 – (Met)

a) *(Met)* The FIC must ensure that appropriate measures are taken to prevent loss and unlawful access to it information. It must continuously identify risks and establish, maintain, and update appropriate safeguards against such risks (FIC Act, ss.41 & 41A). It also has mechanisms in place to ensure this.

b) *(Met)* Information with respect to staff must be gathered in a vetting investigation by the State Security Agency and the Director (of the FIC) must be satisfied that staff may be appointed without the possibility that such person might be a security risk (FIC Act, s.12). Similar requirements are in place with respect to the Director; with the Minister being the one required to be satisfied (FIC Act, s.13).

   - The FIC's implemented security policy covers the following aspects:
   - The legislation applicable to the workings of the FIC and the protection of the confidentiality of its information.
   - The responsibilities of every employee regarding security.
   - Document security including classification, access, handling, and storage of documents.
   - IT/Computer security including access and exit management to networks, levels of access, password control, etcetera, and
   - Communication security including telephone, facsimile, internet, e-mail and secured boardrooms.

c) *(Met)* The Analysis Unit of the FIC is segregated from the other Business Units and access to the operational space of the Business Unit is restricted to those tasked with analysis work.

The FIC's information technology systems are protected from unauthorized access in the following ways:

- Access to files is on a needs basis and controlled through systems access controls based on user roles.
- The FIC has several security layers in place to enforce access control, e.g. VLAN segregated network segments, built-in application access controls, and all information stored on the domain needs domain access first.
- The FIC's database is protected by a double layered access system, meaning that AUs need to firstly have access to the network through a password followed by an additional log-in system to access the database.
- A Managed Security Incident and Event Management service monitors the environment round the clock.

Criterion 29.7 – (Met)

a) *(Met)* The FIC is operationally autonomous. The FIC Director is appointed by the Minister of Finance and can be removed by the Minister based on criteria such as security, misconduct, incapacity, or incompetence (FIC Act, s.7). The FIU may do all that is necessary or expedient to perform its functions effectively including doing anything that is incidental to the exercise of any of its powers (FIC Act, s.5).

b) *(Met)* The FIC has the power to share information held by it with competent authorities and foreign counterparts (FIU Act, s.40). Sharing of information is done through written agreements (MOUs).

c) *(NA)* The FIC is not located within the existing structure of another authority.

d) *(Met)* The FIC may do all that ***is*** necessary or expedient to perform its functions effectively (FIC Act, s.5) including:

- determining its own staff establishment and the terms and conditions of employment for its staff within a policy framework determined by the Minister;
- appointing employees and seconded personnel to posts on its staff establishment, and;
- obtain the services of any person by agreement, including any state department, functionary, or institution, to perform any specific act or function.

The NT leads an inter-governmental committee (the Medium-Term Expenditure Committee), which receives the FIC's strategic and business plans, and recommends allocations based on national priorities and available funds.

Criterion 29.8 – *(NA)* The FIC is a member of the Egmont Group.

Weighting and Conclusion

The framework under which the FIC operates complies with most requirements. However, operational analysis is adversely affected by gaps in the FIU's intelligence holdings based on some DNFBPs not being covered under the AML/CFT framework and strategic analysis is not specific to identifying ML and TF related trends and patterns.

Recommendation 29 is rated largely compliant.

Recommendation 30 – Responsibilities of Law Enforcement and Investigative Authorities

In its previous MER, South Africa was rated largely compliant with the former R.27. The identified defect was an absence of proven effectiveness.

Criterion 30.1 – (*Met)* The SAPS:DPCI, is responsible for the investigation of ML, TF, and serious predicate offenses. It is mandated to prevent, combat, and investigate "national priority offenses". These include serious organized crime, serious commercial crime, serious corruption, terrorism, TF, and ML (SAPS Act, ss.16(1)-(2), and 17B). The SARS is responsible for investigating tax and customs offenses and under an MOU works with the SAPS and the NPA if charges are laid.

Criterion 30.2 – (*Met)* SAPS:DPCI investigators are authorized to pursue ML and TF investigations during PFIs of serious predicate offenses, and when evidence is found of other offenses may extend the investigation to those other offenses (SAPS Act, s.17D(2)). All investigators within SAPS specialist units can also pursue basic ML investigations when investigating predicate offenses. Matters are referred to the SAPS:DPCI and assistance is sought from external forensic experts when more sophisticated predicate offenses or ML schemes are involved. The SARS refers tax and customs cases to SAPS:DPCI for follow up ML investigations. VAs may also be pursued during PFIs; see c.30.3.

Criterion 30.3 – (*Met)* The SAPS:DPCI and the NPA:AFU have operational capabilities to identify and trace property and the NPA:AFU may initiate proceedings for the restraint and confiscation of proceeds of crime. The NPA:AFU and the courts regard applications for seizure as inherently urgent and *ex parte* applications are brought on an urgent basis dispensing with the uniform rules of court. Orders can be obtained immediately upon the filing of the application in court. All divisions within SAPS, all other state entities and organizations and persons outside government can refer matters to the NPA:AFU for consideration to proceed with either ch.5 POCA (conviction based) restraint or ch.6 POCA (non-conviction based) preservation orders. As discussed in c.3.4, property covers VAs.

Criterion 30.4 – (*Met)* The SIU is mandated to investigate all allegations involving serious malpractices and maladministration in connection with the administration of State institutions (including fraud and corruption), to collect evidence, and to institute and conduct civil proceedings in a Special Tribunal or any court for any relief to which the State Institution concerned is entitled (SIU Act, s.4). The SIU as a civil recovery unit investigates, inter alia, cases of theft of public monies and institutes civil action in a bid to recover such monies. It may refer evidence pointing to the commission of an offense to the relevant NPA. It does not have power to seize or freeze assets and initiates such matters by referring them to the NPA:AFU.

Criterion 30.5 – (*NA)* Corruption cases are investigated by SAPS:DPCI. The SIU is not designated to investigate corruption offenses or ML/TF offenses arising therefrom.

Weighting and Conclusion

Recommendation 30 is rated compliant.

Recommendation 31 - Powers of Law Enforcement and Investigative Authorities

In its previous MER, South Africa was rated compliant with the former R.28.

Criterion 31.1 – (Met)

a) *(Met)* SAPS:DPCI, (the competent authority for investigating ML and TF), may apply for a subpoena requiring any person likely to give material or relevant information for an alleged offense including a predicate offense to appear and be examined by a public prosecutor (CPA, s.205). The person can avoid having to appear in person by giving the information or material to the prosecutor in advance. This is the main provision used to compel production of bank records. For the purpose of investigating customs and excise offenses, SARS officers have wide ranging powers including entering premises with a warrant, or without a warrant in certain circumstances, to conduct an inspection, examination, enquiry or search including the production of books and documents and taking copies (C&E Act, s.4(4)). The SARS also has criminal investigative powers for the purpose of the administration of the tax Acts listed in Sch 1 of the SARS Act (TAA, s.3(2)(f)). The SARS may compel production of bank records without judicial authorization: s.46 TAA. The national DPP may request any information from a Government Department or statutory body that may be reasonably required for any investigation in terms of the POCA (POCA, s.71) and to direct a DPP to institute an investigation in terms of the NPA Act, ch.5 with powers to conduct examinations and require production of documents (POCA, s.72). An NPA Investigation Director may also compel a person to appear at an inquiry to be questioned and to produce documents relevant to the inquiry (NPA Act, s.28).

b) *(Met)* SAPS may apply for search warrants to seize articles from persons and premises (CPA, ss.20-21). Articles may also be seized without a warrant in defined instances (CPA, s.22). SARS officers may also enter premises with a warrant, and in certain instances without one, when investigating customs offenses to search for evidence (C&E Act, s.4(4)). The SARS can also obtain a warrant to enforce production of banks records for the purpose of administration of the tax Acts if their prior request for production of the records has not been complied with, (TAA, s.46). The national DPP may direct that a DPP institute an investigation in terms of the NPA Act, ch.5 with powers to conduct searches of premises (POCA, s.72) The SAPS additionally has search and seizure powers under the SAPS Act, s.13, and other statutes such as the Precious Metal Act, s.16**.** An NPA Investigating Director may search for and seize anything which has a bearing on an investigation s/he is conducting (NPA Act, s.29). The SIU can conduct searches of premises and seize books, documents, or

objects relevant to an investigation of any predicate offense within the terms of the President's Proclamation (SIU Act, s.6). The SIU refers all criminal matters to the NPA (SIU Act s.4(2)).

c) *(Met)* SAPS has the power to take witness statements in the course of investigating criminal offenses, derived from its Constitutional mandate to investigate crime and its authority to exercise powers and perform duties (SAPS Act, s.13). The subpoena mechanism of the CPA can be used to compel a witness to give a statement (CPA, s.205). NPA Investigating Directors can also obtain statements from witnesses in respect of specific investigations they undertake (NPA Act, s.28).

d) *(Met)* See c.31.1(b).

Criterion 31.2 (Met)

a) *(Met)* Police traps and undercover operations may be used subject to DPP approval (CPA, s.252A).

b) *(Met)* Video surveillance and interception of communications may be utilized (Regulation of Interception of Communications and Provision of Communications-related Information Act 2002, ss. 16-19).

c) *(Met)* See c.31.2(b).

d) *(Met)* Controlled deliveries may be used subject DPP approval (CPA, s.252A).

Criterion 31.3 – (Met)

a) *(Met)* The FIC may request an AI, RI, and other persons to provide certain types of information, including whether natural or legal persons hold or control accounts at the institution (FIC, s.27). The AI must, without delay, give the FIC all reasonable assistance in the exercise of its powers (FIC, s.27(4)). The response time is stipulated in all FIC requests and the usual turn-around time is 2 to 7 working days. The information can be used to further direct the investigation by LEAs. SAPS may also obtain information under the subpoena mechanism (CPA, s.205). The person must appear and produce the material or information to the prosecutor on the date specified in the subpoena, although avoid the necessity of appearing in person.

b) *(Met)* The NPA:AFU has access to various sources of information, such as credit bureau information, to identify assets without prior notification to the owner and may make *ex parte* applications to court to restrain property without prior notification to the owner. The SARS has similar powers in respect of the obtaining of information and seizure of assets in connection with possible tax offenses: s. 3(2) & 46 TAA.

Criterion 31.4 – (*Met)* Competent authorities (the SAPS, the NPA, the SARS) may seek information held by the FIC (FIC Act, s.40). The SIU may also seek information from the FIC in the course of investigations it is mandated to undertake. The FIC Act, s.40(1), lists the agencies that the FIC can share information it holds, including for ML and TF purposes.

Weighting and Conclusion

Recommendation 31 is rated compliant.

Recommendation 32 – Cash Couriers

South Africa was rated partially compliant with the former SR. IX. The primary concerns were that BNIs payable in foreign currency were not covered; there were insufficient records kept; there was not enough information available to the FIU; the sanctions for failing to report cross-border cash movement were not in force, and; there were effectiveness concerns.

Criterion 32.1 – *(Partly Met)* Any person entering or leaving must declare goods in their possession that are prohibited, restricted, or controlled under any law (C&E Act, s.15). *'Goods'* includes cash and is broad enough to cover BNIs, however the *ECR* is the act that articulates prohibited, restricted and controlled goods and does not prohibit, restrict or control incoming BNIs payable in foreign currency. It is illegal to send cash through the mail,[27] but not BNIs.

Criterion 32.2 – *(Partly Met)* South Africa implements an oral declaration system at international airports and a simple disclosure system at land crossing and ports for all travelers (option c) carrying amounts above a certain threshold[28] (C&E Act, s.15, ECR, Reg 3(1)). At airports, once travelers opt for the "red line" they then must complete a written declaration. There is, however, no requirement to declare incoming BNIs payable in foreign currencies.

Criterion 32.3 – *(Partly met)* The disclosure system at land crossings and ports requires travelers to give a truthful answer and provide the authorities with appropriate information upon request. Incoming BNIs payable in foreign currency are not covered.

Criterion 32.4 – *(Partly Met)* Customs officials have extensive powers to question persons and obtain additional information concerning any matter dealt with in the C&E Act, including whether goods are being transported in violation of any law (C&E Act, s4(7)). Incoming BNIs payable in foreign currency are not covered.

Criterion 32.5 – *(Partly Met)* Non-declaration can result in a fine of R8,000 ($544), or treble the amount not declared, or imprisonment of 2 years or both (C&E Act, s.81). False declarations can result in a fine of R40,000 ($2,720)(or treble the amount in question) or imprisonment of 10 years or

[27] C&E Act of 1933 as well as the ECR, Reg. 3(1)(a) and (b).

[28] R25,000 or the equivalent of $10,000 in foreign currency

both (C&E Act, s.84). These sanctions are proportionate and potentially dissuasive. Incoming BNIs payable in foreign currency are not covered.

Criterion 32.6 – *(Not Met)* The SARB:FinSurv provides the FIC with all cross-border transactions for EFTs to and from South Africa. This information, however, does not contain information of declarations of physical transportation of cash nor information regarding suspicious incidents of such transportation.

Criterion 32.7 – *(Partly Met)* While the OR Tambo International Airport (ORTIA) has a Joint Operational Centre which operates 24/7 and is the coordination hub for any incidents which need an immediate multi-disciplinary tactical level approach to crime or other security related incidents (the SARS:Customs works with the SARS:Criminal Investigations, the SARB, the SAPS:DPCI(Serious Commercial Office), and the NPA in dealing with currency or high value items), this is not replicated at all entry and exit points of the country and it does not constitute domestic level, co-ordination among customs, immigration and other related authorities on issues related to the implementation of R.32.

Criterion 32.8 – (Met)

a) & (b) *(Met)* Goods can be seized and held to determine whether the C&E Act or any other law[29] have been complied with in respect of such goods (C&E Act, s.4(8A)(a));

Criterion 32.9 – *(Partly Met)* The authorities can disclose information pursuant to international agreements in respect of mutual administrative agreements and cooperation or exchange of information in customs matters as well as any other international agreement which is in place and binds the Republic of South Africa in terms of s.231 of the Constitution (C&E Act, s.50). The authorities report that records of declarations that are made are kept electronically in a Passenger Processing System (PPS). During the onsite authorities demonstrated how declarations which exceed the prescribed threshold for ZAR are captured in the system. However, they did not indicate:

- how or if a declaration which exceeds the prescribed threshold in another currency is captured in the PPS.
- how or if false declarations (including non-declarations) are captured in the PPS.
- what the process is for filing reports pertaining to suspicions of ML/TF related to R.32 and how or if these suspicions are captured in the PPS.

Criterion 32.10 – *(Met)* The following laws ensure strict safeguards against improper use of information collected through the declaration system, without restricting either: (i) trade payments between countries for goods and services; or (ii) the freedom of capital movements:

[29] This would include the suspicion of ML or TF.

- C&E Act, s.4(3);
- Tax Administration Act of 2011 (ch.6); and,
- Protection of Personal Information Act 2 of 2013

Criterion 32.11 – *(Mostly Met)* Penalties related to non-declaration (C&E Act, s.81) and false declarations (C&E Act, s.84) in respect of certain goods related to C&E, s.15 are described in c.32.5. In addition, persons carrying currency related to ML or TF can be charged and sanctioned under the POCA or the POCDATARA (see Recs.3 & 5). Customs officials have extensive powers to seize and confiscate goods being transported in violation of the *Act* or any other law (Customs Control Act, ch.34 and ECR, Regs (30&(6). Incoming BNIs payable in foreign currency are not covered.

Weighting and Conclusion

Gaps in the regime pertaining to incoming BNIs payable in foreign currency. The documentation within the PPS is not comprehensive nor routinely made available to the FIC or LEAs.

Recommendation 32 is rated partially compliant.

Recommendation 33 – Statistics

South Africa was rated partially compliant on statistics (former R.32) in the 2009 MER. The main deficiencies were related to the lack of comprehensive data or statistics on ML investigations, criminal sanctions imposed, the number of cases and the amounts of property frozen, seized, and confiscated for ML and TF, cross border transportations of currency and BNI over the thresholds, and MLA and extraditions.

Criterion 33.1 – (Mostly Met)

a) *(Met)* The FIC keeps statistics on STRs received as well as intelligence products derived from STRs disseminated proactively and responsively.

b) *(Met)* The NPA, through its AML Desk, maintains statistics on ML investigations, prosecutions, and convictions. The NPA:PCLU maintains statistics on TF investigations, prosecutions, and convictions.

c) *(Met)* The NPA:AFU maintains statistics on property frozen, seized, confiscated, and recovered through forfeiture, which includes those in virtual currencies in a recent case.

d) *(Mostly Met)* DoJ&CD maintains statistics on number of MLA requests made and received. The FIC, the SAPS:DPCI, and the FSCA also maintain statistics on incoming and outgoing requests for international cooperation. The SARB:PA keeps statistics only on incoming requests. There is no evidence that other authorities do so.

Weighting and Conclusion

The authorities maintain statistics in most required areas.

Recommendation 33 is rated largely compliant.

Recommendation 34 – Guidance and Feedback

In its previous MER, South Africa was rated partially compliant with former R.25. The previous MER found that AML/CFT guidance, had not been issued for casinos (or DPMS, or trust and company service providers that are not attorneys or accountants, although these sectors are not subject to national AML/CFT requirements).

Criterion 34.1 – (Mostly Met)

- *Guidance:* The FIC can give guidance to any person regarding their performance and compliance with their duties and obligations related to the Act (FIC Act, ss.4(c) and (cA)) or that will assist them in meeting requirements to freeze property and transactions pursuant to UNSCRs. Most guidance issued by FIC is contained in dual purpose documents – containing some aspects that are considered binding (i.e., enforceable means) and others which provide more general guidance on implementation. See for example, GN7 on implementing the FIC Act, GNs on CDD, reporting of suspicious and unusual transactions, and CFT, and various public compliance communications (PCCs) all available on the FIC website. The FIC guidance tends to be of general applicability, policy orientated, and may not provide enough sector specific details for all AIs and RIs. While FIC is the central body that publishes AML/CFT guidance, that guidance is usually developed in consultation with the other main supervisors. In addition, some other supervisors have also issued communications to their sectors to assist in compliance. All supervisors, except the LPC, have provided guidance during AML/CFT outreach activities with their sectors.

- *Feedback*: Most supervisors (except the LPC which has not conducted any AML/CFT supervision) provide feedback to their firms following onsite inspections. and via outreach programs mentioned above. The FIC also provides industry level feedback on reporting.

Some FIs and DNFBPs are yet to be captured by the AML/CFT system beyond reporting (see c.1.6), the guidance available for them is limited to the aspect of reporting obligations.

Weighting and Conclusion

FIC issues a broad range of guidance for most AML/CFT obligations that has general applicability and may not provide enough sector specific detail to assist all AIs and RIs to apply national AML/CFT measures. Nearly all supervisors provide feedback and FIC provides industry level feedback on reporting. Guidance for sectors that are yet to be captured by the AML/CFT system beyond reporting is limited to the aspect of reporting obligations.

Recommendation 34 is rated largely compliant.

Recommendation 35 – Sanctions

In its previous MER, South Africa was rated partially compliant under former R.17. The main deficiencies were that only criminal sanctions applied for FIC Act breaches and there was no authority for supervisors of the banking and securities sectors to apply administrative sanctions for such breaches.

Criterion 35.1 – (*Mostly Met)* South Africa has a range of proportionate and dissuasive civil and administrative sanctions available for dealing with breaches of AML/CFT requirements. These sanctions range from directions to take remedial actions, business restrictions, suspensions, financial penalties to custodial sentences.

- *TFS (R6):* Failure to report property associated with terrorist and related activities and financial sanctions pursuant to UNSCRs is an offense and the penalty is a fine up to R100 million ($6.8 million) or a sentence not exceeding 15 years, or both (FIC Act, s.51A).

- *NPOs (R8):* There are no applicable sanctions (see c.8.4(b)).

- *Preventative measures and reporting (R 9 to 23):* Administrative sanctions can be imposed on any persons' compliance failures related to the FIC Act (see c.26.1, c.28.2 and FIC Act, s.45C). The sanctions include: a caution; a reprimand; a directive to take remedial action or be instructed to make specific arrangements, to restrict or suspend certain business activities, and a financial penalty up to R10 million ($680,000) for a natural person and R50 million ($3.4 million) for a legal person. The FIC Act also details criteria on how those administrative sanctions should be calculated and considered. These sanctions are applicable to some FIs and DNFBPs only for non-compliance with the reporting requirements (see c.1.6 and R.20). In addition, criminal penalties of imprisonment up to 15 years or a fine up to R100 million ($6.8 million) are applicable for failure to submit a suspicious report to the FIC (FIC Act, ss. 52 & 68). Additionally, "willful" non-compliance with the FIC Act may also be subject to investigation under the POCA or the POCDATARA.

Criterion 35.2 – (*Mostly Met)* Administrative sanctions discussed under c.35.1 can be imposed on directors or senior management for failure to ensure compliance of an AI with the FIC Act (s.61B). The penalties discussed under c.35.1 also apply to these individuals. These sanctions, however, are not applicable some FIs and DNFBPs (see c.1.6). In addition, the SARB:PA and the FSCA may remove a person from a specified position or function when the person has been involved in financial crime (FSR Act, s.145). Failure to report a suspicious or unusual transaction, or property associated with terrorist or financial sanctions pursuant to UNSCRs constitute a financial crime (FSR Act, s.1; FIC Act, ss.51A & 52). These latter actions are not applicable to ADLAs, the FIs that are not AIs (see c.1.6) public FIs, or DNFBPs.

Weighting and Conclusion

South Africa has a range of administrative, civil, and criminal sanctions to deal with natural and legal persons that fail to comply with the AML/CFT requirements, notably in the FIC Act. For sectors not

captured as AIs in the AML/CFT regime (see c.1.6), these are only applicable to non-compliance with reporting requirements and cannot be applied to their directors or managers.

Recommendation 35 is rated largely compliant.

Recommendation 36 – International Instruments

In its previous MER, South Africa was rated largely compliant with the former R.35. The technical deficiency identified was that the POCA, s.6 (dealing with the acquisition, use and possession) did not apply to the person who committed the predicate offense and is inconsistent with Articles 6(1)(b)(i) and 6(2)(e) of the Palermo Convention.

Criterion 36.1 – (*Met)* South Africa acceded to the Vienna Convention on December 14, 1998, ratified the Palermo Convention on February 20, 2004, ratified the Merida Convention on November 22, 2004, and ratified the TF Convention on May 1, 2003.

Criterion 36.2 – (Mostly Met) The POCA, s.6 still does not cover the perpetrator of the predicate offense. It states that "Any person who, acquires, uses or has possession of, property and knows or ought to have known that it forms part of the proceeds of unlawful activities of another person, shall be guilty of an offence." Reference to another person excludes the perpetrator. The Vienna and Palermo conventions are not fully implemented.

Weighting and Conclusion

South Africa has implemented the international conventions save for the minor deficiency relating to c.36.2.

Recommendation 36 is rated largely compliant.

Recommendation 37 - Mutual Legal Assistance

In its previous MER, South Africa was rated largely compliant with what was then R.36. Two deficiencies were identified, being that the enforcement of foreign restraint orders may be made only when such orders are not subject to review or appeal and that a person subpoenaed to give evidence has to appear in person and cannot provide the evidence prior to the date of hearing and be excused from attending at court.

Criterion 37.1 – (*Mostly Met)* South Africa has the legal basis for the provision of a range of MLA under the International Cooperation in Criminal Matters Act (ICCMA), which authorizes MLA to be provided in relation to requests for assistance in obtaining evidence from witnesses and producing documents (s.8), requests for assistance in compelling attendance of witness in any state listed in Sch 1 (s.11), requests for execution of a foreign monetary sentence (s.15), and requests for the enforcement of foreign restraint and confiscation orders (ss.20 and 24). There are no specific provisions in ICCMA for the execution of search warrants or for production orders without the attendance of a witness in court, however domestic powers under CPA are available for this purpose

and witnesses can be excused from attending an open court hearing when the information supplied is private and confidential. The DoJ&CD has a target turnaround time of 25 days for the decision about whether assistance is to be given before the request is sent to the relevant competent authority to action. In some instances, the request may fall within the jurisdiction of different Directors of Public Prosecution leading to delay in execution. The NPA must also refer files to relevant executing authorities and can only request status updates. No information is available on the overall time taken to provide the assistance requested. These structural deficiencies are not consistent with *rapid* provision of MLA.

Criterion 37.2 – (*Partly Met)* The DoJ&CD is the central authority for transmitting and executing MLA requests. The processes to follow are set out in the ICCMA, however without time frames, and the authorities have not established that they use a case management system to monitor progress of requests. The DoJ&CD mechanism monitors compliance with a 25-day period for deciding about whether to execute the request, but not the overall time taken for execution. The process gives no indication that the requests are prioritized in any way.

Criterion 37.3 – (*Mostly Met)* The Minister of Justice's has authority decide on whether a request should be approved. The ICCMA does not place any unreasonable or unduly restrictive conditions on the provision of MLA. However, the reasons for refusing extradition equally apply to a request for MLA (Extradition Act No 67 of 1962, s.11(b)(IV)). It provides that *"a person shall not be surrendered if [the Minister] is satisfied that the person concerned will be prosecuted or punished or prejudiced at… trial in the foreign State by reason of… gender, race, religion, nationality or political opinion".* These grounds are not unreasonable as they relate to constitutionally entrenched human rights. The other grounds for refusal or limitation of MLA are found in specific articles of the treaties that South Africa signed with different countries[30] and SADC Protocol on MLA in Criminal Matters. These treaties provide for the refusal of MLA if the request relates to a political offense, an offense solely under military law, the request would prejudice national security or is not in compliance with the provisions of the treaty. When there is a request by a foreign country for execution of a foreign sentence of fine under the ICCMA, s.15(1), which the Minister may refuse if satisfied that the person upon whom the sentence was imposed would not have been ordered to be surrendered under South Africa extradition law had a request for the person's extradition been made. This exception to the general rule is considered a minor deficiency.

Criterion 37.4 – (Met)

a) *(Met)* South Africa does not refuse requests for MLA on the basis that the offense involves a fiscal matter.

b) *(Met)* South Africa does not refuse requests for MLA on the grounds of secrecy or confidentiality requirements on FIs and DNFBPs.

[30] The USA, the Hong Kong Special Administrative Region of the People's Republic of China, and Argentina.

Criterion 37.5 – (*Partly met)* The ICCMA does not make provision for confidentiality for MLA requests. However South Africa has included confidentiality clauses in all the MLA Agreements that it has signed. The authorities assert that all MLA requests are treated as confidential including requests based on reciprocity in the absence of a treaty, but this has not been corroborated.

Criteria 37.6 and 37.7 – (*NA)* Not applicable as dual criminality is not a pre-requisite or requirement for the rendering of MLA in terms of the ICCMA.

Criterion 37.8 – *(Met)* The SAPS can use all its investigative powers and techniques in response to a MLA request**.**

Weighting and Conclusion

South Africa possess a legislative regime for processing MLA requests under ICCMA and can also use its domestic investigative powers in response to MLA requests. However, there are minor shortcomings relating to the issue of confidentiality and the absence of a case management system that would help keep case records and provide speedy updates on case progress.

Recommendation 37 is rated largely compliant.

Recommendation 38 – Mutual legal Assistance: Freezing and Confiscation

In its previous MER, South Africa was rated largely compliant. The deficiency was that foreign restraint orders are only enforced where the order is not subject to review or appeal.

Criterion 38.1 – (Mostly Met)

a) and *(b) (Mostly Met)* The ICCMA provides for registration of foreign restraint and confiscation orders (ch.4). The orders are not limited to specific offenses and cover confiscation of property laundered from or proceeds from ML, predicate offenses, and TF. The effect of the registration of a restraint order is that it becomes like an order of the Supreme Court where it is registered, and a confiscation becomes a civil judgment in favor of the State. The person against whom the order is registered may apply to set it aside on certain grounds, including that the foreign order is subject to appeal or review. This is a reasonable condition for enforcement of a foreign confiscation order, but not for a foreign restraint order (unless and until the restraint order is set aside in the foreign jurisdiction). For the identification of laundered property, the LEAs must apply the provisions of the CPA, s.20, which provides for search and seizure of articles which are concerned in the commission or suspected commission of an offense, whether within the Republic or elsewhere or which may afford evidence of the commission or suspected commission of an offense. A senior SARS official may apply for a preservation order on behalf of a foreign jurisdiction which is part to an international tax agreement and where payment is not made it may proceed to apply for confiscation of the property as if the tax was due to the South Africa tax authority and then transmit it to the foreign authority (Tax Administration Act, s.185 read with s.163 of the TA Act').

c) *(Met)* Provision for the seizure of instrumentalities used in the offense is made in the CPA, s.20(a) and for the confiscation of any instrumentality used in the offense upon conviction in s.35.

d) *(Mostly Met)* The seizure of instrumentalities intended for use in criminal activities is covered in the CPA, s.20(c). Section 35 only provides for the confiscation of any instrumentality used in the offense upon conviction.

e) *(Met)* A foreign confiscation order means any order issued by a court or tribunal in a foreign State aimed at recovering the proceeds of any crime *or the value of such proceeds* (s1 ICCMA). A foreign restraint order means an order aimed at restraining any person from dealing in *any* property (s1 ICCMA).

Criterion 38.2 – (*Met)* South Africa can cooperate for non-conviction-based confiscation proceedings by commencing proceedings under the POCA, ch.6. The ICCMA, s.20, also provides for registration of foreign confiscation orders which are final in nature and the definition of foreign confiscation order is broad enough to cover *any* order aimed recovering the proceeds of crime or the value of such proceeds (ICMMA, s.1). Section 20(5)(b) provides for situations where the person against whom the confiscation order is given is not present in the jurisdiction.

Criterion 38.3 – (Met)

a) *(Met)* Authorities indicate that seizure and confiscation actions are coordinated with other countries on a case by case basis.

b) *(Met)* A foreign restraint or confiscation order is treated as domestic order once registered and the property is handled the same way as for domestic cases – see c.4.4. When disposing of property confiscated on behalf of a foreign State, the Director General-Justice may consider any agreement or arrangement entered into with a requesting State and then pay the recovered amount less expenses incurred in connection with the execution of the order (ICCMA, s.21(3)). Property covers VAs.

Criterion 38.4 – (*Met)* The sharing of confiscated property with other countries is permitted (ICCMA, s.21 (3)). South Africa is entitled to recover expenses incurred in connection with the execution of the foreign confiscation order. The Director General: Justice and Constitutional Development may enter into an arrangement with the requesting state on how to share the confiscated property.

Weighting and Conclusion

The legal framework for MLA relating to freezing and confiscation covers most required elements. Minor deficiencies exist in so far as restraint orders can only be enforced if they are not subject to appeal or review and there is no specific provision for confiscation of instrumentalities intended for use.

Recommendation 38 is rated largely compliant.

Recommendation 39 – Extradition

In its previous MER, South Africa was rated largely compliant. The deficiency identified related to effectiveness only.

Criterion 39.1 – (Mostly met)

(Mostly Met) South Africa can execute extradition requests for ML and TF. The definition of extraditable offense covers all relevant predicate offenses (Extradition Act no 67 of 1997, ss.1 & 3). However, South Africa has limited the scope of the offense of TF by exempting from criminality certain acts committed during an armed struggle, (ss.1 (xxvi) (3) and (4) – see c.5.1).

(Partly met) South Africa does not have a case management system and relies on set prescribed times to monitor the progress of each extradition request. The authorities indicate that, where a requesting state indicates that urgent attention is needed, the request is given priority. The authorities have not demonstrated that the extradition process is conducted without undue delay

(Met) The grounds for refusal of extradition requests are not unreasonable and do not impose unduly restrictive conditions on the execution of the request (Extradition Act, s.11 (b)(iv)). In cases where the death penalty applies in the requesting State, extradition will only be granted if assurances are provided the death penalty will not be imposed, or, if imposed, will not be carried out. This is principle is consistent with the rights of persons in South Africa under section 11 of the Constitution.

Criterion 39.2 – (Met)

a) *(Met)* South Africa does extradite its nationals.

b) (NA) This criterion is non-applicable.

Criterion 39.3 – *(Met)* South Africa does not require that for dual criminality to be established the foreign country should place the offense within the same category of offense or denominate the offense by the same terminology. The only requirement is that the offense should be criminalized in both countries and the sentence be at least imprisonment for 6 months or more (Extradition Act, s.1).

Criterion 39.4 – *(Met)* There is a simplified extradition mechanism that allows a magistrate to accept a certificate from the requesting State showing that the requesting State has enough evidence to warrant the prosecution (Extradition Act, s10(2)). This shortens the time it takes to refer the matter to the Minister for consent to the extradition.

Weighting and Conclusion

South Africa meets most of this recommendation's criteria. However, minor deficiencies exist in relation to not being able to execute extradition requests without undue delay, case management is

not in place and the definition of "terrorist and related activities" excludes acts committed in an armed struggle.

Recommendation 39 is rated largely compliant.

Recommendation 40 – Other Forms of International Cooperation

In its previous MER, South Africa was rated as compliant.

General Principles

Criterion 40.1 – *(Mostly Met)* The main AML/CFT competent authorities can provide a wide range of international cooperation for ML, associated predicate offenses, and TF as described below. This they can do spontaneously or on request, but there is no evidence that all competent authorities can cooperate or do so rapidly.

Criterion 40.2 – (Mostly Met)

a) *(Mostly Met)* The main AML/CFT competent authorities can provide cooperation via legislation, MOUs, or agreements. South Africa's constitution provides authority for all government bodies to cooperate based on international agreements. More specifically for some agencies: the SAPS cooperates based on informal cooperation arrangements except where coercive measures must be used. It cooperates with police in SADC countries using the SARPCCO multilateral agreement; the lawful basis for the FIC is discussed in c.40.9; for FSRs[31] in c.40.12; and the SARS has various authorities.[32]

b) *and (c) (Mostly Met)* For most competent authorities, legislation does not state methods to cooperate nor impediments, thus leaving them room to use the most efficient and effective methods and channels to exchange information. More specifically:

- The **SAPS** can also co-operate with LEAs via Interpol which is a secure gateway.
- The **FIC** uses the ESW with other Egmont Group members and also cooperates through goAML and encrypted emails. When dealing with non-members of Egmont, FIC only shares open source information to adhere with Egmont rules. The FIC has signed MOUs

[31] In the context of international information exchange, FSR under the FSR Act means: a) the SARB:PA; b) the FSCA; and c) the National Credit Regulator. Note that it does not include the SARB:FinSurv.

[32] a) Tax Administration Act No. 28 of 2011, ss.3(i), 46, 68(h), 69 and 151; b) Income Tax Act No. 58 of 1962, s.108

Exchange of information between tax administrations is made possible by different legal instruments. See www.sars.gov.za/Legal/International-Treaties-Agreements/Pages/default.aspx for a full list of instruments available to the SARS.

with 91 countries, including 12 non-Egmont members. FIC indicates that it provides cooperation within 15 days at most.

- Any **FSR** can enter into MOUs (FSR Act, s.251(3)(e)). Standard MOU clauses require requests to be in writing and any urgency to be clearly indicated. Oral requests must be followed by a written request that states the assistance required, its purpose, the level of confidentiality, and any need for disclosure to third parties. The SARB transmits confidential information using secure messaging. FI regulators must share information in a secure manner (FSRA, s.252).

No information was provided about how other authorities exchange information.

d) *(Partly met)* Mechanisms to facilitate, transmit and execute requests contained in MOUs may provide for a requester to indicate how urgent the request is, but that does not necessary mean that all requests are prioritized to ensure timely responses. Each request received by FIC is assessed, classified and its priority determined. GoAML is configured to treat TF requests as higher priority with each step to be done within 24 hours; in contrast, "medium" priority cases allow 48 hours per step. The SAPS prioritizes requests based on the seriousness of the offense but this is not always the best way to prioritize as not every serious matter is urgent. No information was provided about how other authorities ensure timely execution of requests.

e) *(Partly Met)* The authorities claim that information received is safeguarded based on their government classification system and also the requesting state's classification is respected and aligned to theirs. They did not provide information to corroborate how all authorities do this. The FIC must safeguard its information (see c.29.6). The SARB:PA has an electronic document repository which controls access to confidential information. There is insufficient information relating to what the other authorities have in place.

Criterion 40.3 – *(Partly Met)* There are no limits for which counterparts the authorities can enter into agreements with. Each sector is guided by its own framework. The FSRs are guided by the FSRA, s.251 and the FIC is guided by the FIC Act, s.40) but the legislation does not have a time frame for concluding agreements. However, the authorities did not demonstrate that information sharing agreements were negotiated and signed in a timely manner.

Criterion 40.4 – *(Mostly Met)* There are no legal provisions compelling the giving of feedback in a timely manner. Most competent authorities can provide timely feedback.

Criterion 40.5 – (Partly Met)

a) *(Met)* South Africa does not impose unreasonable restrictions on providing or exchanging information and requests involving fiscal matters are not a bar to providing information.[33]

b) *(Met)* South Africa does not prohibit the exchange of information on the basis on secrecy or confidentiality (see, for example, FIC Act, s.37 and c.9.1).

c) *(Not Met)* No information was provided about whether South Africa prohibits or places unreasonable or unduly restrictive conditions on provision of exchange of information or assistance if there is an inquiry, investigation or proceeding underway.

d) *(Partly Met)* The FIC and the SARS do not prohibit or place unreasonable restrictions on information exchange based on the nature or status of the requesting counterpart authority. Assessors were not provided information about how other agencies address this criterion.

Criterion 40.6 – *(Partly Met)* For FSRs, there are safeguards to ensure that information exchanged is used for the purpose requested and where there is need for third party disclosure prior permission must be granted for that disclosure (FSR Act, s.251(4)). The same applies to the SARS pursuant to international tax agreements. No information was provided regarding whether similar safeguards are in place for other competent authorities such as LEAs, the NPA, casino and other DNFBP regulators, the CIPC, the Master or the DSD to the extent that they can exchange information.

Criterion 40.7 – *(Mostly Met)* FSRs must apply the same level of confidentiality as they would for domestic records (FSR Act, s.251). Where a state has requested a higher level of confidentiality, the higher level is observed. Confidentiality clauses are standard in MOUs signed by the competent authorities. The FIC must maintain confidentiality and can refuse to provide information if the requesting competent authority cannot protect the information (FIC Act, ss.40(1B) and 41).[34] The SARS has similar obligations (Tax Administration Act, ss.67(1)(a) and 68(1)(h and ch.6). No information was provided regarding whether any other authorities such as SAPS, the NPA, casino and other DNFBP regulators, the CIPC, the Master or the DSD must protect confidentiality or whether agencies other than the FIC can refuse a request if the foreign counterpart cannot protect information.

Criterion 40.8 – *(Mostly Met)* The main AML/CFT competent authorities can conduct inquiries on behalf of foreign counterparts and the standard for exchanging information is the same as for conducting domestic inquiries except in instances where coercive measures have to be applied (for

[33] South Africa has passed legislation, but not brought it into force, that would, in relation to information exchange concerning customs and tax matters, only permit information to be disclosed in circumstances where the international, regional or national interest in disclosure outweighs any potential harm to the person affected by the disclosure(Act 32 of 2014, s.21(f) read with s.23 of Act 31 of 2014).

[34] The FSR Act, s.251(2)(b) limits the disclosure of information provided to the FIC so that an FSR must ensure that the safeguards within which the information provided in respect of the FIC Act, ss.29, 40 and 41, are equally applied when the information is disclosed under the FSR Act.

FSRs and the FIC, see c.40.15; for LEAs see c.40.18). No information was provided regarding whether any other authorities can conduct such enquiries.

Exchange of Information between FIUs

Criterion 40.9 – *(Met)* The FIC has an adequate legal basis to exchange information on ML and associated offenses and TF (FIC Act, ss.3(2)(b), and 40(1)(b) and (1B)).

Criterion 40.10 – *(Met)* The FIC generally provides feedback to foreign counterparts on requests using feedback forms. This they do spontaneously or on request.

Criterion 40.11 – *(Met)* The FIC can share all information reported to it or obtained by it and information generated by its analysis (FIC Act, s.40(1)(b)).

Exchange of Information between Financial Supervisors

Criteria 40.12 to 40.14 – *(Mostly Met)* Any FSR can share regulatory, prudential, AML/CFT and domestically available information with foreign counterparts via agreements (FSR Act, s.251(3)(e)). For FIC as a supervisor see c.40.9. These authorities cover all the types of information referenced in these criteria. However, not all FIs and DNFBPs are regulated or supervised for AML/CFT. This limitation also applies to the other criteria under this heading.

Criterion 40.15 – *(Mostly Met)* Any FSR (except the FIC) can conduct inquiries and obtain information for a foreign counterpart (FSR Act, ss.135(1)(b) and 251(3)€). Bilateral agreements can be used to deal with the participation of foreign counterparts in the inquiry. The FIC when acting as a supervisor can conduct such enquires (FIC Act, s.40).

Criterion 40.16 – *(Mostly Met)* The financial supervisors may not disclose to a third-party information that they received without the consent of the designated authority that provided the information (FSR Act, s.251(4)(d)(ii)).

Exchange of Information between LEAs

Criterion 40.17 – (*Met)* The SAPS can exchange domestically available information with foreign counterparts relating to ML, associated predicate offenses or TF, including to identify and trace proceeds and instrumentalities (which cover VAs within the definition of property). It does this under agreements and Interpol rules. SAPS has entered into 32 agreements with other LEAs. The only limitation is that an MLA request is needed to use coercive measures.

Criterion 40.18 – (Met) The SAPS can use its powers, including the investigative techniques available in their domestic law, to conduct inquiries and gather information on behalf of a foreign counterpart if coercive measures are not involved (see R.31).

Criterion 40.19 – (Met) LEAs can enter into agreements for joint investigations and are not prohibited from forming joint investigative teams but officials from the foreign counterpart do not have investigative powers in South Africa.

Exchange of Information between Non-Counterparts

***Criterion* 40.20 –** (*Mostly Met)* The main AML/CFT agencies can exchange information indirectly with a non-counterpart. In practice, FIC requests are routed through the non-counterpart's FIU. The SAPS can exchange information with foreign intelligence organs, FIUs, FIs and prosecution authorities. Any FSR (but not FIC) may also make agreements for sharing information with any person or institution (FSR Act, s.251 and Banks Act No 94 of 1990, s.4(3) for the SARB:PA). Nothing was provided regarding whether any other authorities can exchange information indirectly.

Weighting and Conclusion

The main AML/CFT competent authorities can provide various forms of international cooperation through agreements and MOUs. However, the following minor deficiencies exist: it is not clear that all authorities can cooperate or that all information can be provided rapidly; it is not established that South Africa exchanges information or assistance when there is an inquiry, investigation or proceeding underway; and the only competent authority which gives feedback is the FIC.

Recommendation 40 is rated largely compliant.

Annex II. Summary of Technical Compliance – Key Deficiencies

Recommendations	Rating	Factor(s) underlying the rating
1. Assessing risks & applying a risk-based approach	PC	• South Africa is yet to conclude its first NRA exercise. • Most authorities that have AML/CFT responsibilities are yet to apply an RBA. • The exclusion of CFIs, credit providers other than money lenders against securities, FinTech companies offering financial services that are not FSPs, DPMS that are not KRDs, accountants (for activities other than providing financial services), and CSPs other than attorneys from most AML/CFT obligations and supervision or monitoring is not based on proven low ML/TF risks.
2. National cooperation and coordination	PC	• South Africa is yet to develop coordinated and holistic national policies on AML/CFT informed by risks identified. • Mechanisms to enable inter-agency cooperation at both policy and operational levels exclude DNFBP supervisors and the CIPC (company registry). • No mechanisms to allow cooperation and coordination to combat the financing of proliferation of weapons of mass destruction. • No evidence of cooperation and coordination between relevant authorities to ensure the compatibility of AML/CFT requirements with Data Protection and Privacy rules and other similar provisions.
3. Money laundering offenses	LC	• A minor shortfall exists for self-laundering (acquisition, possession or use of proceeds does not extend to the perpetrator of the predicate offense)
4. Confiscation and provisional measures	LC	• There is a minor gap for confiscation of instrumentalities intended for use in ML, predicate, and TF offenses.
5. Terrorist financing offense	PC	• Criminalization of TF is significantly narrower than the scope of the TF Convention. • Concern about the proportionality of TF sanctions.
6. Targeted financial sanctions related to terrorism & TF	NC	• Delays in implementing for UNSCRs 1267, 1989, and 1998. • No domestic process for identify or proposing targets for those UNSCRs • UNSCR 1373 mechanism focuses on identified property not all property of designees.
7. Targeted financial sanctions related to proliferation	PC	• Some delays in implementing TFS. • Prohibition does not extend to funds and other assets of persons acting on behalf of, or at the direction of a designated person or entity. • Weaknesses in processes for de-listing.
8. Non-profit organizations	NC	• No assessment to identify those NPOs at risk of TF abuse. • No capacity to monitor or investigate NPOs identified to be at risk of TF abuse.

Recommendations	Rating	Factor(s) underlying the rating
9. Financial institution secrecy laws	LC	• Legal obstacle to information sharing between FIs where required under R.13. 15. or 17.
10. Customer due diligence	PC	• No obligations for CFIs, credit providers other than money lenders against securities, and some fintech companies. • "Beneficial owner" does not extend to a natural person exercising control of a customer who is a natural person; • No requirement to ensure that any other natural person exercising ultimate effective control over a trust must be identified and their identity verified; • No CDD requirements for the beneficiary of life insurance and other investment related insurance policies; • Requirement to apply enhanced measures does not entail higher risk (occasional) transactions, and the application of simplified measures when there is a suspicion of ML/TF or specific higher risk scenarios apply, is not explicitly excluded; • AIs not explicitly permitted not to pursue CDD, when it reasonably believes that performing the CDD process will tip-off the client
11. Record keeping	LC	• No obligations for CFIs, credit providers other than money lenders against securities, and some fintech companies.
12. Politically exposed persons	NC	• No obligations for CFIs, credit providers other than money lenders against securities, and some fintech companies; • The definition of a PEP is limited in time; • International organizations PEPs limited to organizations based in South Africa; • Identified limitations apply to family members and close associates of all types of PEPs; • No clear requirements for AIs to put in place risk management systems to determine whether an existing customer or the beneficial owner becomes a PEP, and to subsequently obtain senior approval for continuing the relationship with such customers.
13. Correspondent banking	LC	• No obligations for CFIs, credit providers other than money lenders against securities, and some fintech companies.
14. Money or value transfer services	PC	• Domestic MVTS are not subject to licensing or registration. • Insufficient action being taken against unlicensed MVTS • Limited circumstances where agents are registered • MVTS need not include agents in their AML/CFT program
15. New technologies	NC	• No obligations for CFIs, credit providers other than money lenders against securities, and some fintech companies. • ML/TF risks relating to new technologies are identified only to a limited extent • AIs not required to undertake ML/TF risk assessments for new products, business practices and technologies nor to take measures to manage and mitigate the risks;

Recommendations	Rating	Factor(s) underlying the rating
		• VAs and VASPs risks not adequately identified, assessed, and understood yet, and no risk-based measures taken • VASPs not required to take AML/CFT measures beyond a general reporting obligation. • VASPs not subject to licensing or registration, nor supervised.
16. Wire transfers	LC	• No obligations for CFIs, credit providers other than money lenders against securities, and some fintech companies. • Minor shortcomings for: verifying originator information with regard to batched transfers, record keeping, and screening wire transfers to comply with international sanctions.
17. Reliance on third parties	NC	• No requirements for AIs to obtain immediately information about outsourced CDD; ensure that copies of data will be available upon request; or to be satisfied that the third party is regulated, supervised, and complies with CDD and record keeping requirements. • No determination about in which countries the third party can be based.
18. Internal controls and foreign branches and subsidiaries	PC	• No obligations for CFIs, credit providers other than money lenders against securities, and some fintech companies. • No requirement for financial groups to implement group-wide programs; • Procedures to screen staff are not required; • Non-core FIs are not required to have an independent audit function; • Mitigation where host country does not permit proper implementation not required.
19. Higher-risk countries	LC	• No obligations for CFIs, credit providers other than money lenders against securities, and some fintech companies.
20. Reporting of suspicious transaction	LC	• Outer limit of 15 days allowed to report after forming suspicion creates an ambiguity that could undermine the requirement to report as soon as possible when a suspicion is formed.
21. Tipping-off and confidentiality	C	
22. DNFBPs: Customer due diligence	PC	• No obligations for CSPs that are not attorneys; accountants (for activities beyond provision of financial services), and DPMS; • Same shortcomings already identified for R.10, R.11, R.12, R.15, and R.17.
23. DNFBPs: Other measures	PC	• No obligations for CSPs that are not attorneys; accountants (for activities beyond provision of financial services), and DPMS that are not KRDs as RIs; • Same shortcomings already identified for R.18 and R.20

Recommendations	Rating	Factor(s) underlying the rating
24. Transparency and beneficial ownership of legal persons	PC	• ML/TF risks of legal persons created in South Africa not fully assessed and identified. • BO information is not always available to competent authorities in a timely manner. • There is limited access to BO information as not all DNFBPs and VASPS are AIs.
25. Transparency and beneficial ownership of legal arrangements	PC	• Professional trustees not required to obtain full information on BO when creating trusts. • AIs not required to obtain BO information for other natural persons controlling a trust. • There is a limited range of sanctions applicable to non-professional trustees.
26. Regulation and supervision of financial institutions	PC	• A few sectors are only subject to reporting requirements and are not monitored for AML/CFT preventive measures • Gaps exist for market entry of certain non-core sectors. • Fit and proper requirements are inconsistent and often not extended to beneficial owners • RB AML/CFT supervision is either at an early stage or does not exist.
27. Powers of supervisors	PC	• Not all supervisors can suspend or withdraw licenses • CFIs, credit providers other than money lenders against securities, and some fintech companies are not subject to most AML/CFT obligations or oversight for compliance
28. Regulation and supervision of DNFBPs	PC	• For all sectors and professions, it cannot be established that adequate controls are in place to prevent criminality from operating. • Supervision for the most part is not risk sensitive • Attorneys not supervised • DPMS, accountants (for activities other than provision of financial services), and CSPs other than attorneys not subject to most AML/CFT obligations and not supervised.
29. Financial intelligence units	LC	• Operational analysis adversely affected by gaps in intelligence holdings due to some DNFBPs not being covered under the AML/CFT framework • Strategic analysis is not specific to identifying ML and TF related trends and patterns.
30. Responsibilities of law enforcement and investigative authorities	C	
31. Powers of law enforcement and investigative authorities	C	
32. Cash couriers	PC	• Gaps in the regime pertaining to BNIs.

Recommendations	Rating	Factor(s) underlying the rating
		• Documentation not comprehensive nor routinely made available to the FIC or LEAs.
33. Statistics	LC	• Not all AML/CFT agencies maintain statistics on international cooperation requests.
34. Guidance and feedback	LC	• Some guidance may not provide enough sector specific detail
35. Sanctions	LC	• No coverage for CFIs, credit providers other than money lenders against securities, some fintech companies, DPMS, accountants (for activities beyond providing financial services), and CSPs that are not attorneys
36. International instruments	LC	• A minor deficiency relating to self-laundering (acquisition, possession or use of proceeds of crime does not extend to the perpetrator of the predicate offense).
37. Mutual legal assistance	LC	• Minor shortcomings relating to confidentiality, the absence of a case management system and timely provision of MLA
38. Mutual legal assistance: freezing and confiscation	LC	• Restraint orders can only be enforced if they are not subject to appeal or review • No specific provision for confiscation of instrumentalities intended for use in criminal activities
39. Extradition	LC	• The authorities have not demonstrated they are able to execute extradition requests without undue delay and there is no case management system in place
40. Other forms of international cooperation	LC	• It is not clear that all authorities can cooperate or that all information can be provided rapidly • South Africa did not establish that it exchanges information or assistance when there is an inquiry, investigation or proceeding underway • The only competent authority which gives feedback is the FIC