

Executive Summary

1. 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

- a) 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.
- b) 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.
- c) 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.
- d) 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

¹ See below for more about the phenomenon described as “*State capture*”.

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.

- e) 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.
- f) 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 remains challenging and efforts to detect and confiscate falsely or undeclared cross-border movement of currency needs substantial improvement.
- g) 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.
- h) 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.
- i) 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).
- j) 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.

- k) 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.
- l) 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

2. 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.

3. 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)

4. 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.

5. 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.

6. 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 owing 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.

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 KRAs as reporting institutions (RIs), accountants (for activities other than providing financial services), and CSPs other than attorneys.

7. 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)***

8. 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.

9. 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 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.

10. 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.

11. 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.)

12. 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.

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

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. 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.

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.

Preventive measures (Chapter 5; IO.4; R.9-23)

20. 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.

21. 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.

22. 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.

23. 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.

24. 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)

25. 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.

26. 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 ADLAs 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.

27. 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.

28. 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.

29. 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)

30. 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)

31. 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 chapter 7).

Priority Actions

- a) 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.

- b) 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.
- c) 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.
- d) 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.
- e) 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.
- f) 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.
- g) 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.
- h) Revise the TFS legal framework to address the major shortcomings identified in R.6 and create robust procedures for implementing UN listings without delay.
- i) 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.
- j) 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.
- k) 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.
- l) 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. Effectiveness Ratings

IO.1 - Risk, policy and co-ordination	IO.2 International co-operation	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	

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

Table 2. Technical Compliance Ratings

R.1 - assessing risk & applying risk-based approach	R.2 - national co-operation 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 organisations	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 - DNFFBPs: Customer due diligence	R.23 – DNFFBPs: 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 DNFFBPs	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 co-operation		
LC	LC	LC	LC		

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