Financial Action Task Force

Eastern and Southern Africa
Anti-Money Laundering Group

Mutual Evaluation Report

Anti-Money Laundering and Combating the Financing of Terrorism

26 February 2009

South Africa

South Africa is a member of the Financial Action Task Force (FATF) and of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG). This evaluation was conducted by the FATF and ESAAMLG and then was discussed and adopted in the FATF Plenary as a 2nd mutual evaluation on 26 February 2009.

TABLE OF CONTENTS

PREFACE

INFORMATION AND METHODOLOGY USED FOR THE EVALUATION OF SOUTH AFRICA

1. The evaluation of the anti-money laundering (AML) and combating the financing of terrorism (CFT) regime of South Africa was based on the Forty Recommendations 2003 and the Nine Special Recommendations on Terrorist Financing 2001 of the Financial Action Task Force (FATF), and was prepared using the AML/CFT Methodology 2004[1]. The evaluation was based on the laws, regulations and other materials supplied by South Africa, and information obtained by the evaluation team during its on-site visit to South Africa from 4-15 August 2008, and subsequently. During the on-site, the evaluation team met with officials and representatives of all relevant South African government agencies and the private sector. A list of the bodies met is set out in Annex 2 to this mutual evaluation report.

2. The evaluation was conducted by an assessment team, which consisted of members of the FATF Secretariat and FATF experts in criminal law, law enforcement and regulatory issues: Ms. Valerie Schilling and Mr. Kevin Vandergrift from the FATF Secretariat, and Ms. Yotsna Lalji from the ESAAMLG Secretariat; Mr. Hay Hung Chun, State Counsel, Criminal Justice Division, Attorney-General's Chambers, Singapore (legal expert); Dr. Michalis Mersinis, Attorney-at-law, Legal Department, Hellenic Capital Market Commission, Greece (financial expert); Ms. Indira Crum, Senior Policy Advisor, Office of Terrorist Financing and Financial Crime, United States Department of the Treasury (financial expert); Mr. Shi Yongyan, Anti-Money Laundering Bureau, People's Bank of China (financial intelligence unit expert); and Mr. Joseph Jagada, Chief Law Officer, Attorney General's Office, Zimbabwe (law enforcement expert). The experts reviewed the institutional framework, the relevant AML/CFT laws, regulations, guidelines and other requirements, and the regulatory and other systems in place to deter money laundering (ML) and the financing of terrorism (FT) through financial institutions and designated non-financial businesses and professions (DNFBPs), as well as examining the capacity, the implementation, and the effectiveness of all these systems.

3. This report provides a summary of the AML/CFT measures in place in South Africa as at the date of the on-site visit or immediately thereafter. It describes and analyses those measures, sets out South Africa's levels of compliance with the FATF 40+9 Recommendations (see Table 1), and provides recommendations on how certain aspects of the system could be strengthened (see Table 2).

[1] As updated in February 2008.

EXECUTIVE SUMMARY

1. Background Information

1. This report summarises the anti-money laundering (AML)/combating the financing of terrorism (CFT) measures in place in South Africa as of the time of the on-site visit (4-15 August 2008), and shortly thereafter. The report describes and analyses those measures and provides recommendations on how certain aspects of the system could be strengthened. It also sets out South Africa's levels of compliance with the Financial Action Task Force (FATF) 40+9 Recommendations (see the attached table on the Ratings of Compliance with the FATF Recommendations).

2. The Republic of South Africa is a developing country located in a region where the economy remains primarily cash-based. It has a first-world banking sector characterised by well established infrastructure and technology, but limited participation (over 60% of the adult population was excluded from any formal financial services in 1994), and a growing demand for financial services. A priority of the Government is to ensure that individuals currently excluded from using formal financial services, particularly potential low-income customers, can access and, on a sustainable basis, use financial services being offered by registered financial services providers and which are appropriate to their needs.

3. Major profit-generating crimes include fraud, theft, corruption, racketeering, precious metals smuggling, abalone poaching, "419" Nigerian-type economic/investment frauds and pyramid schemes, with increasing numbers of sophisticated and large-scale economic crimes and crimes through criminal syndicates. South Africa remains a transport point for drug trafficking. Corruption also presents a problem. However, the South African authorities are committed to pursuing this issue through a range of initiatives such as the introduction of measures to entrench good governance and transparency. Security agencies indicated that the current threat from international and domestic terrorism is low, and will remain to be low for the foreseeable future. Nevertheless, the authorities are vigilant about the concern that South Africa could be used as a transit or hideaway destination for people with terrorist links.

4. The development of AML/CFT systems in South Africa represents work in progress. South Africa has demonstrated a strong commitment to implementing AML/CFT systems which has involved close cooperation and coordination between a variety of government departments and agencies. The authorities have sought to construct a system which uses as its reference the relevant United Nations Conventions and the international standards as set out by the Financial Action Task Force. Since 2003, South Africa has taken numerous steps to address many of the recommendations that were made in its first FATF mutual evaluation report.

2. Legal systems and Related Institutional Measures

5. South Africa has criminalised ML in three separate provisions of the Prevention of Organised Crime Act, 1998 (POCA), which cover the conversion or transfer, concealment or disguise, possession, acquisition of property in a manner that is largely consistent with the 1988 United Nations (UN) Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention) and the 2000 UN Convention against Transnational Organised Crime (Palermo Convention). However, acquisition, possession or use of the proceeds of unlawful activities does not apply to the person who committed the predicate offence. South Africa adopts an "all crimes" approach which covers a range of

offences in each of the 20 designated categories of offences. There is also a broad range of ancillary offences to the money laundering offences. Liability for money laundering extends to both natural and legal persons, and proof of knowledge can be derived from objective factual circumstances. The penalties for money laundering are a fine not exceeding ZAR 100 million or imprisonment for a period not exceeding 30 years. The lack of more comprehensive statistics and data maintained by the relevant authorities means that it is not possible to obtain an accurate picture of the effectiveness of the AML/CFT regime in South Africa.

6. South Africa criminalised terrorist financing in Section 4 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act (POCDATARA). The POCDATARA is comprehensive and criminalises the collection or provision of property with the intention that it be used for the purpose of committing a terrorist act, or by a terrorist organisation or individual terrorist for any purpose. The term property is broadly defined, and there is no requirement that the property actually be used to carry out or attempt a terrorist act, or be linked to a specific terrorist act. Terrorist financing is also a predicate offence for money laundering. A broad range of ancillary offences also apply to the terrorist financing offence. The maximum penalty (which can apply to natural or legal persons) for conviction of a terror financing offence is a fine of R100 million or imprisonment for a period of 15 years. However, the effectiveness of the measures put in place by POCDATARA cannot be assessed as there have been no prosecutions under this provision.

7. The POCA provides for both criminal (conviction based) and civil (not dependent on a conviction) forfeiture. Overall, the confiscation and forfeiture regime is being effectively implemented, with the statistics demonstrating that the value of the proceeds confiscated is high. The Asset Forfeiture Unit (AFU) in the National Prosecuting Authority (NPA) administers and implements the freezing and forfeiture provisions of the POCA which apply to a broad range of proceeds (both direct and indirect) and property of corresponding value. Additionally, the Criminal Procedure Act provides for the search, seizure, forfeiture and disposal of the instrumentalities of crime. Any property which may be subject to confiscation or civil forfeiture may be frozen (restrained) by means of an ex parte application.

8. Provisions in POCDATARA allow authorities to freeze assets pursuant to United Nations Security Council Resolutions S/RES/1267(1999) and S/RES/1373(2001). For S/RES/1267(1999), the President must give notice by proclamation in the Gazette of those who have been designated by the UN Security Council. To date, 63 proclamations have been issued through this process, although no assets relating to designated persons/entities have been located. For S/RES/1373(2001), the National Director of Public Prosecutions may make an ex parte application to a judge in chambers for a freezing order where there are reasonable grounds to believe that the property is related to terrorism. In practice, such a freezing order may be obtained in a matter of hours, is of indefinite duration and may be obtained without commencing a criminal investigation or prosecution in South Africa. To date, the relevant South African authorities have not received a request from a foreign country to freeze assets pursuant to S/RES/1373(2001), so the effectiveness of these procedures remains untested. Although these mechanisms generally meet the technical requirements of Special Recommendation III, better communication mechanisms and guidance are recommended. In addition, the authorities should enhance their monitoring of all financial institutions for their compliance with these obligations.

9. The financial intelligence unit (FIU) of South Africa is the Financial Intelligence Centre ("the Centre") which is an "administrative" FIU under the Ministry of Finance. The Centre is a well-structured, funded, and staffed FIU that is functioning effectively. The Centre became a member of the Egmont Group of Financial Intelligence Units in 2003 and has access to a wide range of financial, administrative and law enforcement information to enhance its ability to analyse STRs. The Centre is also authorised to request additional information from reporting entities and has issued guidance on the reporting obligation and

provides feedback to its stakeholders. Although the Centre has not yet issued any typologies, a unit was recently established for the purpose of conducting typologies work.

10. The South African Police Service (SAPS) is the main agency that is responsible for the investigation of money laundering and terrorist financing. The SAPS also has a specific unit in its Detective Service which deals with terrorist offences, including terrorist financing (although, to date, there have been no terrorist financing investigations). Overall, the SAPS appears to be adequately resourced and dedicated to combating money laundering and terrorist financing. Law enforcement authorities have a broad range of investigative powers, including special investigative techniques. Asset Forfeiture Tracing Teams have been established in all the provinces of South Africa. In the five years from April 2003 to March 2008, there were 64 money laundering cases pending before the courts, and 16 resulted in convictions. While South Africa has most of the necessary legal tools and funding to combat money laundering, there is a low number of ML investigations and prosecutions.

11. To implement Special Recommendation IX, South Africa uses a combination of a declaration system and an exchange control regime. Overall, these provisions cover most types of physical cross-border transportations of currency and bearer negotiable instruments (BNI). The exception is incoming BNI payable in any currency and outgoing BNI payable in domestic currency (where the transportation is made by a person) and incoming BNI payable in any currency (where the transportation is made through the mail). Requirements are not yet in place to ensure that cross-border transportations of currency and BNI are reported to the Centre. Although there are sanctions for failing to report cross-border movements of currency, these are not yet in force.

3. Preventative measures – Financial institutions

12. South Africa had implemented AML/CFT preventative measures through the application of the Financial Intelligence Centre Act, 2001 (FIC Act), the Money Laundering and Terrorist Financing Control Regulations (MLTFC Regulations) and Exemptions in Terms of the Financial Intelligence Centre Act (Exemptions). It should also be noted that the FIC Act has been amended by the Financial Intelligence Centre Amendment Act, 2008 (FIC Amendment Act) which will substantially address some of the concerns identified below when it comes into effect in 2009.

13. Financial institutions covered by the FIC Act (so-called "accountable institutions") are prohibited from establishing a business relationship or concluding a single transaction with a customer before establishing and verifying the customer's identity, and the identity of any person acting on behalf of the customer or on whose behalf the customer is acting. Accountable institutions are also required to establish and verify the identity of all customers with whom it had entered into a business relationship before the FIC Act took effect (so-called "existing customers"). The MLTFC Regulations set out in detail the measures to be taken by accountable institutions when establishing and verifying their customers' identities. However, there is no specific requirement in law or regulation requiring accountable institutions to identify or verify the identity of beneficial owners (*i.e.* the natural persons who ultimately own and control the customer). Certain Exemptions fully exempt certain accountable institutions from all CDD requirements (as well as some or all record keeping requirements) in circumstances defined as being low risk, which goes beyond the FATF Recommendations which allow for simplified but not full exemption from CDD. There are no explicit requirements to understand the ownership and control structure of a customer, obtain information on the purpose of the business relationship or conduct on-going due diligence. Likewise, there is no specific requirement that accountable institutions apply enhanced due diligence for higher risk categories of customers, business relationships or transactions, including politically exposed persons (PEPs) or cross border correspondent banking relationships. There is also a scope issue in that a limited number of financial institutions are not subject to AML/CFT requirements.

14. Financial secrecy provisions do not inhibit implementation of the FATF standards. Accountable institutions are required to keep records of information pertaining to customer identification and transactions whenever they establish a business relationship or conclude any transaction. Such records must be kept for at least five years from the date on which the business relationship is terminated (in the case of a business relationship) or transaction was concluded. Nevertheless, effective application of the record keeping requirements is somewhat eroded by some of the Exemptions provisions which exempt accountable institutions from maintaining records of customer identification and verification. Accountable institutions should also be required to maintain account files or business correspondence.

15. Following the last FATF mutual evaluation of South Africa (2003), the Government established a project team to implement changes to South Africa's national payment system (NPS) which would enable full originator information to accompany wire transfers (domestic and cross-border) being transmitted using the SWIFT messaging formats. The system ultimately developed relies on the operating rules and standards that govern the NPS and the contractual obligations among NPS participants to comply. This system is not considered "other enforceable means". Consequently, although there is a legal requirement for accountable institutions to collect and verify originator information, there is no generalised legal requirement that all wire transfers/payment instructions be accompanied by full originator information. However, this approach appears to be generally effective in practice. It should also be noted that these measures can only be effectively applied to wire transfers/payment instructions being processed through the NPS; payment instructions sent through other means (*e.g.* proprietary networks) are not covered.

16. Transactions with no apparent business or lawful purpose must be reported to the Centre. However, accountable institutions are not expressly required to pay special attention to transactions based on complexity, size or unusual patterns, or to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations. There are some mechanisms in place to ensure that accountable institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries, but no specific provisions for accountable institutions to apply counter-measures in situations where countries do not sufficiently apply the FATF Recommendations exist. The recent efforts to inform accountable institutions of the actions taken by FATF are a step in the right direction and should be formalised.

17. South Africa has a broad reporting regime in which all financial institutions and businesses (not just accountable institutions) are required to report suspicious transactions. Overall, the STR reporting regime is being implemented effectively. All suspicious transactions must be reported to the Centre, including attempted transactions, regardless of amount. No criminal or civil action may be brought against a person who files an STR in good faith, and tipping-off is prohibited. During the 2007/08 financial year, the Centre received 24 585 STRs. This is a 15% increase in comparison to the previous year. Additionally, accountable institutions are required to file Terrorist Property Reports (TPRs) with the Centre if they have knowledge that property in their possession or control is terrorist related.

18. Accountable institutions are required to formulate and implement internal rules that address CDD, record keeping and reporting obligations. Accountable institutions are required to appoint a compliance officer who is responsible for ensuring compliance by employees with the FIC Act; however, with the exception of the banking sector, the compliance officer need not be at the management level. Although the FIC Act does not specifically address the issue of an independent, internal audit function, such requirements do exist in some of the separate financial institutions' legislation. There is no general requirement for financial institutions to put in place screening procedures to ensure high standards when hiring all employees. Accountable institutions are required to provide AML/CFT training.

19. South African licensing requirements effectively prevent the establishment of shell banks. However, there is no direct prohibition on financial institutions from entering into, or continuing, correspondent banking relationships with shell banks, and no requirement that financial institutions satisfy themselves that respondent financial institutions in a foreign country do not permit their accounts to be used by shell banks. Additionally, there should be more specific requirements that foreign branches and subsidiaries apply AML/CFT measures consistent with the FATF Recommendations, and apply the higher of either domestic or South African standards, and inform the home supervisor if it is unable to do so.

20. The South African Reserve Bank (SARB) is responsible for supervising banking institutions, and overseeing South Africa's exchange control regime—powers which it exercises through its Banking Supervision Department (BSD) and Exchange Control Department (ExCon). The Financial Services Board (FSB) is responsible for supervising financial advisors and intermediaries including investment managers, the insurance industry, retirement funds, friendly societies, collective investment schemes, exchanges, central securities depositories and clearing houses. The Johannesburg Stock Exchange (JSE) is a licensed exchange and self-regulatory organisation which is responsible for supervising authorised users of the exchange. A limited number of financial institutions are not subject to AML/CFT supervision because they are not defined as accountable institutions pursuant to the FIC Act. As well, there is no designated supervisory authority for the following accountable institutions: Postbank and members of the Bond Exchange.

21. The FIC Act does not provide any of the designated supervisory authorities with specific powers of AML/CFT supervision or enforcement. Consequently, supervisors must rely on their general statutory powers of supervision, as defined by their constituting or other legislation. This raises a concern since, although the SARB, FSB and JSE may rely on their general supervisory powers to inspect financial institutions within their jurisdiction for compliance with the FIC Act, they have no specific authority to sanction violations of the AML/CFT requirements. Although the Centre has no official powers of supervision or enforcement, it has been able to participate jointly with other supervisory authorities in AML/CFT inspections. These issues will be addressed by the FIC Act amendments which come into force in 2009.

22. The designated supervisors determine their inspection regimes using a risk-based approach. The intensity of the inspection is also based on risk. In the banking sector, inspections found that most bank's internal audit functions were robust, although in some cases know-your-customer documentation was not being kept. In the insurance sector, some technical breaches of the AML/CFT requirements were detected (mainly in the areas of ongoing training and examination of staff members, risk rating of clients and identification of PEPs), although in general, insurers had adequate internal rules and procedures to meet the CDD and reporting requirements. In all cases, the designated supervisors followed up to ensure that these deficiencies were corrected. As initial compliance was poor in relation to smaller foreign exchange dealers which are not banks, the ExCon focused on visiting such dealers more frequently.

23. Both legal and natural persons (including directors and/or senior management of a financial institution who are responsible for the institution's contraventions or failures) are liable to criminal sanctions for violating the FIC Act. The maximum penalties for offences relating to violations of CDD, record keeping and reporting requirements are imprisonment for 15 years or a fine of ZAR 10 million. There is no possibility to apply administrative sanctions directly for breaches of the FIC Act. Although the designated supervisors may apply some administrative sanctions, these are not directly applicable for AML/CFT violations and can generally only be applied if those AML/CFT deficiencies rise to the level of undesirable business practices, safety and soundness issues, or fit and proper criteria. This means that the current range of sanctions for breaches of the AML/CFT requirements is not sufficiently broad to be effective, proportionate to the severity of a situation, and dissuasive. Although this is a serious deficiency, it will be addressed when the FIC Amendment Act comes into force in 2009.

24. Prudentially regulated financial institutions are subject to strict licensing requirements, although fit and proper tests do not apply to the directors and senior management of long-term insurers, or all directors of financial service providers and collective investment schemes. Natural and legal persons providing money or currency changing services must be licensed in South Africa. International remittances are tightly controlled by the Exchange Control Regulations, with international remittance providers being licensed authorised dealers (certain banks) and the Postbank. However, no registration/licensing requirements apply to natural or legal persons conducting a purely domestic money/value transfer business.

4. Preventative measures – Designated Non-Financial Businesses and Professions

25. The following designated non-financial businesses and professions (DNFBP) are designated as accountable institutions pursuant to the FIC Act: attorneys (which includes notaries), trust service providers, (real) estate agents, casinos and public accountants who carry on the business of rendering investment advice or investment broking services. AML/CFT preventative measures described above generally apply to all accountable institutions in the same way, regardless of whether they are financial institutions or DNFBP.

26. Although dealers in precious metals and stones are not subject to the CDD and record keeping requirements of the FIC Act (as they are not defined as accountable institutions), the industry is very committed to the Kimberly process, begun under the auspices of the United Nations, which seeks to improve transparency in the diamond trade. Any person can act as a company service provider and there are, in fact, some specialised firms of professionals who provide the vast majority of company registrations. Accountants are only covered to the extent that they can be characterised as providing investment advice or brokering services.

27. The obligations to report activity suspected of being related to money laundering or terrorist financing, protection for reporting and the prohibition on tipping off apply to all DNFBPs. In general, compliance with the reporting requirements has been improving. However, South African authorities should continue working with the dealers in precious metals/stones and real estate sectors to determine whether they are adequately identifying and reporting suspicious activity.

28. The FIC Act designated authorities responsible for supervising certain DNFBP sectors for AML/CFT compliance, but does not provide them with any specific powers of AML/CFT supervision or enforcement. Nevertheless, some of these authorities are using their general powers to conduct AML/CFT inspections. For casinos, the designated AML/CFT supervisor is the National Gambling Board (NGB). For estate agents and public accountants, the designated AML/CFT supervisors are the Estate Agency Affairs Board (EAAB) and the Public Accountants and Auditors Board (PAAB) (now the Independent Regulatory Board for Auditors (IRBA) respectively. However, it should be noted that the IRBA only has the authority to supervise a limited segment of the accounting sector. For attorneys (and notaries), the Law Society of South Africa (LSSA) is the designated AML/CFT supervisor; however, only the four regional law societies have statutory inspection authority and enforcement power to supervise the conduct of attorneys. This situation has stalled implementation of AML/CFT requirements in the legal profession. South Africa should bring into effect as soon as possible provisions that will provide adequate authority for the DNFBP supervisors/monitoring bodies to inspect for and apply a range of sanctions that is effective, proportionate, and dissuasive for non-compliance with the FIC Act.

29. Although the Centre has no official supervisory functions or powers of its own, designated supervisors who wish to have Centre participation may use their general powers to appoint employees of the Centre to their inspection teams. In this way, the Centre has been able to participate jointly with the National Gambling Board in 25 inspections of casinos (October 2007 to April 2008) and with the Estate Agency Board in 21 inspections of estate agents (November 2006 to June 2007).

5. Legal Persons and Arrangements & Non-Profit Organisations

30. In preventing the use of legal persons for illicit purposes, South Africa relies primarily on an investigatory approach, supplemented by a company registry and corporate record keeping requirements. Overall, there are limited measures in place to ensure that there is adequate, accurate, and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. All companies doing business in South Africa, including foreign companies, must be registered in the national company registry — the Companies and Intellectual Property Registration Organisation Office (CIPRO). South African and foreign companies must keep registers of the directors and officers as well as a register of members (shareholders). Shareholders may be natural or legal persons. While there is a duty to disclose the identity of the person on whose behalf the share is being held, that person could be a natural or legal person, this does not capture the FATF's concept of beneficial ownership/control. There are no impediments to accessing the information available. However, information which is available pursuant to the collection mechanisms does not capture accurate and current information on the beneficial ownership and control of legal persons; the information in CIPRO is not verified, and the provisions relating to nominee shareholders may obscure beneficial ownership in the company's share registry. Share warrants to the bearer may also obscure beneficial ownership and control.

31. With regard to preventing the use of legal arrangements for illicit purposes, South Africa relies primarily on an investigatory approach, supplemented by a national trust registration system whereby a national registry records details on trusts, including information on the settlers (founders), trustees and beneficiaries. The registry system is supplemented by record-keeping requirements related to trust accounting. At the time of the on-site visit, the Master of the High Court was in the process of implementing an electronic version of the trust register which is fully searchable. The Registry does not regulate trusts; it is an office of record. Law enforcement officers have timely access to the contents to the files held at the Master's Office and may make a copy of any document in the file. This includes the names of the founders (settlor), trustees, and beneficiaries of trusts. The Trust Registry is a valuable source of current information on trusts; however, steps should be taken to ensure that the information held in the Registry is accurate (*e.g.* verification), and that the remaining paper files are uploaded into the register.

32. The non-profit organisations (NPO) sector in South Africa is well established and is comprised of various voluntary associations, charitable trusts and corporations. Registered NPOs in South Africa must comply with financial disclosure requirements; accounting records must be kept and financial statements together with a report from an accounting officer certifying compliance with the organisation's constitution, its accounting policies and the NPO Act must be filed annually with the NPO Directorate. A registered NPO must preserve each of its books of account, supporting vouchers, records of subscriptions or levies paid by its members, income and expenditure statements, balance sheets and accounting officer's reports for the prescribed period. Nevertheless, registration of NPOs is voluntary, which creates a loophole that increases the risk of abuse of unregistered NPOs by terrorist financiers. South Africa should assess the potential risks of terrorist financing posed within its NPO sector and review the level of oversight measures to ensure that these are effective and proportional to the risk of abuse. More outreach should also be undertaken with the specific aim to protect the NPO sector from terrorist financing abuse.

6. National and International Co-operation

33. South African authorities have established effective mechanisms to cooperate on operational matters to combat ML and FT. The Centre has mechanisms in place to exchange information and coordinate with the various stakeholders, and regulators and law enforcement agencies effectively and to cooperate effectively amongst themselves.

34. South Africa ratified the Palermo Convention on 20 February 2004, and the Terrorist Financing Convention on 1 May 2003, and acceded to the Vienna Convention on 14 December 1998. The vast majority of the convention's provisions have been implemented. South Africa has implemented components of S/RES/1267(1999) and its successor resolutions and S/RES/1373(2001).

35. South Africa adopts a flexible approach in dealing with mutual legal assistance requests, and is able to render a wide range of mutual legal assistance under the International Cooperation in Criminal Matters Act (ICCMA), South Africa is able to render assistance without the need for a treaty or agreement (although South Africa has a number of agreements in place), and there is also no requirement for dual criminality or where the request is to obtain evidence, there is no requirement that judicial proceedings should have already been instituted before assistance can be rendered. Assistance is generally provided on the basis of an assurance of reciprocity, but this principle is not interpreted in an overly strict manner. Neither the ICCMA nor the treaties impose restrictions against requests relating to fiscal matters.

36. The ICCMA provides for the confiscation and transfer of proceeds of crime or property of corresponding value through the execution of "foreign confiscation orders", which are complemented by domestic provisions in the asset forfeiture regime under the POCA, and provisions in the CPA that are used to cover the search and seizure of instrumentalities intended for use in ML, FT and predicate offences.

37. South Africa's extradition framework is comprehensive and flexible. The Extradition Act provides for extradition in respect of "extraditable offences" namely offences in both states that are punishable with a sentence of imprisonment for a period of six months or more. This would include the money laundering offences and terrorist financing offences. There is no requirement for a treaty, and South Africa can also extradite its own nationals.

38. The Centre, law enforcement agencies, and supervisors are able to provide a wide range of international co-operation to foreign counterparts, and generally do so in a rapid, constructive, and effective manner. South Africa does not refuse co-operation on the ground that offences also involve fiscal matters. The provisions and practices apply to all criminal conduct including money laundering and terrorist financing.

7. Resources and Statistics

39. South African authorities have committed substantial and appropriate human and financial resources to the Centre, police, financial supervisors and prosecutors. The NPA has increased its staff by 27% over the past three years, and receives adequate funding but experiences some challenges with attracting and appointing qualified applicants. All competent authorities are required to maintain high professional standards, including standards concerning confidentiality, and receive adequate AML/CFT training.

40. South Africa maintains comprehensive statistics regarding STRs received, analysed, and disseminated, and statistics relating to financial supervisory cooperation. South African authorities should record and maintain more detailed statistics of money laundering investigations, prosecutions and convictions, so as to be able to more effectively assess the effectiveness of South Africa's AML/CFT system. South Africa should also keep comprehensive statistics of mutual legal assistance and extradition matters. Finally, South Africa should review the effectiveness of its systems for combating money laundering and terrorist financing on a regular basis.

MUTUAL EVALUATION REPORT

1. GENERAL

1.1 General information on South Africa

1. The Republic of South Africa is a developing country which occupies the southernmost part of the African continent. The country has a surface area of 1 219 million kilometres and has common boundaries with Botswana, Mozambique, Namibia, Swaziland and Zimbabwe. Completely enclosed by South African territory is the mountain Kingdom of Lesotho. The results of the most recent census, conducted in October 2001, indicate that there were 44.8 million people in South Africa, while the population at present is estimated to be 47.9 million. The currency is the South African Rand (ZAR)[2].

Economy

2. The country's first democratic elections were held following many years of the economy being wracked by internal conflict and external sanctions. The first democratic government inherited a financial sector that had developed within the context of an inward-looking policy environment, with skewed investment opportunities, client focus and ownership and control of companies in the hands of a select few. Years of political and economic isolation resulted in a regulatory structure which had become progressively de-harmonised from international standards. A highly concentrated financial sector provided financial service providers with little incentive to bring down costs for consumers or spur innovation. As a result, a profound mismatch existed between the allocation of capital and the development needs of the country. The key challenge was reconciling the first-world banking sector — characterised by well established infrastructure and technology, but limited participation (over 60% of the adult population was excluded from any formal financial services in 1994) — with the enormous demand for financial services. The Government took a three-pronged approach to address these issues by: encouraging private firms to initiate stalled investment plans; working to bridge the divide between the first and second economies by providing appropriate savings and risk and transactional products; and building a social security net to alleviate poverty.

3. Economic performance since 1994 has been strong. Public finances have been stabilised, inflation declined (until recently), foreign capital was attracted in growing amounts, and economic growth, after lagging for a time, is starting to show impressive improvement. There was some initial improvement in growth performance after the stagnation of the last years of apartheid, but income growth per capita in the first decade of the democratic era was modest. Nevertheless, the economy has grown by 5% per year since 2003. While consumption is presently slowing, public and private investment is strong, and export performance continues to improve. Large investments in electricity and transport, higher spending on maintenance and more appropriate pricing of public services is intended to improve growth prospects and economic efficiency. A government initiative to boost growth rates to an average of 6% per year between 2010 and 2014 is being undertaken with a view to halving unemployment and poverty.

4. The Government continues to work toward bringing unregulated financial activity within the regulated financial system, thereby providing an audit trail of transactions that extend the reach and effectiveness of AML/CFT controls and bring some measure of consumer protection. This means ensuring that individual clients currently excluded from using formal financial services, particularly low-income

[2] At the time of the on-site visit, ZAR 1 = 0.076 Euros (EUR) and EUR 1 = ZAR 13.

clients, can access and, on a sustainable basis, use financial services which are appropriate to their needs and are being offered by registered financial services providers. The South African Government considers the pursuit of financial inclusion and maintenance of the integrity of the financial system, in the form of an effective AML/CFT regime, as being complementary financial sector policy objectives.

System of Government

5. South Africa is a sovereign, democratic and unitary state, divided into nine provinces, each with its own legislature, premier and executive councils: Eastern Cape, Free State, Gauteng, Kwazulu-Natal, Limpopo, Mpumalanga, Northern Cape, North West and Western Cape. The Constitution determines the matters over which the provinces have concurrent or exclusive legislative authority. For example, casinos, racing, gambling and wagering (excluding lotteries and sports pools) is a matter over which the provinces have concurrent legislative authority with the national legislature. The powers of the law-makers (legislative authorities), governments (executive authorities) and courts (judicial authorities) are separate from one another. Parliament — which consists of the National Assembly and the National Council of Provinces (NCOP), and whose sittings are open to the public — is the legislative authority of South Africa, having the power to make laws for the country in accordance with its Constitution. The NCOP represents provincial interests in the national sphere of government and must have a mandate from the provinces before it can make certain decisions. It cannot, however, initiate a Bill concerning money (the prerogative of the Minister of Finance). 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 in the interest of national unity, in accordance with the Constitution and the law. The national government is advised by Traditional Councils — traditional leaders whose status and roles of traditional leadership according to customary law are recognised, subject to the Constitution.

Legal and judiciary systems and hierarchy of laws

6. South Africa has an uncodified legal system, meaning that there is no single primary source where the law originates and can be found. The sources of law are the Constitution; legislation; case law (court decisions); common law; customary law; old writers/authors; and indigenous law.

7. 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. 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 offences such as murder, fraud, robbery and theft).

8. ***Writings of modern authors:*** The sources of Roman-Dutch law, which is the basis for common law, are the writings of the old authorities. These have binding force as a source of law and include: legislation (*placaaten*) – few of these still apply in South Africa; judgments of the Old Dutch courts; and writings of learned authors (the so-called old authorities) such as Hugo de Groot, Voet, and Van der Linden. Many African communities also live according to ***indigenous law***.

9. The ***Constitutional Court*** is the highest court in all constitutional matters and deals only 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). 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.

10. ***High courts:*** There are 10 court divisions and three local divisions which are presided over by judges of the provincial courts concerned. A provincial or local division has jurisdiction in its own area over all persons in that area. ***Regional courts*** established in each regional division have jurisdiction over all offences, except treason. Unlike the High Court, the penal jurisdiction of the regional courts is limited. Magisterial districts are grouped into 13 clusters. By March 2005, there were 366 magistrates' offices, 50 detached offices, 103 branch courts and 227 periodical courts in South Africa, with 11 767 magistrates. A ***magistrate's court*** has jurisdiction over all offences except treason, murder and rape. There are also six ***specialised commercial crimes courts,*** each having two magistrates, which deal with many of South Africa's money laundering cases.

Transparency, good governance, ethics and measures against corruption

11. Anti-corruption efforts remain extremely high on government's agenda. Government departments have been provided with a new guide to establish minimum anti-corruption capacity, including practical examples of successful implementation. The Prevention and Combating of Corrupt Activities Act (2004) strengthens anti-corruption measures, criminalises corruption and corrupt activities, and provides for investigative measures. Public sector entities are required to implement effective, efficient and transparent systems of financial and risk management, internal control and internal audit, under the control and direction of an audit committee (Public Finance Management Act, 1999). They are required to keep full and proper records of their financial affairs in accordance with prescribed norms and standards, and to submit annually to the Auditor General for auditing financial statements, prepared by their accounting officer in accordance with generally recognized accounting practice. Private sector legal persons are required to comply with accounting standards, maintain certain financial information and appoint audit committees of non-executive directors of the company (Companies Act, 1973). Nevertheless, corruption remains an issue.

1.2 General Situation of Money Laundering and Financing of Terrorism

12. South Africa has not yet undertaken any formal ML/FT typologies study at the domestic level. The South African Police Service (SAPS) and the National Prosecuting Authority (NPA) advised the assessment team that the money laundering investigations which have been conducted to date have involved predicate offences of fraud, theft, corruption, racketeering, and gambling. Major profit-generating crimes include precious metals smuggling, abalone poaching, and "419" Nigerian-type economic/investment frauds. Other trends in ML are based on investment frauds through pyramid schemes and fraud cases through fake cheques. Funds are noted to have been laundered through lawyers or other service providers, purchasing of properties, establishment of shell companies and home businesses. The authorities also pointed to an increase in the sophistication and scale of economic crime and crimes through criminal syndicates, although the increasing statistics may be partly due to better detection. South Africa remains a significant transport point for drug trafficking. Corruption also represents a problem. The South African authorities are committed to pursuing this issue through a range of initiatives such as the introduction of measures to entrench good governance and transparency, the establishment of government agencies to investigate and recover funds lost to the State through corruption, passing legislation addressing corruption in the private and public sectors and instituting criminal prosecutions in appropriate cases. Although there is some human trafficking and migrant smuggling, most are economic refugees. Additionally, there is a high level of thefts of citizens' handguns, with some of the stolen weapons presumably destined for resale. Representatives from the private sector noted that foreign workers and refugees in South Africa often use the transportation network (*e.g.* taxi drivers, bus drivers) to physically move cash, mostly from wage earnings, across the border, rather than making remittances through the formal financial sector. The authorities advise that this form of remittance has been used by migrant labour

and has been integral to regional economic development for more than a century, while the cash component is indicative of the extent to which the regional economy remains cash-based.

13. Security agencies indicated that the current threat from international and domestic terrorism is low, and will remain to be low for the foreseeable future. This low risk also applies to the collection/provision of funds for terrorist activities outside of South Africa and the use of South Africa as a conduit for terrorist financing. In 2000, a white supremacist group carried out terrorist activities which had a very limited impact and which is now being prosecuted. The NPA noted that the authorities are vigilant about the concern that South Africa could be used as a transit or hideaway destination for people with terror links.

1.3 Overview of the Financial and DNFBP Sectors

a. Overview of South Africa's Financial Sector

14. South Africa's financial sector is highly developed. Particularly since 1994, the Government has worked to enhance consumer protection and streamline regulation of the financial sector in line with Basel I and II, the FATF Recommendations and the International Organisation of Securities Commission (IOSCO) standards. As a whole, the financial sector has prospered over the last 14 years in line with the growing prosperity and stability of the economy.

15. The Financial Sector Charter, launched in November 2003, signalled a key milestone in achieving greater financial inclusion and transforming the financial sector. It embodied an agreement among the major financial institutions (banks, insurance companies, brokers and exchanges) on a set of service provision and empowerment targets. The Charter foresees broad-based transformation of the sector, based on human-resource development (HRD), procurement and enterprise development, access to financial services, empowerment financing, ownership, control and corporate social investment. Over the past five years, in line with the Charter, the Government has sought to expand access to financial services. Uptake of formal banking and remittance services has increased to 60% of the adult population (as compared to only 26% in 1994). Of the estimated 40% of the total adult population which does not have access to banking services, 80% are African, 41% are women[3], 9% live in rural areas, a further 36% live in tribal lands.

16. One of the key initiatives flowing from the Charter process is the Mzansi account, a low-cost national bank account, launched in October 2004. Mzansi eased the regulatory burden on account holders by requiring only a valid identification (ID) number for account opening. Transactions were initially limited to deposits, withdrawals, transfers (anywhere in the country) and debit card payments. Crucially, no monthly management fees are charged, and typically several free cash deposits per month are allowed. As highlighted earlier the uptake of Mzansi has been significant to date (4.2 million accounts as of November 2007).

17. The following chart shows the types of "financial institutions" (as defined by the FATF) that operate in South Africa and indicates if they are subject to the AML/CFT requirements of the Financial Intelligence Centre Act (FIC Act), and their AML/CFT regulator where one exists:

[3] 2007 Finscope survey.

Financial Activity by Type of Financial Institution			
Type of Financial institutions activity (see the glossary of the FATF 40 Recommendations)	**Type of Financial Institution that performs this activity**	**AML/CFT Requirements (*i.e.* "accountable institutions" under FIC Act?)**	**AML/CFT Supervisor/Regulator**
Acceptance of deposits and other repayable funds from the public	Registered banks Insurance companies accept "deposits" but are exempted from The Banks Act – refer Financial Services Board (FSB). Postbank	Yes Yes Yes	Bank Supervision Department (BSD) of the South African Reserve Bank (SARB)
Lending	Registered banks Also other credit providers – refer National Credit Regulator	Yes No	BSD
Financial leasing	Registered banks Also other credit providers such as financing arms of motor manufacturers.	Yes No	BSD
Transfer of money or value	Registered banks Postbank Informal remittance sectors	Yes Yes No	Exchange Control and BSD of SARB
Issuing and managing means of payment (*e.g.* credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money)	Registered banks Postbank American Express Travelex	Yes	Primarily National Payment System and Exchange Control and to a lesser degree BSD of SARB
Financial guarantees and commitments	Registered banks	Yes	BSD
Trading in Money market instruments (cheques, bills, CDs, derivatives etc.)	Registered banks Securities dealers in respect of derivatives (considered to be securities)	Yes Yes	BSD FSB (JSE Limited (JSE))
Trading in Foreign exchange	Registered banks licensed as Authorised Dealers Other Authorised Dealers with Limited Authority (ADLAs)	Yes	Exchange Control and BSD of the SARB

Financial Activity by Type of Financial Institution			
Type of Financial institutions activity (see the glossary of the FATF 40 Recommendations)	**Type of Financial Institution that performs this activity**	**AML/CFT Requirements (*i.e.* "accountable institutions" under FIC Act?)**	**AML/CFT Supervisor/Regulator**
Trading in Exchange, interest rate and index instruments	Registered banks	Yes	BSD
	Securities dealers in respect of derivatives (considered to be securities)	Yes	FSB (JSE), FSB (Financial Advisory and Intermediary Services (FAIS))
Trading in Transferable securities	Securities dealers	Yes	FSB (JSE)
Trading in Commodities	Registered banks	Yes	BSD
	Securities and commodities dealers	Yes	FSB (JSE)
	Financial Service Providers (FSP)	Yes	FSB (FAIS)
Participation in securities issues and the provision of financial services related to such issues	Registered banks	Yes	BSD
	Securities dealers	Yes	FSB (JSE)
	Financial Service Providers	Yes	FSB (FAIS)
Individual and collective portfolio management	Financial Service Providers	Yes	FSB (FAIS)
Safekeeping and administration of cash or liquid securities on behalf of other persons	Registered banks in respect of safe deposit boxes.	Yes	BSD
	Registered banks as securities depositories	Yes	BSD
	Financial Service Providers	Yes	FSB
	Trustees of Collective Investment Schemes (CIS)	No	FSB
Otherwise investing, administering or managing funds or money on behalf of other persons	Financial Service Providers	Yes	FSB (FAIS)
	Collective Investment Schemes	Yes	FSB (CIS)
Underwriting and placement of life insurance and other investment related insurance	Financial Service Providers	Yes	FSB (Long term Insurance / FAIS)
Money and currency changing	Registered banks licensed as Authorised Dealers	Yes	Exchange Control and BSD of SARB
	Authorised Dealers with Limited Authority	Yes	

18. The following table summarises the types of financial institutions operating in South Africa.

Type of financial institution	Number of Institutions	Total assets	Authorised/Registered/ Supervised by
Registered banks	20	ZAR 3 853m (as of 30 June 2008)	Registrar of Banks, BSD of SARB
Mutual banks	2		
Local branches of foreign banks	14		Registrar of Banks, BSD of SARB
Life Insurance companies	82	ZAR 1 420 billion	FSB
Pension funds managers			FSB
Financial Service Providers – Category I (Brokers)	14 114	N/A	FSB – FAIS
Financial Service Providers – Category II (Investment Managers)	541	ZAR 2 877 665 million	FSB – FAIS
Financial Service Providers – Category III (Linked Investment Service Providers)	25	ZAR 231 660 million	FSB – FAIS
Collective Investment Schemes (CIS) in Securities	41 Managers & 900 Funds	ZAR 658 755 million	FSB
CIS in Property	6 Managers & 6 Funds	ZAR 22 608 million	FSB
CIS in Participation Bonds	7 Managers	ZAR 3 073 million	FSB
Foreign CIS	67 Managers & 383 Funds	ZAR 117 871 million	FSB

19. ***Banking Sector:*** South Africa has a stable and sophisticated banking system. In total, there are 20 registered banks, two mutual banks, 14 local branches of foreign banks, and 43 representative offices. The five largest banks constitute about 90% of the total banking sector assets.

20. ***Long term insurance companies:*** South Africa has 82 registered long-term insurers. In 2007, the net premium income (net of re-insurance) was ZAR 226 billion (EUR 19 billion) with ZAR 234 billion worth of benefits paid during the same period. The five largest insurers accounted for 76% of the South African market, measured by premium income.

21. ***Collective investment schemes in securities:*** There are 900 approved funds available to the public for investment. In 2007, net inflows in collective investment schemes amounted to ZAR 68 billion (EUR 5.6 billion).

22. ***Foreign exchange dealers:*** Authorised Dealers in Foreign Exchange with Limited Authority (ADLAs) are authorised by the National Treasury to deal in foreign exchange for the sole purpose of facilitating travel-related transactions. There are 130 ADLA branches.

23. ***Investment advisers:*** There are 14 568 Financial Service Providers (FSPs) licensed in terms of the Financial Advisory and Intermediary Services Act (FAIS Act): non-discretionary intermediaries, discretionary FSPs, administrative FSPs and hedge fund FSPs. FSP's are any person (other than a representative) who, as a regular feature of their business, furnishes advice and/or renders any intermediary service.

24. ***Securities brokers:*** The JSE Limited (JSE) is licensed as an exchange under the Securities Services Act (2004) (SS Act), to operate four markets: Equities Market, Equity Derivatives Market, Agricultural Products Market and Yield-X. At the end of 2007, the JSE had about 400 listed companies and a total market capitalisation of over ZAR 6 trillion (EUR 499 billion). The total value of assets under the management of all JSE Equities members was ZAR 625 billion (EUR 52 billion).

25. ***Money remitters:*** Cross-border remission of funds may be undertaken by Authorised Dealers in Foreign Exchange — all of which are registered banks — within the context of the exchange control system. Consequently, the AML/CFT framework relating to banks also applies to money remitters. ADLAs may also conduct certain cross-border transactions with immediate effect provided that they can prove compliance with the Cross-Border Foreign Exchange Transaction Reporting System.

26. ***Postbank***: The Post Office Bank (Postbank) is a division of the South African Post Office (SAPO) regulated under the Postal Services Act and the Independent Communications Authority of South Africa (ICASA). Among its products and services, it provides international and domestic money transfers (Money/Postal orders), third party or intermediary services, short and medium term savings accounts, fixed deposit accounts and Mzansi accounts. The Postbank is not a registered bank and is exempt from the Banks Act of 1990. It does not operate as a lending institution, but processes loans through its network on behalf of other institutions, such as Bayport and National Housing Finance Corporation. Postbank is the leading South African financial institution in terms of Mzansi accounts, with a 41% share of the market. Postbank has introduced debit card functionality on 1.2 million Mzansi accounts. At the end of 2007, Postbank issued just over 1 million Visa-branded debit cards to its customers to replace their ordinary automated teller machine (ATM) cards. SAPO has 1 445 post offices and 1 178 postal retail agencies throughout South Africa, and Postbank's services are available at more than 2 000 SAPO post offices/retail postal agencies and 7 200 ATMs of other financial institutions.

27. The National Treasury together with the South African Reserve Bank and the Department of Communications are working on plans to restructure the Postbank with a view to strengthening its corporate governance and hence minimise Government's contingent liability. The discussions between the parties resulted in a concept document and a Memorandum of Understanding ("MOU") signed by the Minister of Finance and the Minister of Communications. The MOU sets out agreed principles and timelines towards the restructuring of the Postbank as an independent corporate entity from the Post Office and into a regulated institution under the Banks Act.

28. ***Ithala Development Finance Corporation Limited (Ithala):*** Ithala was created by the KwaZulu Natal Ithala Development Finance Corporation Act (1999) to promote, support and facilitate social economic development within the KwaZulu Natal Province. It has 46 branches and agencies throughout the KwaZulu Natal Province.

b. Overview of Designated Non-Financial Businesses and Professions (DNFBPs)

29. South Africa has a large, well-established DNFBP sector and the following table summarises the types of DNFBPs operating in the country, the AML/CFT regime to which they are subject and the regulator responsible for overseeing each type of DNFBP:

Sector	Type of DNFBP in South Africa and size of sector	AML/CFT requirements in Domestic Law	Licensing/Registration and AML/CFT oversight
Casinos	36 casinos, ZAR 13.5 billion	Chapter 3 of the FIC Act	Licensed by Provincial Licensing Authorities (PLA). Overseen by the National Gambling Board (NGB).
Real Estate Agents	58 000 estate agents	Chapter 3 of the FIC Act	Registered and overseen by the Estate Agency Affairs Board (EAAB).
Dealers in precious metals and Dealers in precious stones	A total of 598 licenses, certificates and permits issued out of 871 applications between 1 July 2007 and 30 June 2008.[1]	Reporting of suspicious transaction reports (STRs) under Section 29 of the FIC Act.	Overseen by the Diamond Council of South Africa and Jewellery Council of South Africa.
Legal professionals	Approximately 18 189 practicing attorneys, 4 785 candidate attorneys, and 9 162 law firms in South Africa as at 20 May 2008.	Chapter 3 of the FIC Act	The Provincial Law Societies regulate the conduct of attorneys as prescribed in the Attorneys Act, Act 53 of 1979 (the Attorneys Act). The Law Society of South Africa (LSSA) is designated as the AML/CFT authority under the FIC Act.
Accountants	Approximately 25 000 chartered accountants of which 4 174 are Registered Auditors with the Independent Regulatory Board for Auditors (IRBA). Number of firms registered with the IRBA: 1 863 Attest partners: 2 2809 Non-attest partners: 1 365	Chapter 3 of the FIC Act	Accountants: Licensing authority. No regulator for AML/CFT purposes. Registered auditors: IRBA.
Trust and Company Service Providers (TCSP)	Attorneys, Accountants Chartered Secretaries, and other professionals operate as TCSPs.	Attorneys and Accountants subject to AML/CFT requirements of the FIC Act. Other professionals subject to reporting obligations.	See above for attorneys and accountants. Master of the High Court registers trusts. Other professionals not monitored for AML/CFT.

1. Diamond Council/Jewelry Council Presentation to FATF Assessment Team, August 2008, p. 11. In 2006-2007, ZAR12,9 billion in rough diamonds and ZAR 5 billion in polished diamonds were exported from South Africa (*Ibid,* p. 12).

30. ***Casinos***: Only physical casinos currently exist in South Africa, although steps are being taken to allow internet-based casinos to be established. In the financial year 2006/2007, casinos contributed ZAR 13.5 billion (EUR 1.2 billion) in gross gaming revenue to the South African economy.

31. ***Accountants:*** There are about 25 000 chartered accountants in South Africa. Of these, 4 174 are registered with the Independent Regulatory Board of Auditors (IRBA) and therefore authorised to conduct financial audits of public companies.

32. ***Attorneys:*** Statistics for attorneys, candidate attorneys, and law firms are as follows:

Law society	Attorneys	Candidate attorneys	Firms
Cape Law Society – made up of the following provinces: Western Cape, Eastern Cape, Northern Cape	4 858	980	2 541
KZN Law Society	2 545	980	1 461
Law Society of the Free State	890	437	348
Law Society of the Northern Province – made up of the following provinces: Gauteng, Limpopo, Mpumalanga, North West	9 896	2 388	4 812
Total	**18 189**	**4 785**	**9 162**

33. ***Estate agents:*** There are about 58 000 registered estate agents in South Africa who may represent either the buyer or seller of property. Most of the real estate business in South Africa is conducted by 17 large firms.

34. ***Dealers in precious metals and stones:*** South Africa is the fourth largest world producer and exporter of diamonds. Additionally, about 275 tonnes of gold are mined in the country annually, of which about seven tonnes are used domestically for a variety of industrial and commercial uses, including jewellery manufacturing. Jewellery production in South Africa represents 1% of the world market. There are an estimated 3 000 to 4 000 retailers of precious metals and stones, many of which belong to one of the four or five large chain stores operating in the country.

1.4 Overview of commercial laws and mechanisms governing legal persons and arrangements

35. Legal persons may only operate with a profit motive within the context of the Companies Act (1973) (in the case of companies with share capital) or the Close Corporations Act (1984) (in the case of close corporations with no share capital and limited by guarantee). A ***company*** with a share capital can be a public company (*i.e.* the shares are offered to the public) or a private company (*i.e.* the shares are allotted to a limited number of shareholders). Public companies must have at least two directors, while private companies must have at least one. Directors and others directly or indirectly involved in the management of the company can be nominees, but must be natural persons and not be bankrupt, convicted of certain offences (*e.g.* theft, fraud, or forgery), or previously removed as an office for not being fit and proper (Section (s.) 218). Not-for-gain companies are incorporated as companies without share capital.

36. ***Close corporations*** are a simplified form of corporate legal entity with no share capital and a maximum of 10 members (instead of shareholders), each with a "membership interest" (which is expressed as a percentage and represents the member's share in the profits and liabilities of the close corporation). Members can only be natural persons. The exception is that a trustee of a trust may be a member, provided that he/she does not directly or indirectly benefit from the trust. Close corporations do not have directors; all members are responsible for the control of the corporation and may take active part in running the corporation, in accordance with their membership interest.

37. ***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 organised and operated on co-operative principles. Directors must not be of unsound mind, financially insolvent, or have been convicted of certain offences (theft, forgery, etc.) (s.33 Cooperatives Act).

38. ***Legal arrangements*** such as trusts are formed through an agreement between two parties—the founder (settlor) and trustee. The nature of the trust agreement entails that the founder transfers his/her property to the trustee so that the trustee may administer the property for the benefit of a third party beneficiary or beneficiaries. A trust does not have legal personality. Trust instruments must be registered with the regional Master of the High Court.

39. The following chart indicates the number of each type of legal person registered in South Africa:

Type of institution	Total Number of institutions in 2008
Close Corporations	1 735 111
Companies Act Companies	
Public Companies-total	3 521
Listed (domestic)	382
Listed (foreign)	44
Private Companies	450 966
Non-profit companies	20 359
Limited by guarantee	84
Non-profit external (foreign) companies	5
External (foreign) companies	1 113
Incorporated (professionals)	8 911
Company unlimited	6
Cooperatives	3 529

1.5 Overview of strategy to prevent money laundering and terrorist financing

a. AML/CFT Strategies and Priorities

40. The anti-money laundering (AML)/combating the financing of terrorism (CFT) systems in South Africa are relatively young. However, South Africa has demonstrated a strong commitment to implementing the country's AML/CFT systems which has involved close cooperation and coordination between a variety of government departments and agencies. The authorities have sought to construct a system which uses at its reference the relevant United Nations Conventions and the international standards as set out by the Financial Action Task Force. The implementation of legislation against money laundering gained momentum in 1998 with the promulgation of the Prevention of Organised Crime Act and thereafter, the implementation of the Financial Intelligence Centre Act (2001) (FIC Act) and the creation of the financial intelligence unit, the Financial Intelligence Centre (the Centre). In 2004, South Africa approved the Protection of Constitutional Democracy against Terrorist and Related Activities Act (POCDATARA) which, as the overarching national anti-terrorism legislation, criminalises terrorist financing and contains measures to freeze terrorist related funds in line with international obligations. South Africa became a member of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) and the FATF in

August 2002 and June 2003 respectively and provides technical assistance in the region on AML/CFT issues.

41. In September 2007, the Centre, South Africa's financial intelligence unit (FIU) and South Africa's lead agency on FATF matters, published a new three-year strategic plan 2008-2011 that sets out seven strategic outcomes and targets to be achieved as well as indicators that will be utilised to measure the successful attainment thereof for the three year period. The Centre has interpreted its legal mandate as a series of strategic objectives in which it seeks to: *(a)* identity the proceeds of crime and terrorist financing; *(b)* exchange information with law enforcement and other FIUs; *(c)* monitor the compliance of accountable institutions, as well as supervisory bodies in respect of their AML/CFT obligations; *(d)* prevent and reduce ML/FT activities; *(e)* formulate and lead the implementation of AML/CFT policy; *(f)* advise the Minister of Finance in respect of AML/CFT issues; and *(g)* meet and live up to the international obligations and commitments required of the Centre and South Africa as a country.

42. For the past five years, South Africa continued to make good progress in developing and strengthening all its structures and capacity to investigate and prosecute money laundering, and oversee compliance with regulatory measures. For instance, processes are currently underway to enhance the powers and functions of supervisors in the financial and designated non-financial businesses and professions (DNFBP) sectors in relation to their supervision of compliance with the FIC Act. Many of the relevant agencies are focused primarily on building their capacity and capability to combat ML/FT. For instance, the South African Revenue Service (SARS) recently (two years ago) began its current strategy of building capacity to better tackle cash smuggling and the illicit economy. The current priority of SAPS is to combat organised crime, and crimes against women and children. SAPS is also working with the Centre and the Commercial Crime Unit of the National Prosecuting Authority to develop a more unified strategy, with police officers and prosecutors dedicated to building ML cases.

b. The institutional framework for combating money laundering and terrorist financing

(i) Ministries

43. South Africa has a cluster system of government in which various ministries meet to coordinate policy and implementation issues under the leadership of the Presidency. This 'whole-of-government' approach facilitates integrated and coordinated implementation of government policies. This applies equally to AML/CFT issues.

44. ***Ministry of Finance and National Treasury:*** The Minister of Finance is responsible for AML policy measures and issues, supported by the FIU, the ***Financial Intelligence Centre*** (the Centre), which reports directly to the Minister and the ***National Treasury*** which is responsible for broader financial sector regulatory policy. National Treasury leads an inter-governmental committee (the Medium-Term Expenditure Committee), which receives the Centre's strategic and business plans, and recommends allocations on the basis of national priorities and available funds. It is also responsible for approving companies' authority to act as ADLAs. The South African Reserve Bank (SARB) and the Ministry of Finance form the monetary authority in South Africa.

45. ***Department of Justice and Constitutional Development (DoJ & CD):*** DoJ & CD is the ministry responsible for the National Prosecuting Authority (NPA) and is the central authority for administering all mutual legal assistance and extradition matters.

46. ***Department of Safety and Security:*** The Department of Safety and Security houses the South African Police Service (SAPS).

47. ***Department of Foreign Affairs (DFA)***: DFA participates in the United Nations and other international decision-making fora, facilitates mutual legal assistance and international technical assistance. An Inter-Departmental Counter-Terrorism Working Group was formed under the auspices of the DFA to assist South Africa in its obligations regarding United Nations commitments.

(ii) Criminal Justice and Operational Agencies

48. The ***Financial Intelligence Centre (the Centre)*** is South Africa's FIU. It also supports and guides the activities of supervisors concerning compliance with AML/CFT measures, and assists the Minister of Finance with advice on AML/CFT policy matters.

49. The ***South Africa Police Service (SAPS)*** is responsible for the investigation of money laundering cases and all offences pertaining to terrorism. It is constitutionally mandated to: prevent, combat and investigate crime; maintain public order; protect and secure the inhabitants of South Africa and their property, and uphold and enforce the law.

50. ***Special Investigating Unit (SIU)*** works closely with government departments to deal with fraud, corruption and serious maladministration in state institutions. Established by the Special Investigating Units and Special Tribunals Act (1996), it investigates cases referred by the President. It can conduct forensic investigations and institute civil litigation to recover state assets or public money.

51. The ***National Prosecuting Authority (NPA)*** institutes criminal proceedings on behalf of the State, and carries out necessary functions incidental to instituting criminal proceedings (s.179(1) of the Constitution). The NPA structure includes the ***National Prosecuting Services (NPS)*** and other units:

- ***Specialized Commercial Crime Unit (SCCU)*** prosecutes cases arising from crimes investigated by the SAPS Commercial Branch, including money laundering.

- ***Organized Crime Initiative of the NPS Head Office*** prosecutes money laundering cases arising from cases investigated by the SAPS Organized Crime Unit. The regional Directors of Public Prosecutions conduct the prosecutions, while the NPS Head Office manages, assists and supports the prosecutions in the regions on an ongoing basis.

- ***Directorate of Special Operations (DSO)***, commonly known as "the Scorpions," investigates and prosecutes offences relating to trans-national organised crime, serious and complex financial crime, organised corruption and related money laundering.[4]

- The ***Priority Crimes Litigation Unit*** prosecutes all offences under POCDATARA, including terrorist financing.

- ***Asset Forfeiture Unit (AFU)*** implements the freezing and forfeiture provisions in respect of the proceeds and instrumentalities of crime.

[4] At the time of the on-site visit, a process to redistribute the Scorpions functions had been initiated. On 19 November 2008, Parliament approved legislation to incorporate the investigative functions of the DSO into the SAPS. The new unit--the Directorate for Priority Crime Investigation (DPCI) – will be a separate division of the SAPS that will focus on National Priority Offences. Its mandate will be broader than the DSO's and may include specialised commercial crimes such as money laundering, racketeering and terrorist financing.

52. 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), SARS is involved in controlling the movement of people and goods across the border.

53. ***National Intelligence Agency (NIA):*** NIA is responsible for the domestic intelligence and counter-intelligence security, including vetting of Government officials. It also plays a role in investigating terrorism and terrorist financing.

(iii) Financial Sector Bodies — Government

54. ***South African Reserve Bank (SARB)*** and the Ministry of Finance form the monetary authority of South Africa. The SARB also formulates and implements monetary policy and regulates the supply of money by influencing its cost. The following units of SARB are relevant to AML/CFT:

- The ***Bank Supervision Department (BSD)*** supervises banks for compliance with the FIC Act.

- The ***Exchange Control Department (ExCon)*** supervises ADLA branches for compliance with the FIC Act and provides ADLA staff with informal compliance training when necessary.

55. ***Financial Services Board (FSB)*** is an independent regulator responsible for supervising the following for compliance with the FIC Act: the insurance industry, retirement funds, friendly societies, financial advisors and intermediaries, securities investment managers, collective investment schemes and the various exchanges.

56. ***JSE Limited (JSE)*** is responsible for supervising the approximately 188 securities dealers who are members of the exchange for compliance with the FIC Act, Securities Services Act (SS Act) and JSE Rules.

(iv) Financial Sector Bodies — Associations

57. ***Banking Association of South Africa (BASA):*** BASA is an industry body that represents all registered banks in South Africa, including South African and international banks. The BASA's broad role is to "establish and maintain the best possible platform on which banks can do responsible, competitive and profitable banking."

58. ***Life Offices' Association (LOA):*** The LOA is an association of registered long-term insurance companies in South Africa which seeks to promote the interests of the industry and is a forum where member offices can interact to promote their interests, and the interests of current and future stakeholders.

(v) DNFBPs

59. The ***National Gambling Board (NGB)***, established in 1996 pursuant to the National Gambling Act, monitors casinos' compliance with the FIC Act.

60. The ***Provincial Licensing Authorities (PLA)*** in each of the nine provinces are responsible for issuing gambling licences and regulating their casinos for compliance with licensing conditions.

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

62. The ***Diamond and Jewellery Federation*** is an umbrella forum created to discuss issues relating to both the diamond and jewellery industries in South Africa. Its secretariat supports the following industry bodies: the Diamond Council of South Africa and the Diamond Dealers Club whose members include 73 cutting and polishing licensees (52% of the issued licenses nationally), 154 rough diamond dealers (65% of issued licences nationally), and 201 polished dealers; and the Jewellery Council of South Africa, whose members include 192 wholesalers and affiliate members, 996 retailers, and 170 manufacturers.

63. The ***Law Society of South Africa (LSSA)*** is a voluntary body which promotes the common interests of its members and oversees the compliance of lawyers with the FIC Act (even though it has no regulatory powers). Its constituent members are the Cape Law Society (4 858 attorneys and 2 541 firms), KwaZulu Natal Law Society (2 545 attorneys and 1 461 firms), Law Society of the Free State (890 attorneys and 348 firms), Law Society of the Northern Provinces (9 896 and 4 812 firms), Black Lawyers Association, and National Association of Democratic Lawyers.

64. The ***Independent Regulatory Board for Auditors (IRBA)*** is the statutory regulator for the auditing profession. It is responsible for registering auditors in public practice and monitors their compliance with the FIC Act, as provided for under Section 45 read with Schedule 2 of the FIC Act.

65. The ***South African Institute of Chartered Accountants (SAICA)*** monitors its members, who are chartered accountants and auditors, for compliance with the SAICA Code of Conduct which is based on the International Federation of Accountants (IFAC) Code of Ethics. SAICA is a member of IFAC.

(vi) Legal persons and Arrangements and Non-Profit Organisations

66. The ***Companies and Intellectual Property Registration Office (CIPRO)*** registers companies, close corporations, and co-operatives.

67. The ***Master of the High Court*** receives trust instruments from trustees before they assume control of the trust property to be administered, registers inter-vivos trust instruments and issues letters of authorities to the nominated trustee(s) pursuant to the Trust Property Control Act (1988) (TPC Act).

68. The ***Department of Social Development (DSD)*** administers the Non-profit Organisations Act (1997) (NPO Act), which creates an administrative and regulatory framework for non-profit organisations (NPOs), including a voluntary registration facility for civil society organisations.

c. Approach concerning risk

69. The FIC Act makes limited provision for the application of a risk based approach to establishing and verifying customer identity. As a result, financial institutions apply the same standard criteria for new customers as for high risk customers. The Centre has issued guidance to financial institutions concerning the extent to which a risk-based approach can be applied within the current framework. For example, unless an exemption applies, all clients must be identified. However, financial institutions are not required to follow a "one-size-fits-all" approach in the methods and levels of verification applied. A risk-based approach may be applied to the verification of a customer's identity, implying that the greater the risk, the higher the level of verification and more secure the methods of verification should be.

70. Financial sector supervisors (SARB, FSB and the JSE) apply a risk-based approach to supervising the entities under their purview. The SARB (BSD) considers a wide range of risk factors, including quantitative risks (solvency, market, operational, credit, technological) and qualitative risks (corporate governance and AML/CFT). BSD then prioritises those banks considered to be riskier, considers what the riskier areas of each bank are, and plans its inspection cycle accordingly. FSB introduced a risk-based approach to supervising insurance entities in 2007, using a risk matrix that factors

in the size of the entity, market impact, corporate governance, compliance history, financial strength, evaluation of the fit and proper criteria, and any complaints received. The FSB also categorises FSP licensees according to risk and considers several factors including the size of the entity and whether they handle client funds. Finally, JSE also uses a risk-based approach to review those of its members for which it is responsible for supervising compliance with the FIC Act. In particular, the JSE targets the equities market, as those members hold a significant amount of assets (cash and securities) on behalf of clients. See Section 3.10 ("Ongoing Supervision and Monitoring") for more information.

d. Progress since the last mutual evaluation

71. South Africa was first evaluated by the FATF in 2003. The key recommendations made by the FATF at that time are listed below, along with a short description of the action subsequently taken by South Africa. (Note: Paragraph numbers refer to those in the 2003 Executive Summary).

(a) *South Africa must also act swiftly to pass measures in relation to terrorist financing:* In 2004, South Africa approved the Protection of Constitutional Democracy against Terrorist and Related Activities Act (POCDATARA), which criminalises terrorist financing and contains measures to freeze terrorist related funds. STRs related to terrorist financing must now be reported. See Sections 2.2, 2.4, and 3.7 of this report.

(b) *Supervisors may only currently inspect for compliance in accordance with their existing legislation; the ability to use enforcement powers for AML requirements is unclear. Amendments to enabling legislation should be made to provide supervisors to allow them to inspect and sanction for non-compliance with the FIC Act's provisions (paragraph 19):* Amendments to the FIC Act to address this have been approved and received presidential assent on 27 August 2008, although they will only come into force in 2009.

(c) *There is no general duty to identify the beneficial owner. The Regulations also contain a large number of exemptions from the customer identification and record keeping requirements (paragraph 16*): This issue has not been addressed.

(d) *South Africa should make efforts to increase the number of money laundering prosecutions that are brought (paragraph 6)*: The statistics provided continue to show a low number of investigations and convictions for money laundering.

(e) *The Centre and other supervisory bodies need to issue guidelines to assist in the identification of suspicious activities (paragraph 13):* The Centre issued Guidance Note 4 in March 2008, which provides guidance in identifying and reporting suspicious transactions.

(f) *The number of STR from securities and investment firms, and from casinos, was very low (paragraph 14):* STR reporting has increased from securities and investment firms, and casinos. See the statistics in Sections 3.7 and 4.2 of this report.

(g) *There is currently no requirement for this information to remain with the transfer (paragraph 17):* In practice, wire transfers being processed through the Society for Worldwide Interbank Financial Telecommunication (SWIFT) messaging system must contain full originator information (otherwise, the wire will not transmit). However, there is no legal requirement that all wire transfers, including those being processed through other networks (*e.g.* money remitters), contain full originator information.

2. LEGAL SYSTEM AND RELATED INSTITUTIONAL MEASURES

Laws and Regulations

2.1 Criminalisation of Money Laundering (R.1 & 2)

2.1.1 Description and Analysis

Recommendation 1

Offences

72. South Africa has ratified both the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (Vienna Convention) and United Nations Convention Against Transnational Organised Crime, 2000 (Palermo Convention). The Prevention of Organised Crime Act, 1998 (the POCA) which came into effect on 21 January 1999 is the main legislation criminalising money laundering in South Africa. South Africa adopts an "all crimes" approach, which means that the predicate offences for money laundering cover all offences under South African law. These offences would also include the types of predicate offences contemplated in both Conventions. Specifically, Chapter 3 of the POCA creates the following three principal offences relating to money laundering.

Money laundering

73. Section 4 of the POCA provides that a person is guilty of an offence if he or she knows or ought reasonably to have known that property is or forms part of the proceeds of unlawful activities and:

- enters into any agreement, arrangement or transaction with anyone in connection with that property; or
- performs any other act in connection with that property.

Which has or is likely to have the effect:

- of concealing or disguising the nature, source, location, disposition or movement of the property or its ownership or any interest which anyone may have in respect thereof; or
- of enabling or assisting a person who has committed an offence, whether in the Republic or elsewhere to avoid prosecution or to remove or diminish those proceeds of unlawful activities.

74. The elements of this offence are:

(a) **Mens rea:** The defendant knew or reasonably ought to have known that the property is the proceeds of unlawful activity.

(b) **Physical element: Arrangement or transaction.** The accused must have performed an action in relation to the property in question namely to enter into an agreement, arrangement or transaction concerning the property or performed any other action with the property.

(c) **Purpose: Concealment or avoidance of prosecution or confiscation:** As a factual matter the agreement, arrangement, transaction or other action must have had, or be

likely to have, the effect of concealing or disguising the source of the money or its location or ownership, or enabling someone to avoid prosecution or to hide the proceeds of an offence. The latter would include a transaction designed to help a person protect property from confiscation under the forfeiture laws.

Assisting another to benefit from proceeds of unlawful activities

75. Section 5 of the POCA provides that a person is guilty of an offence if he/she knows or ought reasonably to have known that another person has obtained the proceeds of unlawful activities and enters into any agreement with anyone or engages in any arrangement or transaction whereby:

- the retention or the control by or on behalf of said other person of the proceeds of unlawful activities is facilitated; or

- the said proceeds of unlawful activities are used to make funds available to the said other person, acquire property on his/her behalf or benefit him/her in any other way.

76. The elements of the offence are:

(a) **Mens rea:** The defendant knew or reasonably ought to have known that another person has obtained the proceeds of unlawful activity.

(b) **Physical element:** The defendant entered into any agreement with anyone or engages in any arrangement or transaction in respect of such proceeds.

(c) **Purpose:** The retention or control of the proceeds by or on behalf of the other person is facilitated, or the proceeds are used to make funds available to the other person, or to acquire property on their behalf or benefit them in any other way.

Acquisition, possession or use of proceeds of unlawful activities

77. Section 6 of the POCA provides that a person is guilty of an offence if he or she acquires, uses or has possession of property and who knows or ought reasonably to have known that it is or forms part of the proceeds of unlawful activities of another person.

78. The elements of the offence are:

(a) **Mens rea:** The defendant knew or reasonably ought to have known that the property is or forms part of the proceeds of another person's unlawful activities.

(b) **Physical element:** The defendant acquires, uses or has possession of such property.

(c) **Purpose:** There is no need to establish the purpose of such acquisition, use or possession.

79. The money laundering offences in Sections 4 to 6 of the POCA refer to "property" and "proceeds of unlawful activities" which are defined in Section 1 of the POCA.

80. "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.

81. "Proceeds of unlawful activities" 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.

82. "Unlawful activity" in turn is defined as any conduct which constitutes a crime or which contravenes any law whether such conduct occurred before or after the commencement of the POCA and whether such conduct occurred in South Africa or elsewhere.

Consistency with the Conventions

83. The Vienna and Palermo Conventions require that, subject to the fundamental/constitutional principles and basic concepts of their legal systems, countries criminalise the following acts (with the requisite knowledge that the proceeds are derived from a crime):

- the conversion or transfer of proceeds of crime (Article 3(1)(b)(i) Vienna; Article 6(1)(a)(i) Palermo);

- the concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to such proceeds (Article 3(1)(b)(ii) Vienna; Article 6(1)(a)(ii) Palermo); and

- the acquisition, possession or use of such proceeds (Article 3(1)(c)(i) Vienna; Article 6(1)(b)(i) Palermo).

84. In relation to the "conversion/transfer" limb, the Conventions also require that a defendant converted or transferred the proceeds for one of either two purposes: *i)* concealing or disguising its illicit origin; or *ii)* helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his/her action. In the "concealment or disguise" limb, the purpose is self-explanatory, whereas in the "acquisition, possession or use" limb, there is no requirement that the act of acquiring, possessing or using must be for any specific purpose or to achieve any particular objective.

85. Although Section 4 of the POCA does not specifically refer to "conversion or transfer", the words used in the Section – "enters into any agreement or engages in any arrangement or transaction" (Section 4(a)) or "performs any other act in connection with such property" (Section 4(b)) – are wide enough to encompass the acts of conversion or transfer envisaged in both Conventions. The prosecuting authorities also indicated that, in practice, any financial transaction such as making a bank deposit, writing a cheque, or initiating or receiving an electronic funds transfer, or even the simple act of physical transportation of cash would be covered under Sections 4(a) or (b). It should also be noted that Section 4 of the POCA allows for proof in the alternative that the act either "has or is likely to have the effect" of either one of the two purposes identified in the Conventions. The latter alternative ("is likely to have") goes beyond what the Conventions require.

86. Section 4 of the POCA applies to both self and third party money laundering, while Sections 5 and 6 of the POCA are strictly third-party offences. The Conventions do not specifically call for the criminalisation of the offence of assisting another person in the laundering of that person's illegal proceeds in the specific terms as provided in Section 5 of the POCA. In any event, it also appears that Section 5 may in fact overlap with Section 4 given the latter's extensive provisions.

87. However, in respect of Section 6 of the POCA, and to the extent that the acquisition, possession or use of the proceeds of unlawful activities only applies to a third party laundering scenario, there is a gap

in the coverage of the offence since technically, a person who has committed the predicate offence cannot be liable for the acquisition, use or possession of such proceeds.

88. The South African authorities' view is that Section 6 of the POCA does not criminalise money laundering. It is, in fact, an additional offence to Section 4 which can be used against those that are indirectly associated with a money laundering offence and where the facts of the case do not fully support a conviction under Section 4. The authorities were of the view that neither the Vienna nor the Palermo Convention had specified that the acquisition, possession or use limb should also be applicable to the perpetrator of the predicate offence, and that the language in the Conventions suggests that it is meant to deal with someone other than the perpetrator of the predicate offence.

89. Further, the South African authorities also indicated that an additional charge against a perpetrator of an offence under Section 6 would constitute a duplication of convictions which would be contrary to South Africa's constitutional principles and the basic concepts of its legal system and cited the High Court's decision in *McIntyre and Others v Pietersen NO and Another 1998 (1) BCLR 18 (T)*, where the High Court found that the Constitution required protection from duplication of convictions and that as a result of the adoption of the Constitution, South African law relating to duplication of convictions was required to be revisited. The High Court found that whereas prior to the Constitution, the test was whether the description of the offences differed; post-Constitution this test had to be replaced with one based on whether the two offences were based on the same set of facts.

90. Nevertheless, while there may be some force in the argument that the perpetrator of a predicate crime acquires, or comes into possession of, the proceeds of that crime by perpetrating the crime and hence the whole process could be viewed as part of the commission of the predicate crime itself, it still leaves open the issue of "use" in relation to the proceeds. In the context of the POCA, Section 4 will not be applicable if there is no further transaction or arrangement which is 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 to hide the proceeds of an offence. As for the constitutional argument, the assessment team notes that *McIntyre and Others v Pietersen NO and Another* is a High Court decision on the interpretation of the South African Constitution. The decision would not be sufficient confirmation of a constitutional principle absent the pronouncement by the Constitutional Court of South Africa, and in any case it does not specifically relate to the issue of POCA in particular or the issue of self-laundering in general.

91. Therefore, while the money laundering offence in Section 4 of the POCA fully meets the physical and material elements in Article 3(1)(b)(i) and (ii) of Vienna and Article 6 (a)(i) and (ii) of Palermo, the money laundering offence established under Section 6 relating to acquisition, use and possession is largely, though not fully, consistent with Article 6(1)(b)(i) read with 6(2)(e) of Palermo.

Property and conviction for predicate offence

92. The money laundering offences in the POCA extend to any type or form of property, regardless of amount, which represents the direct or indirect proceeds of a crime, or an unlawful act whether committed in South Africa or elsewhere.

93. There is no requirement to obtain a conviction for the underlying predicate offence in order to secure a conviction for the money laundering offences in Sections 4 to 6. All that is required is proof that the property is the proceeds of unlawful activities and the property must be described with sufficient accuracy, but no allegation has to be made as to the specific offence from which the property is derived. This can be proved through any evidence that would ordinarily be admissible (*e.g.* direct evidence from an accomplice or from surveillance or indirect evidence by a forensic expert concerning an audit trail or circumstantial evidence).

Predicate offences

94. South Africa adopts an "all crimes approach"; hence, the money laundering offences extend to the proceeds of any crime under South African law. Annex 5 contains examples of the range of offences contained in all twenty designated categories of predicate offences.

95. By virtue of the definitions given to the "proceeds of unlawful activities" and "unlawful activity", the money laundering offences in Sections 4-6 would also extend to proceeds or property derived from the commission of predicate offences committed outside of South Africa.

Ancillary offences

96. Generally, South African law recognises the concept of ancillary offences and other forms of inchoate offences including conspiracy, incitement, attempts, and aiding and abetting. According to Sections 18(2)(a) and 18(2)(b) of the Riotous Assemblies Act, 1956, it is an offence either to conspire to commit or to incite another person to commit any criminal act in terms of the common or statutory law. An attempt to commit either a statutory or common law offence is also punishable under Section 18(1) of the Riotous Assemblies Act. According to this Section, any person "who attempts to commit any offence against a statute or a statutory regulation shall be guilty of an offence and, if no punishment is expressly provided thereby for such an attempt, be liable on conviction to the punishment to which a person convicted of actually committing the offence would be liable". South African law also distinguishes between three categories of persons who may be involved in the commission of a crime – namely the perpetrators, the accomplices and the accessories after the fact. Although the terms "aider and abettor" are not formally used in South Africa, a leading South African legal author Professor C.R. Snyman has indicated that the term usually refers to an accomplice in the South African context. Such ancillary offences are equally applicable to money laundering offences.

97. In South African law, the essence of a conspiracy is an agreement to commit a crime. Notably, one of the elements of the offence of ML in Sections 4 and 5 POCA is also an agreement to knowingly deal with unlawful proceeds. It therefore follows that in practice, where there is an agreement to conceal unlawful proceeds, the defendant(s) would be charged with the full offence of money laundering punishable under Sections 4 or 5 of POCA rather than with a charge of conspiracy to commit the said offences read with or pursuant to Section 18(2) of the Riotous Assemblies Act 1956. This explains why no case of conspiracy to commit money laundering has been brought before the court to date.

98. While the POCA[5] contains explicit ancillary offences of conspiracy and attempts for offences relating to racketeering offences (see s.2(1)(g)), and of conspiracy, incitement and attempts for offences relating to criminal gang activities (see s.9 and item 34, Schedule 1), similar ancillary provisions have been left out for the offences under Sections 4 to 6. At the on-site meeting, the anomaly was explained as a drafting oversight. Although the POCA first came into effect in 1998 and has since been amended on at least two subsequent occasions, the omission of specific ancillary offences provisions for Sections 4 to 6 had never been addressed or rectified. Even though the South African authorities indicate that under South African law it is not a prerequisite that the existing laws of general application such as s 18(2) of the Riotous Assemblies Act 1956 be reincorporated into any new legislation, there does not, at the same time, appear to be any good reason to maintain the current anomaly of incorporating specific ancillary offences for racketeering and criminal gang activities in the POCA (when it is not a prerequisite to incorporate such) while at the same time omitting similar provisions for the offences under Section 4 to 6. Nevertheless, given the broad applicability of the Riotous Assemblies Act, the evaluation team did not view this anomaly

[5] Section 14 of the POCDATARA also has similar provisions in relation to terrorist financing offences.

in the POCA as creating an actual, practical problem in applying the full range of ancillary offences for money laundering.

Additional elements

99. There have been no court decisions to date on whether South African authorities would be able to prosecute a money laundering offence in South Africa involving the proceeds of conduct that occurred in another country, but is not an offence in that other country (although the conduct would have constituted a predicate offence had it occurred in South Africa). Be that as it may, the South African authorities are confident that this is possible given the Constitutional Court's pronouncement in a decision that South African courts would have jurisdiction if the conduct had harmful consequences for South Africa (*S v Basson* 2005 (12) BCLR 1192 (CC)).

Recommendation 2

100. The money laundering offences of the POCA apply to any person who "knows" (actual knowledge) or "ought reasonably to have known" (constructive knowledge that the property is or forms part of the proceeds of unlawful activity. A person "ought reasonably to have known" something if a reasonably diligent and vigilant person with the general knowledge, skill, training and experience that may be expected of a person in his or her position and the knowledge, skill, training and experience that the person actually has, would have known that fact (Section 1(3) of the POCA). As a result the money laundering offences apply to persons who knowingly (*i.e.* intentionally, including with wilful blindness) or negligently (*i.e.* without the necessary care) engage in money laundering.

101. South African law permits the acceptance of direct evidence as well as circumstantial or other indirect evidence, which is almost always relied upon to prove intent. A defendant can therefore be convicted of a money laundering offence based on the inferences to be drawn from the objective factual circumstances if these are sufficient to proof the ingredients of the charge.

102. Under South African criminal law liability extends to legal persons. Under the Interpretation Act, 1957, the word "person" when used in any law includes:

- any divisional council, municipal council, village management board, or like authority;
- any company incorporated or registered as such under any law; or
- any body of persons corporate or unincorporated.

103. Additionally, Section 332 of the Criminal Procedure Act (CPA) makes provision for the prosecution of corporate bodies in respect of any offence.

104. Under South African law, criminal prosecution does not preclude civil liability (in respect of damages) or administrative proceedings (which may be used in respect of certain types of legal persons under regulatory supervision).

105. The penalties for money laundering pursuant to Sections 4, 5 or 6 of the POCA are a fine not exceeding ZAR 100 million or imprisonment for a period not exceeding 30 years (s.8 POCA). The penalties for money laundering are on par or even exceed some of the penalties for some more serious offences under South African law including the Explosives Act, Firearms Control Act, robbery and fraud. The maximum punishment (especially the provision on imprisonment) under POCA is also higher when compared with similar offences in other jurisdictions (United Kingdom – maximum 14 years

imprisonment, unlimited fines; Hong Kong - maximum 14 years‘ imprisonment and a fine of five million Hong Kong dollars (about EUR 500 000); Singapore-maximum seven years imprisonment, fine up to 500 000 Singapore dollars (about EUR 257 000); Canada – maximum ten years, fine).

106. The assessment team was provided with some examples of how, in practice, these sanctions have been applied. For instance, a natural person was convicted of money laundering pursuant to articles 5 and 6 of the POCA, involving about ZAR 421 million (EUR 35 million) worth of proceeds, and was sentenced to eight years’ imprisonment: see ***S. v. Maddock*** Case SH7/17/08. In another recent case, two legal persons (companies) were convicted of money laundering pursuant to Section 4 of the POCA and each fined ZAR 500 000 (EUR 42 000): see ***S v. Shaik and Others*** Case CCT86/06. These convictions and sentences were upheld on appeal.

Recommendation 32

Statistic and Effectiveness

107. The assessment team was not provided with comprehensive data or statistics on details of money laundering investigations, prosecutions and convictions which would have been helpful in gauging the effectiveness of the AML/CFT regime in South Africa. The statistics from SAPS show a low rate of money laundering investigations and convictions. In the five years from April 2003 to March 2008, there were 64 pending cases before the courts of which only 16 resulted in convictions. The number of cases brought to court actually dropped in 2006 to its lowest (nine cases) before registering an upturn for the years 2007/2008 (23 cases). According to the SAPS statistics, there were no convictions for the years 2003-2004, and 2006.

108. Statistics from the NPA were more detailed; however, it appears that they come from only one unit (the SCCU) and do not reflect all ML convictions in South Africa. Further information concerning the specific nature of these cases (*e.g.* type of predicate offence, whether the case involved domestic or foreign predicates, and dates of the convictions so as to see if prosecutions/convictions are increasing) was not available.

SAPS investigations of money laundering (ss. 4-6 of POCA)

April 2003 to March 2008

Category	YEAR					TOTAL
	2003	2004	2005	2006	2007/08	
Number of cases registered on the CAS System	0	14	17	9	23	64
Convictions	0	0	3	0	13	16

Notes:
1. Cases pending before court – 15.
2. Several other investigations and or court case may be pending where the offence of money laundering may be added later. The systems will currently not indicate these numbers.

Statistics from the NPA's Specialised Commercialised Crime Unit (SCCU)

Name of Case	Section charged	Value involved in the ML	Self Laundering / Outside Party	Trial / Plea Bargain	Sentence	Asset Forfeiture Assets frozen / confiscated
Snyman	4(b)	ZAR 1 million	Self laundering	Trial	124 years, 18 effective	Yes
Engelbrecht JPG	4(b)	ZAR 4 million	Self Laundering	105A[1]	124 years, 15 effective	No (sequestrated and liquidated)
Engelbrecht JPG	4(b)	ZAR 4 million	Self laundering	105A	15 years wholly suspended and correctional supervision (81 years old)	No (sequestrated)
R E Bailey	4(b)	ZAR 20 million	Self Laundering	105A	ZAR 3.5 million fine or 15 years imprisonment wholly suspended plus payment to curator of ZAR 500 000	No (sequestrated and liquidated)
S A Bailey	4 (b)	ZAR20 million	Self laundering	105A	ZAR 1 million fine or two yrs wholly suspended plus payment to curator of ZAR 200 000	No (sequestrated and liquidated)
Setshedi	4(b)(i)	ZAR 275 000	Outside party	Trial	Still to be sentenced, but convicted	No
Msimango	4(b) (i)	ZAR 329 909.78	Outside party	Plea bargain	three yrs imp.	No
Nyoni	4(b) (i)	ZAR 76 800	Outside party	Plea bargain	three yrs imp.	No
Dladla +1	4(b) (i)	ZAR 4,4 million of which accused laundered ZAR 11 000	Outside party	Plea bargain	four yrs imp	No
Ndhlovu	4(b) (i)	ZAR 185 478	Outside party	Plea bargain	four yrs imp	No
Ncube	4(b) (i)	ZAR 80 000	Outside party	Plea bargain	five yrs imp	No
Bozangwane	4(b) (i)	ZAR 74 640	Outside party	Plea bargain	four yrs imp; one yr suspended	No
Modise	4(a)	ML counts T ZAR 860 000	Self laundering	Trial	76 years imprisonment (30 effective) of which 5 years was for ML charge	No
Mkalipi	4	ZAR 246 942	Outside party	Trial	Convicted and sentenced to (Counts 1 -2): 2 years imprisonment; Count 3: six months imprisonment wholly suspended	No

Name of Case	Section charged	Value involved in the ML	Self Laundering / Outside Party	Trial / Plea Bargain	Sentence	Asset Forfeiture Assets frozen / confiscated
					for three years; Counts 4-9: five years imprisonment to Section 276(1)(i) – 17/09/2007	
CS Smith Bloem	4b	ZAR 8 533 905	Self	Plea Bargain	convicted, sentence 15 years imprisonment of which 3 years was suspended for 5 years	Yes Frozen
SK O' Reilly Jh					15 years' imprisonment	
C Cotton (Dbn)	4;5	ZAR 12 million	Self	Plea bargain	15 years 5 suspended	Yes
l cotton (Dbn)	6	ZAR 275 000	Self	Plea bargain	five years wholly suspended for five years on condition pays ZAR 50 000 fine and ZAR 50 000 to the complainant	Yes
S. Sokhulu (Dbn)	6	ZAR 496 000	Outside	Plea	Fined ZAR 10 000 or five years and a further five years wholly suspended.	No
C Kau (Dbn)	6	ZAR 100 000	Outside	Plea	Fined ZAR 5 000 or six months imprisonment and a further four years wholly suspended for five years on condition the accused pays the ZAR 13 200.	No
M.M. Dlamini (Dbn)	6	ZAR 80 000	Outside	Plea	Fined ZAR 10 000 or 1year imprisonment and a further 4 years wholly suspended for 5 years on condition the accused pays the ZAR 60 712	No
M.G.Nquala (Dbn)	6	ZAR 237 815	Outside	Plea	Fined ZAR 5 000 or six months imprisonment and a further four years wholly suspended for five years on condition the accused pays the ZAR 14 457.	No
De Vries	4 (two counts)	ZAR 690 286 ZAR 719 351	Both – *i.e.* robber and receiver of stolen goods	Trial	18 August 2008	No

Name of Case	Section charged	Value involved in the ML	Self Laundering / Outside Party	Trial / Plea Bargain	Sentence	Asset Forfeiture Assets frozen / confiscated
Q Marinus and 14 Others	47 counts		Both	Trial to commence on 14 April 2009		Yes
S v C Arendse	4 (at least four counts)		Both (OP will plead to be used as witness)	Trial	Trial not yet commenced	No
S v R Jacobs	4	ZAR 90 000	Self	Trial	To be placed on roll	Yes

Note:
1. Section 105A of the CPA makes provision for a person who has committed a criminal offence to enter into a mutually acceptable guilty plea and sentence agreement with the NPA.

Additional elements

109. South African authorities maintain some statistics on the criminal sanctions applied to persons convicted of money laundering (see chart above), although these are not fully comprehensive.

2.1.2 Recommendations and Comments

110. While the POCA is largely consistent with the requirements of the Vienna and Palermo Conventions, there are nevertheless technical gaps to the extent that the offence of acquisition, possession and use of proceeds of crime only apply to third party laundering (not self-laundering). It is therefore recommended that South Africa amend Section 6 of the POCA in order to extend the ML offence of acquisition, possession and use to a person who committed the predicate offence.

111. In relation to ancillary offences, it is noted that while there are specific provisions in Sections 2(1)(g), 9 and Schedule 1 of the POCA (as well as Section 14 of the POCDATARA which makes it an offence to conspire, attempt, threaten, aid, abet, induce, incite, instigate, instruct, command, counsel or procure terrorism-related offences) which extend conspiracy, incitement and attempt to offences relating to racketeering and criminal gang activities, the POCA is silent on conspiracy and attempts to commit money laundering offences under Sections 4 to 6. While there is not a current deficiency in practice, South African authorities should consider amending the POCA to regularise and standardise ss.4-6 with ss.2-9 for avoidance of doubt.

112. The lack of more comprehensive statistics and data maintained by the relevant authorities is another area which the South African authorities should also address. The lack of more meaningful data meant that the assessment team could not obtain an accurate picture of the effectiveness of the AML/CFT regime in South Africa.

2.1.3 Compliance with Recommendations 1 & 2

	Rating	Summary of factors underlying rating[1]
R.1	LC	• Section 6 POCA (acquisition, use and possession) does not extend to the perpetrator of the predicate offence. • Lack of more comprehensive statistics makes it difficult to assess the effectiveness of the ant-money laundering regime.
R.2	LC	• Lack of more comprehensive statistics makes it difficult to assess the effectiveness of the anti-money laundering regime.

Note:
1. These factors are only required to be set out when the rating is less than Compliant.

2.2 Criminalisation of Terrorist Financing (SR.II)

2.2.1 Description and Analysis

113. United Nations and other Conventions, and United Nations Security Council and other Resolutions do not automatically have the force of law in South Africa. Consequently, domestic legislation has to be enacted in order to give effect to resolutions.

114. The POCDATARA came into effect on 20 May 2005. Section 4 of POCDATARA provides for a number of offences related to terrorist financing.

115. Firstly, it is an offence for a person, by any means to:

- acquire, collect, use, possess or own property;
- provide or make available any property, economic support, financial or other service; invite a person to provide or make available any property, economic support, financial or other service; or
- facilitate any of the above,

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* offence; or
- for the benefit of, on behalf of, at the direction of, or under the control of an *entity* which commits or attempts to commit or facilitates the commission of a *specified* offence; or
- for the benefit of 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 (s.4(1) POCDATARA).

116. Secondly, it is an offence for a person to:

- deal with property;
- enter into or facilitate any transaction in connection with property;
- perform any other act in connection with property; or
- provide a 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:

- to commit or facilitate the commission of a *specified* offence;
- for the benefit of, on behalf of, at the direction of, or under the control of an *entity* which commits or attempts to commit or facilitates the commission of a *specified* offence; or

- for the benefit of 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 (s.4(2) POCDATARA).

117. Thirdly, it is an offence for a person who knows or ought reasonably to have known or suspected that property has been acquired, collected, used, possessed, owned or provided:

- to commit or facilitate the commission of a *specified* offence,
    - for the benefit of, on behalf of, at the direction of, or under the control of an *entity* which commits or attempts to commit or facilitates the commission of a *specified* offence; or
    - for the benefit of 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;
- to enter into in, an arrangement which in any way has the effect of:
    - facilitating the retention or control of that property by or on behalf of an *entity* which commits or attempts to commit or facilitates the commission of a *specified offence* 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;
    - converting that property;
    - concealing or disguising the nature, source, location, disposition or movement of that property, the ownership thereof or any interest anyone may have therein;
    - removing that property from a jurisdiction; or
    - transferring that property to a nominee (s.4(3) POCDATARA).

118. An "entity", refers, among others, to a natural person as well as a group of two or more natural persons, and an incorporated or unincorporated association or organization. This would therefore include individuals as well as formal and informal groups of persons with or without legal personality.

119. "Specified offence" refers, among others, to:

- the offence of terrorism created by POCDATARA;
- an offence associated or connected with terrorist activities referred to in Section 3 of POCDATARA;
- an offence in relation to an activity covered by any of the UN Conventions relating to terrorism (including the financing of terrorism); or
- any activity outside South Africa which constitutes an offence under the law of another state and which would have constituted an offence referred to in paragraph here, had that activity taken place in South Africa.

120. “Terrorism” is the offence under Section 2 of POCDATARA of engaging in a “terrorist activity”. “Terrorist activity” is defined in Section 1(1) as an activity that broadly contains three elements namely: *i)* the commission of certain harmful acts; *ii)* with the intention to achieve certain outcomes; *iii)* with a particular motive to promote a cause, ideology etc. Thus the term “terrorist activity” means any act committed in or outside of the Republic, which:

- involves the systematic, repeated or arbitrary use of violence by any means or method;involves the systematic, repeated or arbitrary release into the environment or any part of it or distributing or exposing the public or any part of it to:
  - any dangerous, hazardous, radioactive or harmful substance or organism;
  - any toxic chemical; or
  - any microbial or other biological agent or toxin.
- endangers the life, or violates the physical integrity or physical freedom of, or causes serious bodily injury to or the death of, any person, or any number of persons;
- causes serious risk to the health or safety of the public or any segment of the public;
- causes the destruction of or substantial damage to any property, natural resource, or the environmental or cultural heritage, whether public or private;
- is designed or calculated to cause serious interference with or serious disruption of an essential service, facility or system, or the delivery of any such service, facility or system, whether public or private, including:
  - a system used for, or by, an electronic system, including an information system;
  - a telecommunication service or system;
  - a banking or financial service or financial system;
  - a system used for, or by, an essential government services;
  - a system used for, or by, an essential public utility or transport provider;
  - an essential infrastructure facility; or
  - any essential emergency services, such as police, medical or civil defence services.
- causes any major economic loss or extensive destabilization of an economic system or substantial devastation of the national economy of a country; or
- creates a serious public emergency situation or a general insurrection in the Republic,

and which is intended, or by its nature and context, can reasonably be regarded as being intended:

- to threaten the unity and territorial integrity of the Republic; to intimidate, or to induce or cause feelings of insecurity within, the public, or a segment of the public, with regard to its security,

including its economic security, or to induce, cause or spread feelings of terror, fear or panic in a civilian population; or

- to unduly compel, intimidate, force, coerce, induce or cause a person, a government, the general public or a segment of the public, or a domestic or an international organization or body or intergovernmental organization or body, to do or to abstain or refrain from doing any act, or to adopt or abandon a particular standpoint, or to act in accordance with certain principles, and which is committed for the purpose of the advancement of an individual or collective political, religious, ideological or philosophical motive, objective, cause or undertaking.

121. For the purpose of the offences under the POCDATARA, it does not matter whether the harm referred to in the definition is suffered in or outside South Africa, or whether the public or the person, government, body, or organisation or institution in question is inside or outside South Africa.

122. The offences also cover the three instances for which funds may be used, *i.e.*:

- To carry out a terrorist act – Section 4(1) applies to property collected or provided for a specified offence which is defined to include terrorist acts.

- By a terrorist organisation – Section 4(1) of POCDATARA refers to an "entity", which is defined to include a group, which commits terrorist acts.

- By an individual terrorist – "entity" is also defined to include an individual.

123. Section 1 widely defines property to mean 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. This is an identical definition as used in the POCA.

124. Under POCDATARA, there is no requirement that the funds were actually used to carry out or attempt a terrorist act or that the fund is linked to a specific terrorist act. Section 17 specifically provides that the offences under Section 4 are committed whether the terrorist activity occurs or not, and whether or not the perpetrator's actions actually enhance the ability of any person to commit a terrorist offence, or the perpetrator knows which offence may be committed.

125. Any person who threatens, attempts, conspires, aids, abets, induces, incites, instigates or commands, counsels or procures the commission of a POCDATARA offence has also committed an offence (s.14 POCDATARA). These activities cover the types of conduct contemplated in article 2(5) of the Terrorist Financing Convention.

126. As South Africa has adopted an "all crimes" approach, terrorist financing offences are predicate offences for money laundering. Moreover, Section 4 of POCDATARA specifically criminalises the laundering of property linked to terrorist activities in and of itself (in other words not just the proceeds of a terror financing offence) 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 offence; 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 offence.

127. Terrorist financing offences apply regardless of whether the person alleged to have committed them is in the same or a different country from the one in which the (attempted) terrorist acts or their consequences occurred. The terrorist financing offences of Section 4 of POCDATARA relate to offences concerning "terrorist activity" The definition of "terrorist activity" in Section 1 of POCDATARA provides for 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. Moreover, any of the offences under the Act relating to terrorist activities can be tried by a court in South Africa:

- if the perpetrator was arrested in South Africa;

- if the offence was committed in South Africa;

- if the offence was committed elsewhere:

  - by a South African citizen or resident;

  - against South Africa or a South African citizen or resident;

  - on board a South African aircraft;

  - against a South African government facility;

  - a South African national is seized, threatened, injured or killed during its commission;

  - in an attempt to compel the South African Government to do something or refrain from doing something; or

- if the evidence reveals any other basis recognized by law (s.15 POCDATARA).

128. Additionally, any act which would constitute a terrorist related offence in South Africa and which is committed outside South Africa by a person who does not fall within one of the categories referred to above, is treated as if it was committed in the Republic, regardless of whether or not the act constitutes an offence at the place where it had been committed if:

- the act affects a public body, person or business in South Africa;

- the person is found in South Africa; or

- the person is, for one or other reason, not extradited or there is no application to extradite the person.

129. *Burden of proof and scope of liability:* The *mens rea* required for terrorist financing offences includes both intent and negligence. Under South African law: *i)* the intentional element of the offence can be inferred from objective factual circumstances; *ii)* criminal liability for terrorist financing extends to legal persons; and *iii)* criminal liability does not preclude the possibility of parallel criminal, civil or administrative proceedings where more than one form of liability is available. For more details see Recommendation 2 above.

130. *Sanctions:* The maximum penalty for conviction of a terrorist financing offence is a fine of ZAR 100 million or imprisonment for a period of 15 years (s.4 POCDATARA). Although this is comparable to the sanctions for other serious offences, it is noted that the maximum sentence of 15 years is half that of 30-year terms permissible for the money laundering offences under the POCA.

Statistics and effectiveness

131. To date there have been no prosecutions for terrorist financing pursuant to Section 4 of POCDATARA. However, all suspicions of terrorist activity, including terror financing, arising domestically or through bilateral and/or multi-lateral intelligence operations are pursued by South Africa's intelligence agencies and where relevant referred for law enforcement investigation. To date none of these matters which were actively investigated have resulted in prosecution. A dedicated team of specialist prosecutors have been established to deal with terrorism and terror financing related matters.

132. The South African Government has effectively organised co-operation among the various intelligence and enforcement agencies involved in counter-terrorism, through a series of layered co-ordination mechanisms. All the investigative authorities in South Africa have dedicated counter-terrorism capacities and are continuously, both reactively and proactively, following up all relevant information regarding terrorist financing. The pursuance of terror-related issues is firmly backed by all layers of the state from Cabinet downwards.

2.2.2 Recommendations and Comments

133. The POCDATARA appears to be comprehensive enough to meet the requirements of the Special Recommendation II. However, the effectiveness of the measures put in place by POCDATARA cannot be assessed as there have been no prosecutions. A point to note is that the maximum term of imprisonment for an offence under the POCDATARA is 15 years whereas the offence for money laundering under the POCA provides for a maximum term of 30 years and that for racketeering is up to life imprisonment. In view of the serious nature of terrorist financing, the authorities may wish to reconsider this anomaly.

2.2.3 Compliance with Special Recommendation II

	Rating	Summary of factors underlying rating
SR.II	LC	• The effectiveness cannot be assessed.

2.3 Confiscation, freezing and seizing of proceeds of crime (R.3)

2.3.1 Description and Analysis

134. The POCA provides for both criminal (conviction based) and civil (not dependent on a conviction) forfeiture, pursuant to chapters 5 and 6 of the POCA respectively. All proceedings in terms of Chapters 5 and 6 of the POCA are civil proceedings governed by the Uniform Rules of Court for the conduct of civil matters, and are applicable to both money laundering and terrorist financing offences. The Asset Forfeiture Unit (AFU) in the National Prosecuting Authority administers and implements the freezing and forfeiture provisions of the POCA.

135. The confiscation and forfeiture provisions of the POCA apply to a broad range of proceeds and property. Section 1 broadly defines the "proceeds of unlawful activities" to include any property, service, advantage, benefit or reward which was derived, received or retained, directly or indirectly, as a result of any unlawful activity, and includes any property representing property so derived (for further details see above in Recommendation 2). Similarly, the term "property" is broadly defined to mean money or any other moveable, immovable, corporeal or incorporeal thing and includes any rights, privileges, claims and securities and any interest therein and all proceeds thereof.

136. Individual Acts also contain their own forfeiture provisions, such as those contained in the legislation relating to narcotics, conservation, non-proliferation of weapons of mass destruction and conventional arms.

Post-conviction confiscation (Chapter 5, POCA)

137. Chapter 5 of the POCA provides for the post-conviction confiscation of proceeds of all offences, including ML/FT, or property of corresponding value (ss.12 to 36, in particular s.18). This Chapter of the POCA provides for the confiscation of any benefit derived from any criminal offence for which the accused is convicted. Proceeds received, derived or retained as a result of a conviction for any offence/s, or related criminal activity, form the basis of the calculation of the benefit received. A confiscation order is a money judgement and any realisable property (including legitimately obtained and untainted property) of the accused may be realised, upon an order of court, to satisfy the confiscation order.

138. To determine the property (or proceeds) that is subject to confiscation, the gross value of the defendant's benefit is calculated by adding together the value of all property, services or other benefits received as a result of an offence (s.19 POCA). For the purpose of this calculation it is irrelevant whether the defendant is still in possession of the property or not. There are also presumptions which allow the court to include expenses incurred by the defendant in the calculation of the benefit (s.22(4) POCA).

139. Once the value of the defendant's benefit has been calculated, the court must determine the value of the "realisable property" which the defendant has available to pay a confiscation order. The realisable property is the sum of the value of all property which the defendant's holds (whether obtained from legitimate or illegitimate courses) and the value of all gifts the defendant made in a period of seven years before the restraint of the defendant's property, less any obligations to secured creditors. The value of the "realisable property" may therefore be more than the value of the property which the defendant actually holds and may include the value of property held by third parties.

140. When the court has determined the value of the realisable property, it must make the confiscation order in the form of a money judgement against the defendant to the value of the benefit, unless the value of the benefit exceeds the value of the realisable property. In the latter case, the court must make the confiscation order to the value of the realisable property.

Non-conviction based forfeiture (Chapter 6, POCA)

141. Chapter 6 of the POCA provides for the non-conviction based forfeiture of instrumentalities used in any serious offence listed in Schedule 1 of POCA, including money laundering and terrorist financing (ss.37 to 62, in particular s.50). This Chapter of the POCA provides for the forfeiture of proceeds of any unlawful activity, instrumentalities of serious offences and property associated with terrorist and related activities. The validity of a forfeiture order under this chapter is not affected by the outcome of criminal proceedings, or of an investigation with a view to instituting such proceedings, in respect of an offence with which the property concerned is in some way associated. This chapter targets specific identifiable and tainted property which is preserved and then sought to be forfeited.

142. The non-conviction-based forfeiture procedure in Chapter 6 of the POCA is an *in rem* procedure. This means that the forfeiture is based on the tainted nature of the property in question. The property is tainted if it is the proceeds of unlawful activities, an instrumentality of an offence or property associated with terrorism (s.50 POCA). The action to recover the tainted property (*i.e.* the application for the forfeiture of the property) can follow the property wherever it is, including in the hands of a third party.

Instrumentalities

143. The POCA does not provide for the forfeiture or confiscation of property intended to be used as instrumentalities (*i.e.* where only the intention exists to commit a crime but no action has taken place and the property concerned has not been used in any manner to carry out the offence). However, Chapter 2 of the CPA provides for the search, seizure, forfeiture and disposal of property:

(a) which is concerned in or is on reasonable grounds believed to be concerned in thecommission or suspected commission of an offence whether within the Republic or elsewhere;

(b) which may afford evidence of the commission or suspected commission of an offence whether within the Republic or elsewhere; or

(c) which is intended to be used or is on reasonable grounds believed to be intended to be used in the commission of an offence.

144. Currently, South African law does not provide for the confiscation of property that is of corresponding value to instrumentalities of crime.

Provisional measures

145. In respect of conviction-based confiscation under Chapter 5 of the POCA, provision is made for the freezing (restraint) of property that may have to be realised in order to pay a confiscation order (s.26 POCA). A restraint order may be made at any stage during prosecution, or even before a prosecution is instituted, as long as the court is convinced that a confiscation order against the defendant is likely (s.25 POCA). Since a restraint order applies to all property that may be realised in order to pay a confiscation order, it can apply to any property obtained from legal and illegal sources.

146. In respect of non-conviction-based forfeiture under Chapter 6 the POCA, there is provision for freezing (preservation) of property that may be tainted and therefore subject to forfeiture (s.38 POCA). A preservation order is obtained at the outset of proceedings aimed at the forfeiture of property, in other words before a forfeiture order is applied for.

147. In order to facilitate the implementation of the restraint and preservation orders, the POCA provides for the seizure of property should it be required to prevent the dissipation of the property (ss.26-27, 38 and 41, POCA).

148. The POCA provides that applications for restraint and preservation orders are done by means of an *ex parte* application (ss.26 and 38, POCA). The constitutionality of this principle has been accepted by South African courts [*vide* NDPP v Mohamed 2003(1) SACR 561 CC].

Powers of tracing

149. The competent authorities have adequate powers to identify and trace property that is, or may become, subject to confiscation or forfeiture. General provisions of the CPA allow a Director of Public Prosecutions (DPP) to subpoena persons to supply information in connection with the commission of any criminal offence (s.205, CPA). This power is most often used to access financial records and other confidential information.

150. The National Prosecuting Authority Act, 1998, (NPA Act) provides that an investigating directorate may compel persons to produce evidence relevant to investigations conducted under the NPA Act (s.28, NPA Act).

151. The POCA empowers the National DPP to request Government Departments to furnish him/her with information relevant to investigations under the POCA (s.71, POCA). Courts are also authorised, when making a restraint order, to order the discovery of facts relating to property under the control of the defendant and the location of such property (s.26, POCA).

152. The Centre receives financial information in reports made to it (s.29, FIC Act). In addition, it can obtain additional information relating to those reports (s.32, FIC Act). The Centre also has additional powers to access records (s.26, POCA) and to monitor financial activity (s.35, FIC Act).

Third party rights

153. Confiscation orders under Chapter 5 the POCA are made only against those who have been convicted. Since the confiscation order is in the form of a money judgment against the defendant, it can be executed against any of the defendant's property. The interests of creditors are protected in this process (ss.20, 30 and 31, POCA).

154. The execution of a confiscation order is not limited to property which is connected to criminal activity. A confiscation order is executed against any realisable property of the defendant which includes legitimately acquired property. As such, the relevant authorities have expressed the view that it is therefore not necessary to void contracts in order to recover property under Chapter 5. In addition property in possession of third parties can be included in the calculation of a defendant's benefit from crime if the defendant gave the property to the third party as a gift within seven years of the property being restrained. This results in the gift being ignored for the purpose of calculating the defendant's benefit. "Affected gifts" of this nature also become "realisable property" which may be realised in order to pay a confiscation order (ss.20 and 14, POCA).

155. For forfeiture orders under Chapter 6 of the POCA, a court can exclude the interests of a third party who can show that he/she did not receive the property as a gift and did not have reasonable grounds to suspect that it is the proceeds of unlawful activities (s.52, POCA).

156. The South African Common Law also specifically provides that any party with a direct and substantial interest in the subject matter of civil legal proceedings may request to join the proceedings and, in certain circumstances, must be joined in proceedings.

Additional elements

157. South African law does not allow for the confiscation of property that is found to be primarily criminal in nature (*i.e.* organisations whose principal function is to perform or assist in the performance of illegal activities).

158. Chapter 6 of the POCA provides for so-called civil (non-conviction-based) forfeiture.

159. In cases of conviction-based confiscation, if the defendant does not have legitimate sources of income that are sufficient to justify the interests in any property that the defendant holds. In such circumstances the court shall accept as *prima facie* evidence that the defendant's interests in property form part of his/her benefits from crime (s.22, POCA).

Effectiveness

160. The Asset Forfeiture Unit (AFU) of the NPA is the central repository of the statistics pertaining to all seizures, confiscations and forfeitures in terms of Chapters 5 and 6 of POCA. It maintains comprehensive statistics of the overall value of property confiscated and forfeited, broken down by certain general categories of predicate offences. Overall, the forfeiture regime is being effectively implemented. However, no statistics are maintained concerning the number of cases and the amounts of property frozen, seized, and confiscated specifically in relation to money laundering and terrorist financing.

AFU Statistics : 2003/04/01 to 2008/04/01					
Freezing orders					
	Total	**Chapter 5**	**Chapter 6**	**Chapter 5**	**Chapter 6**
	No.	**No.**	**No.**	**Value in ZAR**	**Value in ZAR**
Corruption	75	44	30	183 114 529.78	10 602 684.14
Economic Crime	566	316	250	1 797 700 094.18	207 494 571.13
Drug dealing	126	26	100	40 084 898.40	42 434 740.63
Drug house	15	0	15		4 086 641.65
Drug money	84	3	81	826 193.74	11 198 815.27
Car (majority chapter 6)	8	1	7	102 145.00	363 000.00
Brothels	3	0	3		1 030 100.00
Gambling	2	0	2		1 042 655.19
Precious metals and stones	24	4	20	9 082 000.00	4 326 844.05
Natural Resources	142	7	135	3 805 881.00	21 063 575.30
Violent crime	24	10	14	7 986 226.00	4 812 331.00
Racketeering	2	2	0	60 000 000.00	
Total	**1 071**	**413**	**657**	**2 102 701 968.10**	**308 455 958.36**
Confiscation/ Forfeiture					
	Total	**Chapter 5**	**Chapter 6**	**Chapter 5**	**Chapter 6**
	No.	**No.**	**No.**	**Value in ZAR**	**Value in ZAR**
Corruption	64	34	28	110 163 460.67	6 005 783.77
Economic	486	293	193	269 524 845.03	84 746 422.71

AFU Statistics : 2003/04/01 to 2008/04/01					
Drug deal	94	18	76	10 194 194.56	13 153 204.13
Drug house	12	0	12		2 118 605.92
Drug money	79	5	74	1 217 008.74	11 039 238.06
Car	3	0	3		65 000.00
Brothels	2	0	2		730 100.00
Gambling	2	1	1	1 419 209.00	42 655.19
Precious metals and stones	16	4	12	9 027 000.00	1 128 214.05
Natural Resources	151	26	125	35 728 640.82	17 665 232.80
Violent crime	16	7	9	1 535 631.71	1 763 060.00
Racketeering	1	1	0	200 000.00	
Total	**926**	**389**	**535**	**439 009 990.53**	**138 457 516.63**

2.3.2 Recommendations and Comments

161. South Africa should extend its confiscation provisions to include the confiscation of instrumentalities of corresponding value. In addition, while the value of the proceeds confiscated are high, comprehensive statistics and data should be maintained on matters relating specifically to money laundering and terrorist financing.

2.3.3 Compliance with Recommendations 3

	Rating	Summary of factors underlying rating
R.3	C	• This Recommendation is fully observed.

2.4 Freezing of funds used for terrorist financing (SR.III)

2.4.1 Description and Analysis

Law and Procedures to freeze pursuant to S/RES 1267(1999)

162. South Africa implements S/RES/1267(1999) primarily through the process described in Section 25 of POCDATARA, read with Section 4 of the Act. Section 25 provides that the President must give notice by proclamation in the Gazette, and other appropriate means, of those who have been identified by the United Nations Security Council (UNSC) as being:

- entities who commit, or facilitate the commission of, terrorist related activities; or
- any entity against whom Member States of the United Nations (UN) must take actions as specified in Security Council Resolutions on terrorist activities.

163. In practice, the process works as follows. South Africa is subscribed to a UN system which sends immediate e-mail notifications to subscribed countries of changes made by the UNSC to the 1267 list. Additionally, a designated senior member of the SAPS Legal Services Division monitors the UN website daily at 06h30. This official is based at the SAPS Head Quarters, is legally qualified and is a permanent

member of the Inter-Departmental Working Group on Counter-Terrorism and, as such, is fully conversant with the counter-terrorism regime.

164. If the 1267 list has been amended, the SAPS official prepares a draft proclamation under Section 25 of POCDATARA and forwards it via the Minister to the President for signature. If the Minister/President is not available for any reason, an acting Minister or President will be appointed so that their absence does not affect the speed of the listing process. As soon as the proclamation is signed by the President (or acting President), it is published in a Special Gazette. A Special Gazette is an exceptional form of the Government Gazette that can be published at any given time (as opposed to the ordinary Gazette which is only published once a week). This avoids delay because there is no need to wait for a specific day of the week when the ordinary Gazette is usually published. Proclamations come into effect as soon as they are published.

165. The administrative process for preparing the proclamation, obtaining the requisite signature and publishing the proclamation in the Special Gazette begins as soon as the UN listing is made, and usually takes no more than a few days. During the intervening time, all persons are prohibited from dealing with such property or providing any financial or other services in relation to it, pursuant to Section 4 of the POCDATARA. Section 4 creates an immediate *de facto* freeze on such property, without delay, even before the proclamation is published and comes into effect.

166. Section 4 of POCDATARA criminalises certain conduct relating to property of terrorist organisations, property associated with terrorist activity, or property which is meant to benefit a terrorist entity. It is an offence for a person to:

- deal with property;
- enter into or facilitate any transaction, or perform any other act in connection with property; or
- provide a financial or other service 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:
  - to commit or facilitate the commission of a specified offence;
  - for the benefit of, on behalf of, at the direction of, or under the control of an entity which commits, attempts to commit or facilitates the commission of a specified offence; or
  - for the benefit of 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 (s.4(2), POCDATARA).

167. In practice, this means that funds are *de facto* subject to freezing action from the moment it becomes known that they relate to a terrorist activity or organisation, or are meant to benefit such an organisation. The prohibition on dealing set out in Section 4(2) of POCDATARA is consistent with the FATF definition of "freeze" which means to prohibit the transfer, conversion, disposition or movement of funds or other assets. In addition, the provisions of Section 23 read with Section 25 may be used in appropriate cases to reinforce this freezing mechanism by enabling the State to take control of specific assets in appropriate cases.

168. Every financial institution met with by the assessment team understood that finding a match (or close match) with a presidential designation triggers an obligation to file a "terrorist property report" (TPR) with the Centre pursuant to Section 28A of the FIC Act, and then await instructions (*i.e.* not deal with the assets until and as directed by the Centre). The Centre can then formally instruct the bank to freeze the

account or transaction for five days. During that time the Centre can make further inquiries to determine if the match is genuine and, if appropriate, advise the SAPS/NPA so that further action may be taken, including obtaining an indefinite freezing order pursuant to Section 23(1)(b) of POCDATARA or initiating confiscation proceedings (FIC Act, s.34).

169. All individuals and organisations that have been designated thus far by the UNSC, through the Al-Qaida and Taliban Sanctions Committee, have been named in proclamations by the President under Section 25. In total, 63 proclamations have been issued through this process. However, to date, no assets relating to persons/entities designated pursuant to S/RES/1267(1999) have been located in South Africa.

Freezing pursuant to S/RES/1373(2001)

170. The process described above in respect of Section 25 of POCDATARA pertains only to specific UN designations and therefore cannot be applied in respect of S/RES/1373(2001). South Africa has implemented a separate mechanism for giving effect to, if appropriate, the actions initiated under the freezing mechanisms of other jurisdictions. The provisions of S/RES/1373(2001) are primarily enforced by means of the freezing procedure contained in Section 23(1)(a) of POCDATARA.

171. This provision authorises the National Director to make an ex parte application to a judge in chambers for a freezing order, "concerning property in respect of which *there are reasonable grounds to believe* that the property is owned or controlled by or on behalf of, or at the direction of: (a) any entity which has committed, attempted to commit, participated in or facilitated the commission of a specified offence; or (b) a specific entity identified in a notice issued by the President under Section 25." This closely matches the definition of "without delay" as defined in the FATF methodology relating to S/RES/1373, which indicates "For the purposes of S/RES/1373(2001), the phrase *without delay* means upon having reasonable grounds, or a reasonable basis, to suspect or believe that a person or entity is a terrorist, one who finances terrorism or a terrorist organisation."

172. A foreign country may request that the South African authorities give effect to a freezing action. Such requests must be received through the appropriate channels (Ministry of Foreign Affairs, SAPS or South Africa's intelligence agencies) and accompanied by information that demonstrates "reasonable grounds" to believe that the property is owned or controlled by, on behalf of, or at the direction of an entity designated pursuant to Section 25 or any entity which has committed, attempted to commit, participated in or facilitated the commission of a specified offence. The authorities confirm that "reasonable grounds" is a very low standard of proof (well below the criminal and civil standard of proof) and may be based on information or an affidavit from the requesting country.

173. There also needs to be sufficient information to establish reasonable grounds for believing that there is property located in South Africa over which the authorities can take jurisdiction (*i.e.* give effect to the freeze). If the requesting country does not already have sufficient information to establish a connection with South Africa then, upon receipt of the request, the South African authorities liaise with the requesting country and conduct their own inquiries. For example, the SAPS and the Centre can exercise their powers pursuant to Section 27 of the FIC Act and Section 205 of the Criminal Procedure Act respectively to determine whether such property is located in South Africa or whether the person who is the subject of the request is (or has been) a client of an accountable institution. In practice, such inquiries can be conducted quickly, and any relevant information added to the material in support of an application for a freezing order pursuant to Section 23 of POCDATARA.

174. A freezing order obtained pursuant to Section 23 of POCDATARA is of indefinite duration and may be obtained without commencing a criminal investigation or prosecution in South Africa. Section 23 authorises the High Court to issue, against any person, an order to cease any conduct concerning property

covered by Section 4 of the Act. The order may be sought ex parte from a judge sitting in chambers (not necessarily in court) which means that this type of judicial freeze can be effected quickly. In urgent matters, the normal filing procedures and timelines are abridged, and a freezing order may be obtained in a matter of hours, even outside of normal court hours, if necessary.

175. This freezing procedure is reinforced by the offences created under Sections 2, 3 and 4 of POCDATARA and the forfeiture provisions of Section 19 of the Act. In addition, Section 15 of POCDATARA gives the South African courts jurisdiction to try extraterritorial offences in appropriate cases.

176. To date, the South African authorities have not received a request from a foreign country to freeze assets pursuant to S/RES/1373(2001), so the effectiveness of Section 23 remains untested. However, it should be noted that Section 23 of POCDATARA is virtually identical to the freezing mechanism in Section 38 of the POCA which has been used effectively on numerous occasions to freeze proceeds of crime, including in urgent matters on an ex parte basis. Nevertheless, in the absence of clear communication mechanisms and guidance to accountable institutions, an effectiveness concern remains (as described below).

177. South Africa has not formally designated entities of its own choosing pursuant to S/RES/1373(2001). If an appropriate case arose, the authorities indicate that they would seek a court order under Section 23 of POCDATARA to freeze the funds of a person/entity deemed by South Africa to be a terrorist.

Scope of "property" to be frozen

178. As noted above in the discussion of Special Recommendation II, the POCDATARA definitions of the words "entity" and "property" are widely drafted to include an individual and any possible grouping of individuals, and assets of every kind, regardless of whether those assets are legitimate or illegitimate, or wholly or jointly owned or controlled, directly or indirectly, by one or more persons.

Communication and guidance

179. In relation to 1267 designations, the President issues a notice by proclamation which is published in the Government Gazette, and reproduced on the websites of the SAPS and the Centre. Such notices instruct the readers that the 1267 list is updated regularly, and refers the public to the UN and South African websites which provide this information. The SAPS site also contains separate links to relevant areas of the UN website, including the consolidated 1267 list, and overviews of the work of the Al-Qaida and Taliban Sanctions Committee and other UNSC sanctions committees. All of the financial institutions that the assessment team met with were aware of the 1267 list and the proclamations. However, there is no pro-active communication to the financial sector; rather, it is up to the private sector itself to check the SAPS and the Centre websites to keep itself aware of any updates.

180. The proclamation and related communication process described above only apply to designations made pursuant to S/RES/1267(1999). In relation to 1373 designations, a freezing order obtained pursuant to Section 23 of POCDATARA must be served upon all interested parties in the same way that any court order or other process document must be served in civil proceedings. However, beyond this, there are no specific mechanisms in place to communicate actions taken under a freezing mechanism implemented pursuant to S/RES/1373(2001). This is problematic since it is not clear how accountable institutions which are not interested parties at the time the freezing order is obtained, but later come into possession of related terrorist assets, would become aware of the freezing action and their obligation not to deal with such assets pursuant to Section 4 of POCDATARA.

181. No guidance on the provisions of POCDATARA and its implications for financial institutions in relation to the FIC Act has been issued yet, although the authorities advise that such guidance is currently being developed.

Delisting and unfreezing

182. When persons/entities on the 1267 list are delisted by the UNSC, the President of South Africa must give notice of the delisting by proclaiming the amended list in the Government Gazette as per Section 25 of POCDATARA. Publication of the amended list with the deletion of the affected individual or organisation's name effectively brings the freezing under Section 4 of POCDATARA to an end. South Africa has implemented this procedure in each case where the UN has removed someone from the 1267 list – although none of the persons delisted had any assets frozen in South Africa. There is, however, no specific procedure through which South Africa can bring a delisting request to the attention of the UNSC for consideration.

183. There is no delisting process in relation to freezing actions taken pursuant to S/RES/1373(2001). This is because, as noted above, South Africa does not use a "list approach" to implementing this resolution, but instead uses the Section 23 freezing mechanism.

184. South Africa has implemented clear and publicly-known procedures for unfreezing assets in a timely manner or authorising access to frozen assets in appropriate cases, in the context of freezing actions taken pursuant to either S/RES/1267(1999) or S/RES/1373(2001). The Uniform Rules of Court set out procedures whereby a person/entity affected by a freezing order can seek relief from the Court in the form of an interdict or mandamus against the administrative actions of the executive. This is consistent with the general constitutional right of citizens to have disputes resolved before a court (s.34, Constitution) and the inherent jurisdiction of the courts to provide relief to persons whose rights have been affected by administrative actions of the executive. For example, in the case of freezing actions taken pursuant to S/RES/1267(1999), anyone who believes to have been incorrectly included in the President's notice may petition the courts for an order (mandamus) directing the President to issue a new proclamation reversing the previous inclusion of the person/entity's name in the notice in question. Likewise, if a financial institution refuses to deal with funds belonging to a person because it mistakenly believes the person is named in a Presidential proclamation, the affected person may apply to a court for a declaratory order that the President's Proclamation does not apply to him/her and an order instructing the financial institution to carry out the transactions in question. Similarly, an application for an order authorising access to funds frozen pursuant to S/RES/1267(1999) could be brought; however, there is no corresponding procedure in place for notifying and obtaining the approval of the 1267 Committee as is required by S/RES/1452(2004). This process has not been tested yet in the specific context of delisting or unfreezing actions relating to S/RES/1267(1999) or S/RES/1373(2001) since, to date, no assets have been frozen in South Africa pursuant to those resolutions.

Freezing, Seizing and Confiscation in other circumstances

185. The normal procedures in the POCA and the CPA relating to freezing, conviction-based confiscation and civil forfeiture of proceeds and instrumentalities of crime apply to all terrorism related offences, including terrorist financing (for more detail see Section 2.3 of this report).

Rights of third parties

186. Section 6(4)(b) of the Supreme Court Act provides a mechanism whereby any person having an interest which may be affected by a decision on an ex parte application (such as a freezing order) may apply to a court for relief. Additionally, Section 20 of POCDATARA provides for the protection of the

rights of bona fide third parties in relation to forfeiture orders upon conviction. Likewise, Sections 52 and 54 of the POCA provide for the exclusion of an innocent third party's interest form the operation of a forfeiture order.

Monitoring compliance and sanctions

187. The Centre and other supervisors monitor compliance by verifying whether financial institutions have appropriate internal rules, training, and systems to pick up and report matches or close matches to listed entities. While larger financial institutions have purchased commercial software to check accounts against the UN list, smaller financial institutions cannot afford such software. There is not adequate monitoring for compliance by all financial institutions.

188. Section 4 of POCDATARA criminalises a wide range of conduct associated or connected with the financing of the offences created by POCDATARA. It not only criminalises offences committed with a terrorist intent, but also the offences created under the Conventions known as the Universal Anti-Terrorism Instruments, as well as other offences which compromise State security. Section 4 also makes it an offence to deal in any way with the property of a person who has been listed under Section 25, even in the case where the listed person has not committed any criminal offence.

189. A maximum penalty of ZAR 100 million or 15 years' imprisonment may be imposed on a person convicted for contravening an offence under Section 4 (s.18(1)(c), POCDATARA). Since the offences in terms of POCDATARA (which include Section 4) are listed as Item 32A of Schedule 1 of POCA, an offence under Section 4 could be charged as an offence under Section 2 of POCA (racketeering) provided the activities which form the basis of the offence under Section 4 fall within the definition of a pattern of racketeering activity. In such a case, the offence would be punishable under Section 3 of POCA which makes provision for a fine not exceeding ZAR 1 000 million or life imprisonment or both.

Additional elements:

190. South African authorities indicate that the majority of the measures set out in the Best Practice Paper for SR III have been implemented.

191. The POCDATARA does not have explicit provision authorising access to funds or other assets that were frozen pursuant to S/RES/1373(2001). The person concerned would have to apply to a court for such expenses, and the state would have to argue that it should be done in the spirit of the appropriate UN resolutions.

192. All designations pursuant to S/RES/1267(1999) have been reproduced in notices by the President under Section 25 of POCDATARA. To date, no applications for freezing orders in respect of listings have been brought. Likewise, there have been no prosecutions for terrorist financing and no applications for related restraint or confiscation orders.

2.4.2 Recommendations and Comments

193. South Africa is committed to combating international terrorism within the ambit of UN Security Council Resolutions, UN Counter-Terrorism Conventions, the African Union Convention on Terrorism and its domestic law, and has implemented mechanisms that allow it to freeze assets pursuant to S/RES/1267(1999) and S/RES/1373(2001). However, South Africa should implement effective mechanisms for communicating freezing actions to accountable institutions and others who do not qualify as "interested parties" at the time the freezing order is obtained. The South African authorities should also issue guidance to the financial sector on how to meet its obligations pursuant to Special

Recommendation III. Better communication mechanisms and guidance would address most of the effectiveness concerns in relation to these processes which are currently untested.

194. Additionally, the authorities should enhance their monitoring of all financial institutions for their compliance with these obligations. South Africa should also implement a mechanism to bring a delisting request to the attention of the UNSC for consideration, 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).

2.4.3 Compliance with Special Recommendation III

	Rating	Summary of factors underlying rating
SR.III	PC	• No mechanism for effectively communicating freezing actions taken pursuant to S/RES/1373(2001) to those accountable institutions and others who do not qualify as "interested parties" at the time the freezing order is obtained. • No guidance has been issued. • There is not adequate monitoring for compliance by all financial institutions. • Effectiveness concerns: Although the system remains untested, effectiveness concerns remain in the absence of clear communication mechanisms and guidance to accountable institutions, particularly in relation to freezing actions pursuant to S/RES/1373(2001). • For S/RES/1267(1999), No mechanism for bringing delisting requests to the attention of the UNSC for consideration, or 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).

Authorities

2.5 The Financial Intelligence Unit and its functions (R.26)

2.5.1 Description and Analysis

Recommendation 26

Functions and responsibilities of the FIU

195. South Africa established the Financial Intelligence Centre ("the Centre") as the national centre for receiving, analysing and disseminating information on suspected money laundering and terrorist financing. The Centre was created in terms of Section 2 of the Financial Intelligence Centre Act No.38 of 2001 (the FIC Act) and became operational on 3 February 2003. Its mandate was expanded to include the detection of terrorist financing when POCDATARA was passed in the Parliament and amended the FIC Act in 2005.

196. As an "administrative" FIU under the Ministry of Finance, the Centre does not have any investigative powers. Rather, its intelligence is meant to support the existing investigative bodies and other role players in the intelligence and criminal justice system. Its principle objective is to assist in identifying the proceeds of unlawful activities, and combating ML, FT and related activities (s.3, FIC Act). Other objectives of the Centre include: (a) making information collected by it available to investigating authorities, the intelligence services and the SARS to facilitate the administration and enforcement of South Africa's laws; and (b) exchanging information on money laundering activities and similar offences with similar bodies in other countries.

197. Specifically, the Centre is tasked with: (a) processing, analysing and interpreting information disclosed to it; (b) informing, advising and co-operating with investigating authorities, supervisory bodies, the SARS and the intelligence services; (c) monitoring and giving guidance to accountable institutions, supervisory bodies and other persons regarding their performance of their duties and compliance with the provisions of the FIC Act; and (d) retaining all information received pursuant to compliance with the provisions of the FIC Act (s.4, FIC Act).

198. Section 29(1) of the FIC Act requires any person who carries on a business, manages, or is employed by such business to report to the Centre the suspicious and unusual transactions concerning money laundering and terrorist financing.

Guidance and procedures for STR reporting

199. Pursuant to Section 77 of the FIC Act, the Minister of Finance issued the Money Laundering and Terrorist Financing Control Regulations (the MLTFC Regulations) on 20 May 2005, amending and substituting the Money Laundering Control Regulations issued on 20 December 2002. MLTFC Regulations 22 to 24 specify the manner of filing an STR report, including the information to be contained in the report and the period within which the report must be filed.

200. The following basic information must be included in an STR report:

- the person or entity making the report;
- the transaction that is reported;
- any account/s involved in the transaction;
- the person conducting the transaction or the entity on whose behalf it is conducted;
- the representative, if any, who is conducting the transaction on behalf of another; and
- general information concerning the transaction (MLTFC Regulation 23).

201. Additionally, the report must include: (a) a full description of the suspicious or unusual transaction or series of transactions, including the reason why it is deemed to be suspicious or unusual as contemplated in that Section; (b) what action the natural or legal person making the report, or other entity on whose behalf the report is made, has taken in connection with the transaction or series of transactions concerning which the report is made; and (c) what documentary proof is available in respect of the transaction or series of transactions concerning which the report is made and the reasons why it is deemed to be suspicious or unusual (MLTFC Regulation 23(6)). Overall, the form consists of eight parts. All fields applicable should be completed, such as full names and surname of the subject, the identity number, passport number, addresses and similar particulars. Reporters are encouraged to supply as much detail as they have available at all times. While the form is comprehensive, some reporting entities indicated that the form is too geared towards banks.

202. Following amendments to POCDATARA by the FIC Act, the Centre issued the Circular to Stakeholders on Terror Reporting on 8 May 2005, which specified new reporting requirements for accountable institutions that have knowledge of terrorist related property in their possession or control. MLFTC Regulation 22A specifies the information to be included in these so-called Terrorist Property Reports (TPRs).

203. Both STR and TPR forms are available for downloading on the Centre's website.

204. The Centre is also empowered in terms of Section 4(c) of the FIC Act to monitor and give guidance to accountable institutions, supervisory bodies and other persons regarding the performance of their duties and compliance with the provisions of the FIC Act.

205. The Centre issued the FIC Guidance Note 2 concerning the meaning of the word "transaction" and Guidance Note 4 on suspicious transaction reporting (on 18 June 2004 and 14 March 2008 respectively). These guidance notes provide general guidelines on suspicious transaction reporting, including guidance on the manner of reporting and the reporting procedures to be followed. Guidance note 4 is divided into six parts. Part 1 provides information to help persons determine whether they fall within the category of persons for whom a reporting obligation under Section 29 of the FIC Act could arise. Part 2 provides information to help persons determine when the obligation to report under Section 29 of the FIC Act arises. Part 3 provides information to help persons understand the nature of a suspicion. Part 4 provides examples of indicators that may be taken into consideration to determine whether a transaction should give rise to a suspicion. Part 5 provides information on the implications of making a report to the Centre under Section 29 of the FIC Act. Part 6 provides a step-by-step guideline on how to use the internet-based reporting mechanism.

206. Guidance Note 4 indicates that a report should be made by means of internet-based reporting provided by the Centre. Only in exceptional cases may an STR be sent via fax or delivered by hand to the Centre. Presently, around 98% of the STRs are submitted electronically with only 2% of STRs being submitted manually. Reporters also have the option of submitting STRs via batch reporting. This method is utilised when high volumes of STRs are submitted to the Centre on a regular basis. Reports are submitted in bulk to a dedicated email address.

Access to information from reporting parties and other sources

207. The Centre has access to a variety of sources of financial, administrative and law enforcement information through a number of mechanisms in order to effectively realise its objective of receiving, analysing, and disseminating valuable financial intelligence. The primary source of financial intelligence is STR information received from people/entities/accountable institutions with statutory reporting obligations, namely 19 categories of accountable institutions as listed in Schedule 1 of the FIC Act, as well as people who carry on a business, are in charge of a business or managing a business as per the generic reporting obligation under Section 29 of the FIC Act.

208. The FIC Act enables the Centre to gather customer identification and transaction information. The Centre has the power to access and take copies of any records kept by an accountable institution in terms of Sections 22 or 24 of the FIC Act. The Centre may examine and make extracts from, or copies of, any such records. This power can only be exercised during ordinary working hours on the authority of a warrant issued in chambers by a magistrate, regional magistrate or judge (s.26(1)-(2)).

209. In addition to these sources of information, the FIC Act also enables the Centre to gather customer identification and transaction information at its discretion without any further requirements for a warrant. Section 27 allows the Centre to request an accountable institution whether: *(a)* a specific person is

or has been a client of that institution; *(b)* a specific person is acting or has acted on behalf of any client of that institution; or *(c)* a client of the accountable institution is acting or has acted for a specific person, and the accountable institution must inform the Centre accordingly.

210. Section 27 is used to follow up on STRs received, in order to determine a more complete financial profile of the subject being reported. The information can also assist a law enforcement agency to determine whether the subject of an investigation is (or has been) a client of the said accountable institution and can be used to further direct the investigation accordingly. This allows for a more targeted approach to be followed in the issuing of legal instruments such as subpoenas under Section 205 of the CPA.

211. During the financial year 2007/08, the Centre made 2 763 queries using Section 27 of the FIC Act. The Centre also sent 752 requests to accountable institutions for addition documents, which is a 41% increase in comparison to 2006/07.

Statistics concerning additional client information sought pursuant to Section 27

Financial year	Total
2005/06	247
2006/07	1 069
2007/08	2 763

212. The Centre is also authorised to obtain additional information relating to a report received, which it may reasonably require to perform its functions (s.32, FIC Act). Obtaining such additional information from the accountable institution, person or entity that had submitted the STR is done by mere request without any requirements for a warrant. When a financial institution or person receives such a request, the Centre must be furnished with the additional information without delay. The information that may be accessed under this provision depends on the nature and content of the report in question, since the information must be "additional information concerning the report and grounds thereof". Requests in terms of Section 32 can be directed to any accountable institution/person/entity that has made a report to the Centre pursuant to the reporting obligation in the FIC Act. For example, the following information can be obtained from financial institutions: copies of all opening account information (*e.g.* signature cards, identity documentation, registration documents related to legal entities and completed account opening documentation forms), and transaction records (*e.g.* bank statements, copies of cheques and deposit slips relating to transactions mentioned in the report). From casinos, gaming records and surveillance footage can be obtained. From estate agents, copies of offers to purchase, copies of contracts of sale, and know-your-customer (KYC) documentation can be obtained.

Statistics of Section 32 concerning requesting additional information

Financial year	Total
2005/06	230
2006/07	533
2007/08	752

213. If the Centre wishes to obtain further information from a different institution which is not associated with the submission of the STR, the Centre would have to do so under authority of a warrant in terms of Section 26 of the FIC Act. In the normal course of the Centre's analysis work it is has not proved to be necessary to access further information on other accounts held at other financial institutions. The Centre's analysis would normally provide the relevant investigative authority with sufficient information on other accounts that may be relevant to an investigation to enable that authority to obtain the necessary subpoenas, etcetera, to access the relevant information from the financial institutions in question as part of the financial investigation that would follow the Centre's referral or a request for information. The Centre has thus far exercised the power under Section 26 of the FIC Act to access information held by another financial institution under authority of a warrant in one instance.

214. The Centre can also gather information relating to the transaction profile of a person with a particular institution (s.35, FIC Act).The Centre may obtain an order from a judge directing an accountable institution to monitor and report to the Centre each transaction performed by a particular customer over a period not exceeding three months at a time. This period may be extended on application to the judge.

215. The Centre may also obtain information from supervisory bodies and the SARS upon request (s.36, FIC Act). Requests of this nature override secrecy obligations which apply, for instance, to the SARS.

216. The Centre endeavours to maintain healthy relationships with supervisory bodies as well as the SARS. It is therefore possible for the Centre to approach some supervisory bodies directly to obtain information (*e.g.* the SARB in relation to exchange control transactions). No formal requests via Section 36 of the FIC Act are initiated, as the information is indirectly obtained.

217. The Centre has both direct and indirect access to non-publicly available databases. Firstly, the Centre has direct access to information in databases maintained by other government departments (*e.g.* the population register maintained by the Department of Home Affairs). Secondly, the Centre has indirect access to information such as that held by the SAPS which can provide a subject's cross-border movement and criminal record. The Centre can also indirectly access information held by the Exchange Control Division of the SARB and tax information held by the SARS. In these instances, the Centre depends on the relevant governmental agency maintaining the database to extract the required information at the Centre's request. Having the ability to access these sources of information ultimately adds value to the analysis product of the Centre and can assist law enforcement agencies to prioritise the focus of their investigations. The average time for the Centre to obtain information on an indirect basis across the range of government and regulatory agencies is 14 days.

218. The Centre has further direct access to commercial databases that offer the Centre access to information pertaining to registered legal entities and the composition of their governing structures, credit histories of individual/entities, ownership of property and lists related to politically exposed persons (PEPs). The information gained from these databases enables the Centre to provide law enforcement agencies who are the recipients of the information with a consolidated intelligence product.

219. Other methods to access information include secondments, MOUs and information shared via the Egmont secure web. The Centre also makes use of open sources of information such as internet and the media.

220. The combination of the above-mentioned information from various sources, with the analysis of STRs and additional documents, enables the Centre to properly undertake its mandate.

Analysis and disseminating information

221. Every STR received by the Centre undergoes an initial evaluation process and is assessed against internal rules to identify cases which have possible ML/FT indicators. Once such an instance has been identified the matter is assigned to an analyst. Thereafter, the intelligence cycle is followed to develop a tactical/strategic intelligence product and the powers to gather more information as described above are utilised, as appropriate.

222. Under Section 3 of the FIC Act, the Centre shall make information collected by it available to investigating authorities, the SARS and the intelligence agencies. In addition, Section 40 of the FIC Act provides for information to be provided either upon the initiative of the Centre or upon written authority of an authorised officer to a domestic investigating authority, the SARS and the intelligence services. The Centre is therefore entitled to disseminate a broad category of information to domestic authorities for investigation or action, when the Centre reasonably believes such information is required to investigate suspected unlawful activity.

223. The Centre refers, a package of information, which will normally include the demographical profile of the subject, his/her banking exposure, and his/her transacting pattern with specific reference to any unusual or suspicious transacting corroborated by specific examples to this effect. Information referred to the domestic authorities will therefore include the Centre's analysis and interpretation of the reported information and where possible, substantiated conclusions regarding possible involvement with certain predicate offences. Demographical information will include all relevant information which the Centre has direct or indirect access to (*e.g.* ID and passport number, marital status, children, previous convictions, the subject's involvement with legal entities, credit history, immovable property registered in name of the subject, entities/people associated with the subject, cross border movement and tax status). This is done with the understanding that information provided should be integrated into the intelligence bases of the domestic authorities and investigated in line with their respective mandates.

224. The Centre does not contemplate achieving a 1:1 ratio between STRs received and matters referred to law enforcement agencies. Typically the Centre's reports may involve information from a number of STRs where there is some underlying link in the information reported. The possibility even exists that information from a particular STR may be referred to law enforcement on more than one occasion.

225. In the financial year 2007/08, the Centre created and disseminated 999 referrals to the investigating authorities, which denotes a 83% increase in comparison to the 2006/07 year. The Centre has estimated the financial value of the referrals made to be about ZAR 2 billion (EUR 169 million). This is a 44.1% increase in estimated value compared to the previous year.

226. In addition to pro-actively disseminating referrals to domestic law enforcement authorities, the Centre also supplies information drawn from STRs to law enforcement upon request to support a pending investigation. In order to meet legislative requirements and to ensure integrity of the requesting process, the domestic authorities appoint Authorised Officers in terms of the FIC Act. The Centre is kept informed of the current Authorised Officers in the domestic authorities and provides training to them to ensure that the integrity of information is maintained even during the investigation stage.

Statistics of local requests per agency

Received						
Financial year	**AFU**	**DSO**	**SAPS**	**NIA**	**SARS**	**SASS**
2005/06	77	32	91	1	5	1
2006/07	128	37	101	12	5	7
2007/08	185	43	52	27	20	0
Disseminated						
Financial year	**AFU**	**DSO**	**SAPS**	**NIA**	**SARS**	**SASS**
2005/06	62	21	68	1	3	1
2006/07	122	33	92	10	5	6
2007/08	126	19	30	13	17	0

227. The Centre received 406 requests for information during the 2007/08 financial year. Of these requests, 79 were received from international sources (other FIUs) denoting a 61% increase, while there were 327 requests from domestic sources representing a 22% increase in the use of the Centre's information, year-on-year.

228. The Centre performed 4 interventions in terms of Section 34 of the FIC Act, which remains unchanged in comparison to 2006/07, while the estimated financial value of the interventions was ZAR 2.7 million (EUR 228 000). This indicates a 75 % increase in comparison to 2006/07.

Statistics of Section 34 concerning intervention by the Centre

Financial year	Total	Value	Accumulated Totals
2005/06	3	ZAR 3 365 724.94	ZAR 3 365 724.94
2006/07	4	ZAR 1 546 127.31	ZAR 4 911 852.25
2007/08	4	ZAR 2 700 000.00	ZAR 7 611 852.25

Operational independence and autonomy

229. The Centre has sufficient operational independence and autonomy, and is free from undue influence or interference. The Centre is created as a statutory body with legal personality, which means it can conduct business in the commercial sphere, employ and remunerate its staff and procure services in its own name (s.5, FIC Act). It is located within the Ministry of Finance and accountable to the Minister of Finance. The Centre is an institution outside the public service but within the public administration (as envisaged in Section 195 of the Constitution of the Republic of South Africa). It is registered as a Section 3(a) entity in terms of the Public Finance Management Act, 1999 (the PFM Act). This means that while the Centre is regarded as an independent entity within "government", it is not bound by the same rules that apply to government departments. The PFMA Section 3(a) status provides the Centre with a degree of independence in regards to its functioning, developing its own remuneration framework, policies, staffing and skills requirements, and other policies.

230. The head of the Centre (the "Director") is a statutory position. The Director is appointed by the Minister of Finance, performs the functions of this office within a policy framework determined by the Minister, and reports directly to the Minister of Finance for the performance of the Centre. However the

Centre only provides strategic intelligence to the Minister and policy makers. The Director has the authority to take all decisions of the Centre in the exercise of its powers and the performance of its functions. Moreover, the Director of the Centre is prohibited from disclosing to the Minister any information that would identify an individual who made a report to the Centre or who is the subject of a report to the Centre.

231. Only the Minister of Finance may remove the Director from office or suspend the Director and this may only be done on grounds of misconduct, incapacity or incompetence, or that the Director does not meet the standards of a security vetting.

232. The Director is the chief executive officer and accounting authority of the Centre in terms of the PFMA which means that the Director is responsible for the formation, development and management of the Centre's administration, and the control, and maintenance of discipline, of the Centre's staff (Sections 6 and 10 of the FIC Act). It also means that the Centre does not fall within a particular Government Department (s.2, FIC Act). The sources of the Centre's funds are restricted by law to money appropriated annually by Parliament for the purposes of the Centre, any government grants made to it and any other money legally acquired by it. The Centre may accept donations only with the prior written approval of the Minister.

Protection of the information

233. The Centre's reputation depends on the integrity, accuracy and reliability of the information it receives and that which it disseminates. It is in this understanding that the following measures have been put in place to guard against violations of information integrity. The Centre's staff is security vetted by the National Intelligence Agency which is the agency responsible for vetting of Government officials. In addition all staff sign an Oath of Secrecy. The Centre also implements a security policy which covers the following aspects:

- The legislation applicable to the workings of the Centre and the protection of the confidentiality of its information.
- The responsibilities of every employee with regard to 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.

234. Document security within the Centre is implemented to the standard required by the National Minimum Information Security Standards set by the National Intelligence Agency. The premises where the different Sections of the Centre are located are equipped with access/egress control which includes security spot-checks. Access to the Centre's database where reported information is stored is restricted to those that require access to execute their duties. Furthermore, the database, which operates on a SQL server 2000, is protected by a double layered access system, which means that an employee needs to firstly have access to the network (which requires a password), then an additional log-in system needs also to be accessed.

235. Dissemination of information is legislated in Section 40 of the FIC Act which provides for the dissemination of information to investigating authorities, the SARS and intelligence services. It also provides for the dissemination of information to entities outside the Republic which perform similar

functions as to those of the Centre. It also clearly stipulates who is entitled to request information from the Centre and defines the requirements to access information from the Centre.

236. To ensure that the Centre disseminates information in accordance with the relevant legal provisions, referrals of information must be approved by the Director or a designated Senior Official of the Centre. Dissemination of information is being done via fax, email or physical collection by a designated member (authorised officer/nodal point) of the recipient agency who will be notified to collect the product. This is a controlled process where the nodal point would have to formally acknowledge receipt of the product. Another mode of delivery is the Egmont website for information exchange amongst the Egmont members.

Periodic reports

237. The Centre releases an annual report in terms of the PFM Act. The Annual Report is required to be tabled in Parliament no later than 30 August each year and shall include the annual audited financial statements and a Directors' activities report. Before the report is tabled, it is required that it be signed off by the Auditor-General as well as the Minister of Finance.

238. Information, including the Annual Report, is published on the Centre's public website. These annual reports information on the following:

- the number of requests received from local and international stakeholders;
- the number of STRs received from accountable institutions; and
- the number of referrals disseminated to various domestic authorities.

239. The public reports do not contain information on typologies and trends. The assessment team was informed that this was due to the relative newness of the Centre. This was a conscious decision to proceed incrementally, gather information so as to be able to analyse and understand typologies, and thereafter publish typologies that are therefore more substantiated. The Centre has recently established a unit to work on this and develop typologies.

240. The Centre does conduct stakeholder feedback sessions with various stakeholders to discuss past activities, challenges and successes, emerging trends and typologies with a view to improving their AML efforts and future cooperation. In addition, the Centre provides public feedback by means of an electronic query facility. Members of the public can make enquiries relating to the FIC Act and the Centre via the Centre's website. A response is forwarded within five (5) days of the initial query.

Total number of queries

April 2007 – June 2007	161 queries received and responded to
July 2007 – September 2007	107 queries received and responded to
October 2007 – December 2007	65 queries received and responded to
January 2008 – March 2008	35 queries received and responded to

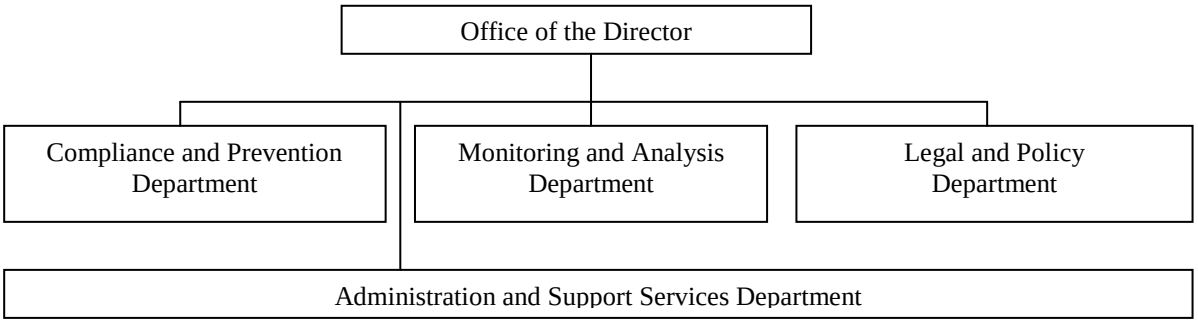
The Egmont Group

241. The Centre became a member of the Egmont Group of Financial Intelligence Units in 2003. In doing so the Centre agreed to the adherence of the principles laid out in the Egmont Group Charter.

Recommendation 30

Structure, funding, staffing, and other resources

242. The present structure of the Centre is as follows:



243. The Legal and Policy department has three major areas of responsibility. It administers the FIC Act, engages with international and regional policy forming and standard-setting organisations (such as the FATF), and provides policy advice on matters of a strategic nature concerning ML/FT.

244. The Compliance and Prevention department focuses on compliance oversight of the FIC Act. A core function is to inform, advise and collaborate with the supervisory bodies to ensure their effective supervision of AML/CFT compliance. Another is to liaise with accountable and reporting institutions to assist them in applying and implementing the compliance provisions within their respective institutions. The department's preventative focus includes raising public awareness and providing training to affected entities. This department liaises closely both internally with other departments on compliance-related issues, and externally with the supervisory bodies and accountable institutions. See Section 3.10 of this report for more details of the Centre's compliance work.

245. The Monitoring and Analysis department receives data and reports from the reporting and accountable institutions. It is responsible for storing the information, analysing it and, if necessary, disseminating reports to the law enforcement authorities, intelligence agencies and SARS based on an analysis of the information at its disposal. The department also liaises with law enforcement authorities, and conducts feedback sessions and training of various kinds (*e.g.* training for authorised officers or for financial investigators).

246. The Administration and Support Services provide the infrastructure to support and enable the Centre's work. The primary functions within this division include those of office management, financial and administrative management, procurement and supply chain management, human resources, registry and document storage services, in-house staff training and development, security services, marketing, in-house legal services, and information and communication technology.

247. The Director's office is responsible for the policy and strategic direction of the organisation, planning and management oversight, communication and press liaison, as well as initiating and overseeing special projects that might be initiated from time to time.

248. The Centre currently employs 108 people on a fulltime basis, while an additional 25 persons are contracted on a short-term basis. While the assessment team views these staffing levels as adequate, the Centre plans to increase its staff to around 200 in the next three years in order to increase, *inter alia*, its compliance functions (which will be increased once amendments to the FIC Act enter into force).

249. The Centre's budget is developed by the Centre itself, in accordance with all Section 3(a) public entities registered and operating in terms of the PFM Act. The Centre develops all its strategic planning priorities and estimated expenditure as projected over a three-year period. These strategic plans identify and map areas of new work within a three-year cycle, the development of targets and indicators as well as estimated costs, which are ultimately matched against annual performance reporting. The strategic plans are then submitted to the Minister of Finance for approval and thereafter followed by approval by Parliament and official publication.

250. When Parliament passed the FIC Act in 2001, it allocated ZAR 12 million (EUR 1 million) for use by the Centre in its first financial year, followed by ZAR 35 million (EUR 3 million) in year two and ZAR 37 million (EUR 3.1 million) in year three.

251. As the Centre created infrastructure and employed staff, so the original funds allocated were fully utilised during the 2006/07 financial year. National Treasury has granted the Centre an additional ZAR 44 million (EUR 3.7 million) for 2008/09 most of which is being utilised for IT infrastructure development and staff expansion. To date, the Centre has not experienced any difficulties in obtaining the funds for its budget.

252. The Centre was physically housed in the National Treasury building since its establishment. It has "outgrown" these premises and is re-locating to independent premises. The Centre is now fully responsible for all issues relating to these premises including: rental; facilities management; security; budgeting; etc.

253. The Centre developed an information technology (IT) system upon its establishment which enables it to receive reports, analyse these and interact with various other sources of data for various value-added activities to the information it receives. For the past two years, the Centre has been developing the specifications of an enhanced independent IT system intended to serve and provide capability to the Centre for the next decade. The infrastructure architecture for the Centre's IT system is completed and the Centre has embarked on the next stage of the process, which is to build the new infrastructure. The budget allocated to this process is ZAR 263 million (EUR 22.2 million).

Integrity and confidentiality standards

254. The FIC Act (Section 12) requires that all staff are security vetted before they may be employed by the Centre. In addition, all staff at the Centre are required to sign an oath of secrecy upon contracting to work for the Centre.

255. All employees are required to provide the Centre with a Financial Disclosure Statement, on an annual basis. The disclosure form is required to be signed before a Commissioner of Oaths and all such forms require the signature of the Director. In the case of the Director and Senior Managers, all Financial Disclosure Forms are lodged with the Minister. The financial disclosure form requires that an employee reveal to the Centre information on: any shares and/or financial interests; directorships, partnership and trusts; remunerated work outside the Centre, which requires the name of employer, the type of work and the remunerated amount; consultancies and retainership; sponsorships and donations; gifts and hospitality from a source other than a family member which includes providing information on the description, value and the source of the particular gift; land and property which requires a description of the property, its extent, the area involved and the value; and other assets.

256. The Centre has a Code of Ethics that applies to everyone working within the entity. The Centre has also initiated a whistle-blowing facility allowing any member of staff to anonymously report any fraud or wrong-doing to an independent faculty for initial investigation.

257. The Centre seeks to employ individuals who have the necessary combination of education, skill and experience for any of the positions needing to be filled. The Centre is gradually moving towards a situation where in future it will almost exclusively employ university graduates.

Training

258. All staff is provided with an annual training budget to develop new skills or enhance existing skills. The amount allocated per individual during the 2007/08 financial year was ZAR 25 000 (EUR 2 100).

259. In addition, all staff are also eligible for a study bursary of ZAR 15 000 (EUR 1 300) to assist them enrol for university/ tertiary level education. In many instances staff have used this facility to enrol for post-graduate university courses.

Recommendation 32 (FIU)

Statistics and effectiveness

260. The Centre maintains comprehensive statistics on STRs received, analysed, and disseminated, including a breakdown by type of financial institution, DNFBP, and other businesses and persons making the STR. See Section 3.7 for full statistics on STRs that accountable institutions have reported to the Centre.

261. The Centre receives a certain amount of feedback on an ongoing basis from recipients of its information (SAPS, SARS, NIA, AFU, SARB, FSB and Special Commercial Crimes Unit) to contribute to its statistics. Feedback normally takes the form of hard copy letters being faxed to the Centre.

Statistics of the Centre referrals and case outcomes

		SAPS	SARS	EXCON	DSO	AFU	SASS	FSB	NIA	Total
2003/04	**Total referred**	**16**	**15**	**2**	**1**	**2**	**0**	**0**	**0**	**36**
	STR referrals not relating to terrorist financing	16	15	2	1	2	0	0	0	36
	FT referrals*	0	0	0	0	0	0	0	0	0
	Total feedback	**17**	**4**	**0**	**1**	**4**	**0**	**0**	**0**	**26**
	Investigations pending	1	0	0	0	2	0	0	0	3
	Investigations finalised/ Closed cases	13	4	0	0	0	0	0	0	17
	STRs associated with pending investigations (STRs filed as a result of a s.205 application)**	2	0	0	1	1	0	0	0	4
	Arrests	1	0	0	0	1	0	0	0	2
	Convictions	0	0	0	0	0	0	0	0	0
2004/05	**Total referred**	**37**	**67**	**3**	**19**	**5**	**1**	**2**	**0**	**134**
	STR referrals not relating to terrorist financing	37	67	3	19	5	1	2	0	134
	FT referrals*	0	0	0	0	0	0	0	0	0

		SAPS	SARS	EXCON	DSO	AFU	SASS	FSB	NIA	Total
	Total feedback	**37**	**3**	**0**	**1**	**2**	**0**	**0**	**0**	**43**
	Investigations pending	**9**	3	0	0	0	0	0	0	12
	Investigations finalised/ Closed cases	19	0	0	0	0	0	0	0	19
	STRs associated with pending investigations (STRs filed as a result of a s.205 application)**	4	0	0	1	1	0	0	0	6
	Arrests	4	0	0	0	1	0	0	0	5
	Convictions	1	0	0	0	0	0	0	0	1
	Total referred	**20**	**146**	**0**	**24**	**0**	**1**	**0**	**0**	**191**
	STR referrals not relating to terrorist financing	20	146	0	24	0	1	0	0	191
	FT referrals*	0	0	0	0	0	0	0	0	0
	Total feedback	**72**	**0**	**0**	**1**	**3**	**0**	**0**	**0**	**76**
2005/06	Investigations pending	23	0	0	0	2	0	0	0	25
	Investigations finalised/ Closed cases	35	0	0	0	0	0	0	0	35
	STRs associated with pending investigations (STRs filed as a result of a s.205 application)**	6	0	0	1	0	0	0	0	7
	Arrests	7	0	0	0	1	0	0	0	8
	Convictions	1	0	0	0	0	0	0	0	1
	Total referred	**278**	**255**	**5**	**6**	**4**	**6**	**0**	**5**	**559**
	STR referrals not relating to terrorist financing	273	254	5	6	4	4	0	2	548
	FT referrals*	5	1	0	0	0	2	0	3	11
	Total feedback	**239**	**0**	**0**	**7**	**3**	**0**	**0**	**4**	**253**
2006/07	Investigations pending	11	0	0	0	2	0	0	0	13
	Investigations finalised/ Closed cases	6	0	0	0	0	0	0	0	6
	STRs associated with pending investigations (STRs filed as a result of a S205 application)**	220	0	0	7	1	0	0	4	232
	Arrests	1	0	0	0	0	0	0	0	1
	Convictions	1	0	0	0	0	0	0	0	1
	Total referred	**808**	**108**	**7**	**4**	**2**	**33**	**1**	**36**	**999**
	STR referrals not relating to terrorist financing	779	89	7	2	2	7	1	2	889
2007/08	FT referrals*	29	19	0	2	0	26	0	34	110
	Total feedback	**262**	**0**	**0**	**2**	**4**	**0**	**0**	**8**	**276**
	Investigations pending	49	0	0	0	3	0	0	0	52
	Investigations finalised/ Closed cases	2	0	0	0	0	0	0	0	2

		SAPS	SARS	EXCON	DSO	AFU	SASS	FSB	NIA	Total
	STRs associated with pending investigations (STRs filed as a result of a S205 application)**	210	0	0	2	1	0	0	8	221
	Arrests	0	0	0	0	0	0	0	0	0
	Convictions	1	0	0	0	0	0	0	0	1

Note: 1*Consist of Terrorist Property Reports (TPRs) and STR related to terrorist financing. 2.**A Section 205 application is a warrant authorized by a Magistrate or Judge to gain access to specified information.

2.5.2 Recommendations and Comments

262. The Centre is a well-structured, funded, and staffed FIU that is functioning effectively. However, the Centre's annual report and other publications do not yet contain information concerning AML/CFT cases, typologies or trends analysis.

263. All businesses, at least 19 categories of accountable institutions and two categories of reporting institutions, are required to submit STRs. However, the STR reporting requirements and forms issued by the Centre are mainly designed for the banks, which could lead to some confusion and inconvenience for non-banking institutions, although this has not impacted the effectiveness of the system sufficiently to warrant a downgrade in the rating. The Centre should consider tailoring STR forms to meet the needs of the non-bank reporting parties. Additionally, the Centre should issue sector-specific guidance concerning the reporting obligation.

264. Though the Centre maintains the statistics on number of STRs received, analysed and disseminated, it is noted that the Centre published only the statistics on the number of STRs in general categories of financial institutions and non-financial sector in the Centre's annual reports. No other statistics are issued or published to the supervisory bodies and reporting entities.

2.5.3 Compliance with Recommendation 26

	Rating	Summary of factors relevant to s.2.5 underlying overall rating
R.26	LC	• No annual reports concerning AML/CFT cases, typologies and trends analysis have yet been issued or published.

2.6 Law enforcement, prosecution and other competent authorities – the framework for the investigation and prosecution of offences, and for confiscation and freezing (R. 27 & 28)

2.6.1 Description and Analysis

Recommendation 27

265. The SAPS is the main agency that is responsible for the investigation of money laundering and terrorist financing, and operates under a constitutional mandate to: prevent, combat and investigate crime; maintain public order; protect and secure South Africa's inhabitants and their property; and uphold and enforce the law (s.205, Constitution). Within the SAPS, the **Division: Detective Service** is responsible for the investigation of all crime, including money laundering and terrorist financing.

266. One of the strategic priorities of the SAPS is to dismantle organised crime networks. Every organised crime investigation has two primary focus areas: to obtain evidence on the predicate offence, and to prove a case in terms of the POCA. The latter investigations focus on two primary contraventions as stipulated in the act, namely racketeering and money laundering. Racketeering in South Africa is a statutory offence and will be substantiated by predicate offences. The offence of racketeering is wider in its interpretation as it is intended to address the problem of syndicates and their management. Several other investigations may be pending, where the offence of racketeering may be added later to the charge sheet as a statutory offence. The SAPS system does not currently indicate investigations that are pending. All organised crime investigations include an asset forfeiture investigation. In practise, the asset forfeiture and racketeering part of the investigation generally exposes the money laundering activity. Consistent with the current priorities of the SAPS (dismantling organised crime networks as soon as possible, thereby ensuring an impact on the crime rate), cases (charges) of racketeering supersede money laundering cases.

267. There is also a specific unit in the Detective Service which deals with terrorist offences, including terrorist financing (although, to date, there have been no terrorist financing investigations). The SAPS also has a Counter Terrorism Centre.

268. The **Division: Crime Intelligence** is responsible for crime intelligence and assists other operational components within the police to combat crime effectively. The combating of organised crime and financing of terrorism is an integral part of crime intelligence priorities.

269. The law enforcement authorities have the powers, which are exercised at their sole discretion, and subject to the domestic laws of South Africa, to arrest suspects and seize property. In practice, in ML cases, the investigating officer often uses this discretion in consultation with the prosecutor in charge of the investigation. No legislative authority is required to make decisions as to the timing of arrests or seizures.

Additional elements

Special investigative techniques

270. Investigators use special investigative techniques such as controlled deliveries, undercover operations and electronic surveillance, depending on the circumstance of the crime and the activities of the perpetrators.

271. The method of controlled deliveries has been successfully implemented for monitoring, investigating, and combating crimes including ML and predicate offences such as drug trafficking, illegal firearms smuggling, stolen motor vehicles etc.

272. Section 252A of the CPA regulates all aspects of police traps and undercover operations, including the admissibility of evidence obtained during an undercover operation. In terms of these provisions the DPP gives the necessary authority on application by an investigator to conduct an undercover operation.

273. Another technique utilised is electronic surveillance, both silent video surveillance and interception of communications, in either oral or electronic format. Interception of communications is presently regulated by the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002. These Acts also provide for the interception of postal articles.

274. Although controlled deliveries and undercover operations were said to be the most commonly used special investigative techniques, the SAPS did not have statistics on the number of cases where these

techniques had been used. However the SAPS anticipated that the maintaining of statistics was due to improve with the appointment of a National Coordinator to capture such data.

275. Special investigative techniques can be used in any criminal investigation, and have been used in money laundering investigations. The SAPS Authorities informed the assessors that until 2007 there were 23 cases relating to organised crime under investigation, 29 cases under prosecution, 15 applications lodged with the DPP and 25 cases where conviction had been secured. Although the authorities could not specify in which of these cases special investigative techniques had been used, they were positive that such techniques would have been used for ML cases.

276. Asset Forfeiture Tracing Teams have been established in all the provinces of South Africa within the structures of the Component: Organised Crime. These teams are assisting investigating officers of the Organised Crime Units and the AFU to trace property or assets, obtain statements from relevant parties and to assist the AFU of the NPA in conducting matters in terms of the POCA. The cases with asset forfeiture potential are referred to the AFU for confiscation and freezing of the assets.

277. Asset Forfeiture Tracing Teams are used to trace assets, identify the criminal route the assets were being channelled, and do preliminary investigations, the findings of which are returned to the investigating team. They do not investigate actual criminal offences.

278. Money laundering investigations by Organised Crime Units are conducted by:

- non project investigations, where an investigation officer is attached to the Organised Crime Unit, assisted by the AFU task team member; or

- project and undercover investigation by the investigation or project team which is joined by a member of the AFU who forms part of the project team and is identified with the registration of the project.

- Due to the relationship between the investigation into the assets of organised crime networks and the method they use to launder money, these investigations are frequently managed collectively within the project team framework. The SAPS also often makes use of the services of chartered accountants/accountancy firms to conduct forensic accounting investigations (*e.g.* investment frauds). The SAPS informed the assessors that they do not have such expertise in the Police Service and that chartered accountancy companies are being used. The assessors were also informed that there was no risk of the investigations being compromised as the accounting firms did not have free access to information relating to the investigation.

279. Joint investigations with foreign law enforcement agencies do take place. During these investigations special investigation techniques are applied if the circumstances require so.

280. SAPS members serve on several forums where methods, techniques and trends of crime in general, money laundering and terrorist financing are discussed. One-on-one meetings on specific matters and investigations also take place frequently. These interagency forums include among others: the Centre, SARS, NPA (*e.g.* prosecutors, Specialised Commercial Crime Unit and Specialised Commercial Crime Courts, AFU, DPP, etc.). The Centre conducts reviews of trends, based on reported information at its disposal. Information emanating from these reviews is shared with other institutions through stakeholder feedback sessions.

Recommendation 28

Compel production of information

281. The general power to compel production of information is contained in the CPA, which provides that a judicial officer may issue a subpoena requiring any person who is likely to give material or relevant information as to any alleged offence to appear at a date and place in the subpoena and be examined by a public prosecutor (s.205, CPA). The person can avoid having to appear in person by providing the required information to the satisfaction of the public prosecutor in advance. This is the main provision used to compel persons/entities to divulge information that may be subject to confidentiality, such as bank records. Although the authorities cited the above provision as the enabling provision to compel production of information in terms of the CPA, they seemed to be unsure as to what sanctions would apply for a failure to comply with the subpoena requiring the production of the information.

282. The NPA Act provides that an Investigating Director of the NPA may compel a person to appear at an inquiry where the person will be questioned and will have to produce any book, document or other object which may be relevant to the inquiry (s.28, NPA Act). This is not a general subpoena power and the information that the person in question is believed to have must be relevant to an investigation which the Investigating Director is undertaking in terms of the NPA Act.

283. In respect of both these provisions the information which a person may be compelled to produce can include information which is subject to confidentiality arrangements such as transaction records, identification information relating to a customer, account files, business correspondence and any other records relating to a customer which a financial institution may hold.

284. The SAPS informed the assessors that legal practitioners often claim legal professional privilege in respect of documents that are to be seized. In one specific case, the SAPS hired an independent counsel to assist in determining the correct interpretation of the term "privileged document".

Search and seizure

285. The general powers to search for (via search warrants), and seize, articles are contained in Sections 20 and 21 of the CPA. The CPA also provides for exceptions where a search and seizure may take place without a warrant (s.22, CPA). Articles which may be seized under these provisions include articles that may afford evidence of the commission or suspected commission of an offence. This can include information which is subject to confidentiality arrangements such as transaction records, identification information relating to a customer, account files, business correspondence and any other records relating to a customer which a financial institution may hold. Searches and seizures in terms of these provisions are conducted by police officials.

286. The NPA Act also provides that an Investigating Director of the NPA may search for and seize anything which has a bearing on an investigation conducted by the Investigating Director (s.29, NPA Act). In particular, s.29(10)(a) indicates that the Investigating Director may without a warrant enter upon any premises if he or she upon reasonable grounds believes that the required warrant will be issued to him or her if he or she were to apply for such warrant, and the delay caused by the obtaining of any such warrant would defeat the object of the entry, search, seizure, and removal. Items that can be searched for and seized under this power can include any object, book or document and can therefore also information which is subject to confidentiality arrangements such as transaction records, identification information relating to a customer, account files, business correspondence and any other records relating to a customer which a financial institution may hold.

287. Additionally, the Centre has access to any records which an institution is required to keep in terms of that Act, including records of customer identification information and transaction records which are referred to in the FIC Act (s.26 and 22, FIC Act). The Centre may access the relevant records by virtue of a warrant issued by a judicial officer. The Centre may make extracts from, or copies of, the records to which it has access.

Power to take witnesses' statements

288. Obtaining statements from witnesses is a prerequisite for investigations and prosecutions of all offences in South Africa. The power to take witness statements in the course of investigating criminal offences is generally exercised by the SAPS. This power is derived from its Constitutional mandate to investigate crime, and its authority in terms of the SAPS Act to exercise the powers and perform the duties and functions that are conferred by law on a police official (s.13, SAPS Act). In cases where coercive measures are required to obtain witness statements, the subpoena mechanism of the CPA referred to above is used to compel a witness to give statement (s.205, CPA).

289. In addition to the general power of police officials to take witness statements, an Investigating Director of the NPA may also obtain statements from witnesses in respect of specific investigations undertaken by that Investigating Director as discussed above (s.28, NPA Act). The requirement for the Director to first make an application to the court or a judicial officer before proceeding to record a statement in certain cases potentially delays an investigation where circumstances to first get such an order are not conducive. In making this note the assessors were also alive to the fact that the legislature may have included such a provision to ensure that the Office of the Investigating Director does not abuse its powers.

Recommendation 30

The SAPS

Structure, funding, staffing, and other resources

290. The SAPS is constitutionally mandated to investigate crime of any nature. It is established as a national police service and performs its policing responsibility in respect of all nine provinces. The Service comprises 1 115 police stations. The current police/population ratio is 1:365. During the on site visit the assessors raised concerns on whether the above distribution ratio was sufficiently adequate to successfully contain crime. While agreeing that the crime figures were not quite proportionate to the number of police officers available, the authorities were satisfied with their current performance.

291. The SAPS' operations are divided into a number of divisions. Of these, the Division: Detective Service and the Division: Crime Intelligence are responsible for the investigation of crime and the gathering of intelligence.

292. The **Division: Detective Service** is responsible for the investigation of common law offences and statutory offences. It is divided into four components: the Component: Organised Crime, the Component: Commercial Branch, the Component: General Investigations, and the Component: Hi-Tech Project Centre. The components Organised Crime, Commercial Branch and General Investigations are responsible for the investigation of all crimes including ML. The component: Hi Tech Project Centre renders technology and analytical support to these components. Such support is provided in form of analysing documents and evidence for court cases, rendering of support in undercover operations, testifying in court and providing any other support function to the actual investigations.

293. The **Division: Crime Intelligenc**e is responsible for the providing intelligence for investigations and assists other operational components within the SAPS accordingly.

294. The budget of SAPS for the fiscal year 2006/2007 was ZAR 32.5 billion (EUR 2.7 billion) (an increase of 14.2% over the previous financial year).

295. The staffing of the SAPS is comprised of:

SA Police Service Act Employees	129 864
Public Service Act Employees	33 552
TOTAL	**163 416** **(as of 31 March 2007)**

296. To improve the capacity of the SAPS to perform security functions at borderlines, ports of entry and exit, and during the 2010 FIFA World Cup, the number of employees will increase from 156 000 in 2005/06 to approximately 190 000 by the end of 2009/10. This will be complimented by the expansion of the Service's vehicle fleet, equipment supplies, technological infrastructure and reservists.

297. Of the total number of police officials in the South African Police Service, members within two divisions, namely the Divisions: Detective Service and Crime Intelligence are responsible for the investigation of crime and the gathering of crime intelligence, respectively, and the Division: Detective Service and the Division: Crime Intelligence. The activities of members in both these Divisions include dealing with offences relating to money laundering and terror financing.

298. The Division: Detective Service has a total of 24 595 operational members (as of September 2008). Within this division the following Specialised Units with their personnel capacities (of which the numbers are included in total figure) are responsible for the investigation and combating of, *inter alia*, money laundering and terrorist financing:

Organised Crime	1 424
Commercial Branch	619
Hi Tech Project Centre	24
TOTAL	2 067

299. The Components: Organised Crime and Commercial Branch are dedicated components within the Detective Service and are supported by the Component: Hi-Tech Project Centre that provides, among other things, analytical support. The Hi-Tech Project Centre is not involved in the investigation of criminal cases nor does it conduct undercover operation, but rather renders assistance to investigating officers in undercover operations.

300. Although reference is made to the Commercial Branch and Organised Crime Unit, the components: General Investigations (also within the Division: Detective Service) can also be involved in the investigation of money laundering cases, *e.g*. laundering of funds from vehicle theft. This type of crime is currently being investigated by the Vehicle Theft Unit. The Commercial Branch and/or Organised Crime can render assistance in a financial investigation, when required.

301. The Division: Crime Intelligence has 7 707 operational members. Within this division there are several units responsible for the gathering and analysis of intelligence regarding money laundering and the combating of terrorism.

302. Depending on the extent and nature of a crime(s), a task team consisting of members of the different divisions and components can be established to investigate. Resources will then be allocated from other detective service units to assist.

303. Overall, the SAPS appears to have adequate resourced dedicated to combating money laundering and terrorist financing.

Integrity standards and confidentiality

304. The SAPS is overseen by the **Independent Complaints Directorate**. The Directorate is a statutory body established to investigate complaints of misconduct and criminality allegedly committed by members of the SAPS and Municipal Police Services. It is also responsible for proposing reforms to reduce the incidence of the behaviour that gives rise to such complaints.

305. The SAPS has developed the following policies and procedures to address corruption and fraud prevention:

- a national risk assessment of corruption and fraud;
- corruption and fraud-related policies, including a whistle-blowing policy and a case referral policy and procedures;
- a training programme on corruption and fraud to sensitize SAPS employees about the nature and implications of corruption and fraud; and
- a marketing and communication plan for the Corruption and Fraud Prevention Strategy.

306. The SAPS also participates in the national, inter-departmental Anti-Corruption Coordinating Committee which addresses developments within the public sector relating to corruption and fraud. The SAPS has a national Corruption and Fraud Prevention Plan to address corruption and fraud in the SAPS. The SAPS has both an obligation to investigate criminal cases of fraud and also to address corruption and fraud within the SAPS. All provincial commissioners and the different divisions within SAPS have to abide by SAPS's Corruption and Fraud Prevention Plan. The Division: Detective Service will conduct investigations against members in the Police Service. All police officers have an obligation to report corruption by fellow officers. While corruption continues to be an issue, South African authorities also continue to take action to address this as evidenced by the following figures. The following statistic gives an overview of the number of members within the Police Service that have been investigated and found guilty of fraud and corruption.

Description	2006/07 Financial Year	2007/08 Financial Year
Number of cases of fraud and corruption reported against members of SAPS	307	285
Number of cases in which SAPS members were found guilty of fraud and corruption	95	106
Number of pending investigations	108	123

307. All SAPS employees are required to follow a Code of Conduct which supports the SAPS Values and Code of Ethics and is available on the SAPS website. The Code of Conduct requires employees who

are occupying senior positions (*e.g.* Directors and upwards) are expected to make financial disclosures. The SAPS also has a specific policy on accepting gifts and any other rewards.

308. Adequate legal provisions are in place to protect information at the disposal of the SAPS. Members of the Divisions: Detective Service and Crime Intelligence have to undergo a security clearance every five years. Members who work with top secret information and documents also have to undergo a polygraph test.

Training

309. Police officers must undergo 24 months of basic training (divided into three semesters) and obtain an Entry-Level National Certificate in Policing. The basic training programme is conducted at the ten SAPS Training Institutions and designated Field Training Police Stations. To qualify for enrolment in the basic training programme, the applicant must:

- be between 18-29 years (35 years of age for serving Reservists /Public Service Act Personnel of SAPS);
- be a South African citizen;
- have a Grade 12 certificate (High school qualification);
- not have any criminal convictions/records;
- allow their fingerprints to be taken;
- be able to speak, read and write English, and one other official language; and
- have a Code B driver's license.

310. The **Division: Training of the South African Police Service** provides training to members of the Detective Service and Crime Intelligence and other Divisions and Components of the SAPS. The different components of the Detective Service and Crime Intelligence are involved in the providing of training and the setting of standards for training.

311. The Detective Learning Programme was introduced in 2004 for the purpose of equipping detectives with skills and knowledge to investigate crimes and enhance service delivery. The duration of the course is 14 weeks. Training is also provided to members of the Detective Service on conducting of financial investigations and the provisions of the POCA. Several members of the Detective Service have attended the financial investigators courses that are being presented by the Centre. Training courses for specialised investigators and operatives cover money laundering and proceeds of crime. Training is also provided to specialist units on the FIC Act, the POCA, and POCDATARA. Members of the Detective Service and especially the Specialised Units also attend external courses, including university courses (*e.g.* the University of Johannesburg offers ML and forensic investigation courses). Topics covered in external training include: money laundering, terrorist financing, asset forfeiture, financial investigations, forensic investigations, the Centre and the FIC Act, banking systems; and companies and intellectual property.

312. The current training programme of the Specialised Units, such as the Commercial Branch and Organised Crime was developed by internal and external developers, and consists of courses which are done in class. These training programmes are more advanced than the Detective Learning Programme and it is expected that a member can apply the basic principles after attending the specialised courses. The

course content is specific to the respective mandates of the Specialised Units and is designed to provide the member with a very wide understanding of the specific related investigations and applicable legislation. Additionally, the Organised Crime Unit of the SAPS is training police officers throughout South Africa specifically on ML. The authorities report that this initiative has begun to generate results. In particular, by the time of the on-site visit, 16 cases had already been reported to the SAPS.

313. Crime Intelligence members receive training on intelligence gathering, managing sources, and related legal issues and analysis. They also receive training in financial analysis during the Operational Analysis course.

The NPA

Structure, funding, staffing, and other resources

314. The Constitution provides for a single National Prosecuting Authority in South Africa with the mandate to institute criminal proceedings on behalf of the State, and to carry out necessary functions incidental to instituting criminal proceedings (s.179(1), Constitution). This constitutional mandate is implemented in terms of the NPA Act.

315. The NPA consists of three operational units: the National Prosecuting Service, the National Specialist Services Division, and the Asset Forfeiture Unit and the Directorate for Special Operations. significant majority of the NPA's prosecutors are housed in the NPS, which is by far the organisation's largest unit. The NPS is responsible for the general prosecution service in South Africa and comprises nine offices (one for each seat of the High Court) headed by a DPP.

316. The National Specialist Services Division comprises four offices which are responsible for prosecutions and other services of a specialised nature on a national basis: the Sexual Offences and Community Affairs Unit, the Witness Protection Unit, the Specialised Commercial Crimes Unit and the Priority Crimes Litigation Unit. The Priority Crimes Litigation Unit has been mandated to manage investigations and prosecute all offences under POCDATARA throughout South Africa.

317. The Asset Forfeiture Unit implements the freezing and forfeiture provisions of the POCA. It comprises five regional offices responsible for Gauteng (excluding Johannesburg), Johannesburg, the Western Cape, KwaZulu Natal, and the Eastern Cape.

318. The Directorate for Special Operations (DSO, also known as "the Scorpions") is a national unit for the investigation and prosecution of offences relating to trans-national organised crime, serious and complex financial crime (including money laundering and predicate offences), and organised corruption. The Directorate comprises five regional offices namely Gauteng, KwaZulu Natal, the Eastern Cape, the Western Cape, and the Free State. It should be noted that, at the time of the on-site visit, there were ongoing discussions about disbanding the Scorpions.

319. The responsibility for prosecute money laundering cases is shared among a number of NPA units. The Specialized Commercial Crime Unit prosecutes ML cases arising from crimes investigated by the SAPS Commercial Branch. The Organized Crime Initiative of the NPS Head Office prosecutes ML cases arising from crimes investigated by the SAPS Organized Crime Unit. While the prosecutions are conducted by the regional Directors of Public Prosecutions, the NPS Head Office manages, assists and supports the prosecutions in the regions on an ongoing basis.

320. The NPA falls under the Department of Justice and Constitutional Development's budget vote. The funds are allocated by Treasury. The authorities did not provide further information concerning the NPA's budget or how it is allocated amongst its three divisions.

321. Over the past three years, the staffing level of the NPA has increased by 27%, with a view to ensuring that two prosecutors are deployed per court to ensure effective and efficient case flow management. Although the NPA has received the funding needed to reach these levels, this goal has not yet been achieved. Currently, human resources are acquired through various methods including labour brokers. One of the challenges experienced with recruitment and selection, especially with recruiting for Prosecutor posts, is that these positions are filled mainly from internal applications, which results in an increase in costs per employee, but does not significantly affect the vacancy rate. In some cases, the NPA experiences challenges with attracting and appointing applicants with the required number of years experience and some courts also experience challenges with attracting applications for certain posts generally. The NPA is therefore investigating a scarce skills framework, to meet the needs of the organisation. The current Aspirant Prosecutor Programme provides a pool of qualified and trained employees who are capacitated in the skills of prosecutions during the programme and then if successful, absorbed into vacant entry level Prosecutor posts. Although the current level of staffing appears to be inadequate, new initiatives such as Community Prosecutions have been launched.

Integrity standards and confidentiality

322. All NPA officers sign oaths of confidentiality. Those in sensitive areas are security screened (at the top secret, secret, or confidential level) every five years under the same process that is used by SAPS. The NPA also has a Code of Conduct that employees must follow.

Training

323. Within the NPS, extensive money laundering training is provided. To this end, international experts are engaged to provide training to the prosecutors in all regions of South Africa. For example, an expert from the United States Department of Justice has provided AML training to relevant staff around the country, on a regular basis with the next session taking place in the third quarter of 2008. This session will focus on training the top management of the NPA, including the staff from the central office dealing with mutual legal assistance and extraditions.

324. Additional training has taken place to develop and maintain a cyber forensic capacity in the DSO. The AFU has also provided training to the DSO. In 2004, the DSO in conjunction with United States Agency for International Development (USAID) and the United States Department of Justice held four-day AML seminars for DSO staff. DSO staff also attend an Organised Crime Course presented by the Justice College Course which covers money laundering and asset forfeiture. The SCCU also has annual training at the University of Johannesburg, and has done so since 2004.

Statistic and Effectiveness

325. The assessment team was not provided with comprehensive data or statistics on details of money laundering investigations which would have been helpful in gauging the effectiveness of the AML/CFT regime in South Africa. Of the statistics and information provided, these mainly contain basic figures on the total number of investigations and convictions.

326. It should be noted, however, that the SAPS does collect statistics and related information through the SAPS CAS system which can provide information on all the case dockets across the board that are still under investigation, including case dockets that are under investigation by the Detective Service. The system can provide information on the number of case dockets that are under investigation by the Component: Commercial Branch and Organised Crime. However, some case dockets may have been registered with preliminary criminal charges and others may later be added

327. Overall, the statistics show a low rate of ML investigations and convictions. In the five years from April 2003 to March 2008, there were 64 pending cases before the courts, of which 16 resulted in convictions. The number of cases brought to court actually dropped in 2006 to its lowest (nine cases) before registering an upturn for the years 2007/08 (23 cases). According to the SAPS statistics, there were no convictions for the years 2003-04, and 2006.

SAPS investigations of money laundering (ss. 4-6 of POCA)

April 2003 to March 2008

Category	YEAR					TOTAL
	2003	2004	2005	2006	2007/2008	
Number of cases registered on the CAS System	0	14	17	9	23	64
Convictions	0	0	3	0	13	16

Notes:
1. Cases pending before court – 15.
2. Several other investigations and or court case may be pending where the offence of money laundering may be added later . The systems will currently not indicate these numbers.

2.6.2 Recommendations and Comments

328. While South Africa has most of the necessary legal tools and funding to combat money laundering, there is a very low number of ML investigations and prosecutions, despite an acknowledged level of organised crime and predicate offences. The South African authorities should focus more pro-actively on pursuing specific money laundering offences.

329. While the legal provisions for obtaining privileged documents are adequate, South Africa should consider additional guidance to law enforcement on obtaining production of privileged documents.

330. It is recommended that the SAPS consider developing its own expertise in forensic analysis (*e.g.* in accounting and auditing) as expertise in these fields will always be required in analysing ML and FT trends. There is also need to appoint more prosecutors and provide them with a more skills-based through training.

331. The SAPS should consider maintaining statistics on cases where special investigative techniques are used (*e.g.* controlled deliveries and undercover operations). This would enable effectiveness of the use of such techniques to be determined.

2.6.3 Compliance with Recommendations 27 & 28

	Rating	Summary of factors relevant to s.2.6 underlying overall rating
R.27	LC	• Effectiveness: Lack of more comprehensive statistics makes it impossible to assess the effectiveness of the money laundering regime; the information provided shows a low number of money laundering investigations.
R.28	C	• The Recommendation is fully observed.

2.7 Cross Border Declaration or Disclosure (SR.IX)

2.7.1 Description and Analysis

General Overview

332. Currently, only ten airports are designated as ports of entry for the movement of goods and people. Eight seaports were reclassified into five fully fledged international seaports, two with reduced functions and one classified as an inland dry port. There are 54 land border posts in South Africa. Only 19 of these are designated for the movement of commercial goods. The land borders are all rated from A to C, according to the level of service provided at the border post. At an 'A' status border post, all three of the main government departments involved in the control of the movement of people and goods across the border post are present (SARS – Customs, DHA – NIB and SAPS). At the 'B' border posts, only two of the departments are present, and at the 'C' status border posts, only one department is present. The SAPS is present at all land border posts in South Africa.

333. All incoming and outgoing mail is processed through one of three international mail centres – Cape Town, Durban or Johannesburg, of which the Johannesburg International Mail Chamber (JIMC) is the largest. Both the SARS and SAPS have a permanent presence at the international mail centres.

334. To implement SR IX, South Africa uses a combination of a declaration system (pursuant to Customs law and regulations, and customs declaration forms) and an exchange control regime. Customs officers derive their powers from Section 4 of the Customs Act and administer controls relating to currency by virtue of this provision and their designation as "appropriate officer" in terms of the Currency and Exchanges Act, 1933, together with the relevant Exchange Control Regulations which are principally administered by the Exchange Control Department of the SARB (ExCon). The Exchange Control Regulations apply equally to both cross-border movements of Rand between South Africa and the Rand Common Monetary Area (RCMA) countries and between South Africa and other countries.

Incoming persons

335. Any person entering South Africa shall declare at the time of such entering, all goods (including goods of another person) upon his person or in his possession which are being brought into South Africa and which:

- are prohibited, restricted or controlled under any law; or
- were required to be declared before leaving South Africa (s.15(1)(a), Customs Act).

336. Section 1 of the Act defines "goods" as "including all wares, articles, merchandise, animals, currency, matter or things." This definition specifically captures currency and is broad enough to include bearer negotiable instruments (BNI). Currency is a restricted good in South Africa by virtue of the exchange control regime. In particular, the exchange control regime restricts the import and export of domestic currency (South African Rand), and the export of foreign currency and BNI payable in foreign currency (s.3(1)(a) and 3(6), Exchange Control Regulations).

337. The declaration form for travellers, which is used to implement this requirement, makes a distinction between "goods" and "currency". Bearer negotiable instruments are not covered. Persons entering South Africa are required to declare if they are in possession of domestic currency exceeding ZAR 5 000 (EUR 423) (which is also the amount which can be brought into the country pursuant to the

Exchange Control Regulations)[6] or foreign currency exceeding 10 000 United States dollars (USD) (EUR 7 000) or the equivalent thereof. The person would make such a declaration by taking the red channel where the declaration form also captures information identifying the bearer. Signs are posted at border entry points advising travellers of the obligation to declare.

Outgoing persons

338. Any person leaving South Africa "shall, in such a manner as the Commissioner may determine, unreservedly declare …before leaving, all goods which he proposes taking with him beyond the borders of the Republic" (s.15(1)(b), Customs Act). Additionally, the Exchange Control Regulations restrict the export[7] of domestic currency (South African Rand), foreign currency and BNI payable in foreign currency (s.3(6)), and impose a corresponding outgoing declaration obligation (s.3(3)). The export of BNI payable in domestic currency would be contrary to Regulation 10(1)(c) of the Exchange Control Regulations.

339. Signs are posted at border departure points advising travellers of the obligation to declare. However, there is no corresponding declaration form for departing persons. Instead, the South African authorities implement this obligation through intelligence-based targeting and random sampling. Targeted persons will be asked to fill in a declaration form (the same form as is used for incoming persons).

Transportations through cargo

340. A declaration system applies to all goods (as that term is defined in the Customs Act) imported into South Africa, with the exception of containers temporarily imported (*i.e.* in transit through South Africa), human remains, good imported under an international carnet, and goods of no commercial value or of a value for duty purposes not exceeding ZAR 500 (EUR 43) (s.38(1), Customs Act). The declaration (a bill of entry or SAD form T8500) must be filed with the SARS. The bill of entry form solicits information about, *inter alia*, the exporter, importer, agent (declarant), type and value of goods, and type of transportation (s.39, Customs Act).

341. A declaration system also applies to goods (as that term is defined in the Customs Act) exported from South Africa (s.38(3), Customs Act). The declaration (a bill of entry or SAD form T8500) must be filed with the SARS either before the goods are exported or within a reasonable time in the case of goods which are not subject to export duty or any obligation/condition to be fulfilled under any law, or which are being exported overland by vehicle (other than aircraft or train) and are being loaded for export at a place other than a customs controlled area.

342. In terms of implementation, the customs authorities review domestic importers and exporters, with a view to targeting high risk consignments. The customs authorities use both non-intrusive methods of monitoring cargo shipments, including through the use of cash detection dogs, and more intrusive methods such as unpacking cargo shipments and/or baggage scanners.

Transportations through mail

343. It is illegal to send cash through the mail. It is not illegal to send BNI through the mail, although the Postal Service encourages customers to use a registered and insured service when doing so. Insured mail is always accompanied by a postal declaration form; however, if the customer chooses to send it through uninsured mail, there will be no accompanying postal declaration form. However, outgoing BNI

---

6 Section 3(1)(b) and (bis), Exchange Control Regulations; Section H, Part 2.2.11, Exchange Control Manual.

7 The Exchange Control Regulations allow for some exemptions from these requirements to be obtained from the Treasury in appropriate cases.

payable in foreign exchange can only be performed with prior authorisation from the Treasury and must still be declared to the SARB pursuant to the Exchange Control Regulations. Outgoing BNI payable in domestic currency is prohibited pursuant to Regulation 10(1)(c) of the Exchange Control Regulations. Incoming BNI payable in domestic and foreign currency is not covered.

Overview of the types of physical cross-border transportations covered

344. Based on the above discussion, the following chart summarises what aspects of SR IX are covered.

TYPE OF TRANSPORTATION	TYPE OF CURRENCY/BNI	INCOMING	OUTGOING
Persons	Domestic currency	Yes	Yes
	Foreign exchange	Yes	Yes
	BNI payable in domestic currency	No	No
	BNI payable in foreign currency	No	Yes
Cargo	Domestic currency	Yes	Yes
	Foreign exchange	Yes	Yes
	BNI payable in domestic currency	Yes	Yes
	BNI payable in foreign currency	Yes	Yes
Mail	Domestic currency	N/A	N/A
	Foreign exchange	N/A	N/A
	BNI payable in domestic currency	No	Yes
	BNI payable in foreign currency	No	Yes

Powers to obtain further information, stop and restrain

345. Customs officers may stop, detain and examine any goods (including currency or BNI) while under customs control in order to determine whether the provisions of the Customs Act or any other law have been complied with in respect of such goods (s.4(8A)(a), Customs Act). This means that the grounds for possible detention include suspicion that: *(a)* a false (or no) declaration has been made as required pursuant to the Customs Act; *(b)* the goods are related to ML/FT pursuant to the POCA or POCDATARA; or *(c)* there has been a violation of the Exchange Control Regulations.

346. Customs officials indicated that where there is a suspicion of ML/FT, a period of up to two weeks was considered a reasonable period in which to determine and verify whether evidence of ML/FT can be found. Other grounds would include intelligence information received, trends and patterns and random targeting. The authorities also indicated that, at times, this period is negotiated with the person involved.

347. Customs officials also have extensive powers to question persons and obtain additional information concerning any matter dealt with in the Customs Act, including whether goods are being transported in violation of the Customs Act or any other law (s.4(7) and (8), Customs Act). Additionally, they have broad powers of search and seizure (s.4(4)-(6), Customs Act).

348. SAPS officers, who are present at all border control points, have designated powers of search and seizure pursuant to the Exchange Control Regulations. An officer may search a person who is about to leave South Africa and any accompanying articles to determine whether he/she has any bank notes, foreign

currency, BNI payable in foreign currency, gold or securities in their possession (s.3(3)). If any of these items are found during a search, they may be seized unless the officer is satisfied that the person is exempt from the Exchange Control Regulation restrictions or has a valid exemption certificate granted by the National Treasury. Additionally, SAPS officers can rely on their general search and seizure powers set out in the CPA as well as specific powers set out in the SAPS Act. In particular, a police official may, without a warrant search any person within 10 kilometres from any border or at any airport and seize anything found in the possession of such person which may lawfully be seized (s.13(6), SAPS Act).[8]

349. The Postal Service is also authorised to examine any postal article (other than a letter) by means of a detection device to determine whether an item has been posted in contravention of the Postal Services Act (s.37). Large parcels are routinely scanned. Through this process, large amounts of cash will be detected; however, letters containing small amounts of cash will not. If a large amount of cash is detected, the postal service works with SARS to determine who will open the parcel. False declarations of currency or BNI that violate the Exchange Control Regulations are referred to the SARB for investigation. The Postal Service reports that transportations of cash through the mail is not a big issue.

Sanctions

350. Making a false statement, filing false documents or making false declarations in contravention of the Customs Act is punishable by criminal fines of up to ZAR 40 000 (EUR 3 400) or to imprisonment for a period not exceeding ten years (s.84, Customs Act). As an alternative to the criminal sanctions, administrative penalties for failure to comply with any law administered by the customs authorities for and on behalf of any agency are also available (s.91, Customs Act). The Postal Services Act does not provide for any sanctions to be applied in instances where a false postal declaration is made. Any goods restricted and/or prohibited must still be processed through Customs irrespective of the modality of import/export. In this instance non-declaration would constitute a Customs offence that is sanctioned in the Customs and Excise Act.

351. The FIC Act also prescribes sanctions for failing to report the conveyance of cash across the border – imprisonment for up to 15 years or a fine not exceeding ZAR 10 000 000 (EUR 861 000) (s.68, FIC Act). However, this provision will not come into force until 1 January 2009.

352. Cases involving violations of the Exchange Control Regulations, including the related declaration requirements, are adjudicated through the SARB. In such cases, the currency is seized, and fines, penalties and forfeiture may result. The SARS is currently developing automated targeting capabilities, including the ability to raise the risk ratings and screen the parameters of known and repeated offenders.

353. Money laundering or terrorist financing through the physical cross-border transportation of currency/BNI (regardless of whether the transportation is effected by persons, in cargo or through the mail) is punishable pursuant to the POCA (ZAR 100 million (EUR 8.6 million) or up to 30 years imprisonment for ML) and POCDATARA (ZAR 100 million or up to 15 years imprisonment for FT) (see Sections 2.1 and 2.2 above for a detailed description of the applicable sanctions). In such cases, the freezing, confiscation and forfeiture provisions discussed in Section 2.3 above would apply.

[8] The FIC Act provides that a police official or designated person who has reasonable grounds to suspect that a person has failed to report the conveyance of cash may, at any time, search any person, container or other thing in which the cash in question may be found. If any unreported cash is found the police official or designated person may seize it (s.70, FIC Act). This provision is not yet in force.

354. The provisions of POCDATARA and the POCA relating to the freezing and forfeiture property related to terrorist financing (as discussed in detail in Section 2.4) apply to currency or BNI that are transported across the border and are related to terrorist financing.

Collection and use of information

355. There is not yet a requirement to report threshold movements of currency to the Centre or make the information available to it in some other way; however, in practice, customs officials are sending the declaration reports on incoming persons to the Centre in electronic form. Section 30 of the FIC Act provides that a person intending to convey an amount of cash above a certain threshold to or from South Africa must report that to a designated person (the Centre). However, this provision will not come into force until 1 January 2009, so as to give the Centre sufficient time to improve its technical infrastructure so as to be able to handle the volume of such reports. Section 30 will not, however, apply to reports relating to cross-border transportations by cargo or through the mail. There are also concerns that information would not be recorded or made available to the Centre in cases where there is a false declaration or no declaration (but there should have been) and there is no seizure, or in cases where ML or FT is suspected.

356. For cargo, bills of entry are collected and forwarded to the SARB in electronic form. They are not made available to the Centre.

357. For mail, postal declarations are collected and maintained by the Postal Service. Where irregularities are detected, the postal declaration is forwarded to the SARB. However, postal declarations are not made available to the Centre.

358. The SARS is subject to legislation, policies and procedures to ensure that information is securely protected and disclosed only in accordance with the law (s.4 and 50, Customs Act). Current measures include agreements by passengers that information may be shared with agencies/departments under the jurisdiction of the Minister of Finance.

Domestic and international co-operation

359. A variety of coordination mechanisms exist to facilitate co-operation at the domestic level. Coordination at the domestic level takes place between the SARS (Customs) and relevant law enforcement authorities. Communication channels and structures exist between SARS and other agencies (local and international) and designated persons serve as single points of contact for the entry/exit of information requests in pursuit of enquiries and/or investigations. As well, a joint initiative exists between the SARS, the Centre and the NPA regarding the targeting, detection and subsequent prosecution of unauthorised cross border movements of cash. Additionally, the Postal Service has had some success, working with the SAPS, in disrupting the theft of BNI (cheques and postal orders) being sent through the mail and identifying hotspots where such activity is taking place.

360. In addition, the Border Control Operational Coordinating Committee (BCOCC) is a structure that was formed at Cabinet level and includes heads of law enforcement agencies. The BCOCC has structures at National, Provincial and Port Levels. It is responsible for the strategic management of the South African border environment in a co-ordinated manner and is focused on national crime prevention. A National Integrated Border Management Strategy has been developed and adopted by Cabinet. The strategy includes initiatives for the development of systems that enable South Africa to comply with international Conventions, standards, Recommendations and other instruments it has acceded to, including the integration of information, process and procedures and co-ordination of activities and infrastructure.

361. Cooperation takes place in terms of legislation, through agreements and informal channels (*e.g.* Interpol and World Customs Organisation Regional Intelligence Liaison Offices (RILO) and the Customs Enforcement Network (CEN). Section 50 of the Customs Act allows for the disclosure of information pursuant to the various mutual assistance agreements in place with other Administrations and accession to the Nairobi Convention. Direct co-operation also takes place on an agency to agency basis.

362. South Africa currently has the following bilateral and multilateral legal frameworks in place to support Customs-to-Customs information sharing. The following are currently in force:

(a) *Bilateral Agreements on Mutual Administrative Assistance (MAA Agreements):* Algeria, China (PRC), France, India, Mozambique, Netherlands, United Kingdom and United States of America.

(b) Multilateral Frameworks:

(i) EU: Trade, Development and Cooperation Agreement, Protocol 2 on mutual administrative assistance in Customs matters (Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden and United Kingdom).

(ii) IBSA (India-Brazil-South Africa) Trilateral: IBSA Agreement on Customs and Tax Cooperation (Brazil and India).

(iii) SADC Protocol on Trade, Annex II concerning Customs cooperation with the Southern African Development Community (Angola, Botswana, Lesotho, Malawi, Mauritius, Mozambique, Namibia, Swaziland, Tanzania, Zambia and Zimbabwe – Congo (DRC), Madagascar & Seychelles still to be confirmed.

(iv) International Convention on mutual administrative assistance for the prevention, investigation and repression of Customs offences (Nairobi Convention) – only certain Annexes (Albania, Jordan, Qatar, Algeria, Kenya, Saudi Arabia, Australia, Latvia, Senegal, Azerbaijan, Lithuania, Slovakia, Belarus, Malawi, Sri Lanka, Côte d'Ivoire, Malaysia, Swaziland, Croatia, Mauritius, Sweden, Cuba, Moldova, Togo, Cyprus, Morocco, Tunisia, Czech Republic, New Zealand, Turkey, Finland, Niger, Uganda, France, Nigeria, Ukraine, India, Norway, Zambia and Indonesia, Pakistan, Zimbabwe).

Unusual cross-border movements of gold

363. Both the Precious Metals Act, 2005 as well as the Diamonds Act, 1986 prescribe that permits are required for the importation of precious metals, including gold. Permits for the above materials will only be issued by the Regulator after consultation with the SAPS. In addition, South Africa has boards which assist the authorities in retaining information on precious metals such as the Diamond and Jewellery Councils of South Africa and the South African Diamond and Precious Metals Regulator which issue licenses to the dealers in the sector.

364. Should an unauthorised cross-border movement of gold be detected, the appropriate authorities will liaise with each other. Cooperation takes place in terms of legislation, agreements and informal channels (*e.g.* Interpol). Interpol channels can be used especially in cases where there are no formal agreements in which case the request will be dealt with by Interpol. Where agreements do exists, direct co-operation takes place on an agency to agency basis. For example, the SAPS recently sent a delegation to Greece in respect of stolen jewellery. This was facilitated through Interpol in the absence of a formal cooperation agreement.

365. The first phase of the Customs Border Control Unit (CBCU) has been piloted with Standard Operating Procedures developed with assistance from the United States Customs and Border Protection. CBCU officers have undergone paramilitary training, canine units have been established and x-ray equipment has been procured. Additional equipment is being procured in a phased manner. The legislation for the mandatory submission of advance electronic information is being developed for tabling, and the technology capabilities are being reviewed.

366. Where an offence is detected relating to a false disclosure and the currency is seized, this information is captured and is available to the competent authorities within the current legislative parameters.

Recommendation 30

Structure, funding, staffing and resources (Customs authorities)

367. The SARS (Customs) has a staff complement of approximately 400 officers (20% of Customs establishment) at its various Ports of Entry and Customs Controlled areas that are responsible for the Border control and anti smuggling enforcement interventions. These officers work on customs enforcement priorities which include cash smuggling. The Customs Border Control Unit (CBCU) also has canine teams with detector dogs covering seven disciplines (including currency detection) at the two largest Ports of Entry (O.R Tambo International Airport (traveller) and the Durban Harbour seaport (cargo)). These two ports are responsible for the most significant portions of South Africa's international traveller and trade volumes respectively. The CBCU is being improved to include specialised units for certain enforcement priority areas.

368. The SARS has a recruitment strategy which includes vetting of potential candidates. The development of CBCU capability places an emphasis on training and standard operating procedures which are being developed in line with international best practices. Stringent disclosure standards are in place and an anti corruption strategy exists and is being further developed. SARS has a training academy as well.

369. All SARS officers are required to subscribe to a Code of Conduct. The SARS (Customs) complies with the provisions relating to the Arusha declaration on integrity. Furthermore legislation and policies are in place to minimise compromise of integrity. Examples of such policies are the oath of secrecy, declaration of interest and gift policies. Additionally, SARS officials are also obliged to sign an oath of secrecy and follow a code of conduct. The SARS also has a security unit that includes, amongst others, integrity, ethics and anti-corruption units. The SARS conducts security screening of potential new employees and of employees that apply for different positions within the organisation.

370. The SARS has been exposing its personnel to international forums where money laundering and other types of fraud typologies are discussed and best practices exchanged. The SARS regularly sends officers to the World Customs Organisation (WCO) working groups and committee meetings. SARS officers attend the annual global targeting symposium and FATF meetings. These initiatives are part of the ongoing capacity building programme. Frontline officers also have access to the WCO e-learning platform and SARS has a training academy with courses relating to the predicate offences as they relate to Customs matters. SARS Criminal investigators have attended training events on legislation enacted by Parliament relating to terror financing and money laundering. Additionally, SARS officials are receiving training from United States officials on targeting methodologies.

371. The SARS keeps annual statistics on the following: *(a)* matters referred by the Centre (all such referrals are disseminated); *(b)* seizures of cash being illegally transported across borders; *(c)* tax evasion

cases conducted where money laundering was present or suspected, including records of every request received/made and what revenue was collected.

Financial year	Number of seizures of cash/cash equivalent	Value of seizures	
		ZAR	EUR
2006-2007	84	ZAR 4.56 million	EUR 393 000
2007-2008	5	ZAR 83.14 million	EUR 7.2 million
Financial year ending 2008	140	ZAR 32.2 million	EUR 2.8 million

2.7.2 Recommendations and Comments

372. There is need for South Africa to establish more effective measures to monitor all incoming and outgoing cross-border transportations of currency and BNI.[9] There is a need to establish clearer requirements and procedures to declare inbound BNI above the threshold, and outgoing BNI payable in foreign currency. Bills of entry for cargo and postal declarations should be made available to the Centre.

373. In order to compliment the measures being put in place by the SARS to control cross-border movement of currency and bearer instruments, the proposed amendments to the FIC Act which will enhance that process (including amendments which will make declaration reports available to the Centre and impose sanctions for failing to report cross-border conveyances of currency) should quickly be brought into effect.

374. There is need for the SAPS to retain readily available records and comprehensive records where there is a false declaration or disclosure and there is no seizure, and when there is a suspicion of ML/FT. There should also be more detailed statistics of seizures done according to the offence committed, statistics on seizures relating to tax evasion involving ML, or illegal cross-border transportation of cash.

2.7.3 Compliance with Special Recommendation IX

	Rating	Summary of factors relevant to s.2.7 underlying overall rating
SR.IX	PC	• The following aspects of SR IX are not covered in the case of cross-border transportations by persons or by mail: inbound BNI and outgoing BNI payable in foreign currency. • There are no records kept when: *i)* there is a false declaration or disclosure and there is no seizure; *ii)* there is a suspicion of ML/FT; or *iii)* there is a cross-border transportation of BNI through uninsured mail. • There is not yet a requirement to report threshold movements of currency to the Centre or make the information available to the FIU in some other way, and bills of entry for cargo and postal declarations are not available to the Centre. • The sanctions for failing to report a cross-border conveyance of cash are not yet in force. • There are concerns about the effectiveness of measures to monitor the incoming declaration obligation.

[9] In order to compliment the measures being put in place by the SARS to control cross-border movement of currency and BNI, the proposed amendments to the FIC Act which will enhance that process (including amendments which will make declaration reports available to the Centre and impose sanctions for failing to report cross-border conveyances of currency) should quickly be brought into effect. The extent of enforcement (risk based vs. 100%) to ensure compliance needs to be agreed upon. Additional resources and infrastructure have to be determined and the concomitant budget found.

3. PREVENTIVE MEASURES – FINANCIAL INSTITUTIONS

Preamble: Law, regulation and other enforceable means

375. South Africa had implemented AML/CFT preventative measures through application of the Financial Intelligence Centre Act, 2001 (FIC Act) and two related regulations: the Money Laundering and Terrorist Financing Control Regulations (MLTFC Regulations) and the Exemptions in Terms of the Financial Intelligence Centre Act (Exemptions).

376. The requirements are further elaborated in Guidance Notes issued by the Centre and circulars issued by the SARB, neither of which constitute "other enforceable means" as defined by the FATF. The introduction of each Guidance Note states that, although they are authoritative, the Guidance Notes are intended for information purposes only. The Notes have been issued by a competent authority, in this case the Centre under the authority of the FIC Act. There is no specific range of sanctions associated with non-compliance, although the Banking Supervision Department (BSD) of the SARB checks for compliance with these Notes and exercises its supervisory authority to request information. However, this is insufficient to consider any of the Guidance Notes to be legally enforceable. The Registrar of Banks has also indicated that the Circulars issued by the SARB are not considered to be legally enforceable. Nevertheless, the authorities advise that, in practice, the banks do comply with these instruments and BSD checks for compliance with these Guidance Notes and exercises its supervisory authority to request information.

377. It should also be noted that South Africa's AML/CFT framework is currently undergoing a process of transition. The FIC Act will be substantially amended by the Financial Intelligence Centre Amendment Act, 2008 (FIC Amendment Act) which was gazetted on 28 August 2008. Although these amendments are flagged, where significant, the FIC Amendment Act is not taken into account in the ratings because it will not come into effect until 2009, which is not within the normally accepted time period of two months after the on-site visit.

Customer Due Diligence & Record Keeping

3.1 Risk of money laundering or terrorist financing

378. South Africa's regulatory framework does not directly address the risk of money laundering or terrorist financing and a number of financial activities are not subject to certain AML/CFT requirements. However, these exclusions have not been justified based on demonstrated low risk for ML/FT (see the below discussion of scope issues).

379. BSD addresses the risk of money laundering and terrorist financing in that banks have to submit their AML/CFT Policies and Procedures for verification of compliance with the FATF Recommendations. In instances where these are found to be inadequate, the bank concerned has to indicate a time frame and measures it intends to take to ensure compliance. BSD monitors these plans until a sufficient level of compliance is attained. Regulation 50 of the Regulations Relating to Banks compels banks to ensure that they have and maintain policies and procedures that guard against the bank being used, intentionally or unintentionally, for criminal activities. This includes the prevention and detection of criminal activity *e.g.*

market abuse and financial fraud such as insider trading, market manipulation, money laundering and reporting of such suspected activities to the appropriate authorities. In addition to reporting to the financial intelligence unit or other designated authorities, banks report to the banking supervisor suspicious activities and incidents of fraud when they are material to the safety and soundness or reputation of the bank.

380. Guidance Note 1 issued by the Centre indicates that although the provisions of the FIC Act and the MLTFC Regulations require accountable institutions to identify all clients with whom they do business, they are not required to follow a "one-size-fits-all" approach in the methods and levels of verification applied. The Centre's Guidance Notes 1 indicates that this risk-based approach to verifying customer identification implies that a bank can take an informed decision based on its risk assessment as to the appropriate levels and methods depending on the circumstances. Guidance Note 3 provides further guidance to banks on assessing different levels of risk. Risk factors such as product type, business activity, source of funds, location of client, and transaction value can be taken into account to differentiate between low, medium, and high-risk clients.

381. Under the provisions of the FIC Act, financial institutions are required to establish and verify a customer's identity regardless of the level of risk associated with that customer. However, the Guidance Notes issued by the Centre to financial institutions define the extent to which the risk-based approach can be applied within the current framework by allowing financial institutions to utilise a risk-based approach to determine the level and nature of verification required. For example, unless an exemption applies, all clients must be identified. A risk-based approach may be applied to the verification of a customer's identity, implying that the greater the risk, the higher the level of verification and more secure the methods of verification should be.

382. Financial sector supervisors (SARB and FSB) apply a risk-based approach to supervising the entities under their purview. Section 4(6) of the Banks Act allows the Registrar of banks to implement such international regulatory or supervisory standards and practises as deemed appropriate in consultation with banks. The Registrar has found a risk-based approach to supervising banks and this works for South Africa. See "Ongoing supervision" in Section 3.10 for further details.

Scope issues

383. The FIC Act lists 19 categories of "accountable institutions" which are the categories of banking and non-banking institutions required under the FIC Act to identify customers, keep records, report information and implement internal rules concerning these obligations. The accountable institutions listed in Schedule 1 are:

- a management company registered in terms of the Unit Trusts Control Act, (Act 54 of 1981);
- a person who carries on the "business of a bank" as defined by the Banks Act (Act 94 of 1990);
- a mutual bank as defined in the Mutual Banks Act (Act 124 of 1993);
- a financial instrument trader as defined in the Financial Markets Control Act;
- a person who carries on a "long-term insurance business" as defined in the Long-Term Insurance Act (Act 52 of 1998) including an insurance broker and an agent of an insurer;
- a person who carries on a business for which a gambling license issued by a provincial licensing authority is required;

- a person who carries on the business of dealing in foreign exchange;
- a person who carries on the business of lending money securitized by securities;
- a person who carries on the business of rendering investment advice or investment broking services, including a public accountant defined in the Public Accountants and Auditors Act (Act 80 of 1991) who carries on such a business;
- a person who issues, sells or redeems travellers' cheques, money orders or similar instruments;
- the Postbank;
- a member of a stock exchange licensed under the Stock Exchanges Control Act (Act 1 of 1985);
- a person who has been approved or who falls into the category of persons approved by the Registrar of Stock Exchanges in terms of Section 4(1)(a) of the Stock Exchanges Control Act;
- the Ithala Development Finance Corporation Limited;
- a person who has been approved or who falls into the category of persons approved by the Registrar of Financial Markets in terms of Section 5(1)(a) of the Financial Markets Control Act (Act 55 of 1989);
- a person who carries on the business of a money remitter;
- an attorney as defined in the Attorneys Act, 1979 (Act 53 of 1979);
- an estate agent as defined in the Estate Agents Act, 1976 (Act 112 of 1976); and
- a board of executors of a trust company or any other person that invests, keeps in safe custody, controls or administers trust property within the meaning of the Trust Property Control Act, 1988 (Act 57 of 1988).

384. In relation to the above list of accountable institutions, it should be noted that the Unit Trusts Control Act (UTC Act) was repealed in 2003 and replaced by the Collective Investment Schemes Control Act, 2002 (Act No. 45 of 2002). Similarly, the Stock Exchanges Control Act (SEC Act) and Financial Markets Control Act (FMC Act) were repealed in 2004 when the Securities Services Act (SS Act) came into force. Schedule 1 of the FIC Act was not amended to redefine these accountable institutions in terms of the new legislation. Nevertheless, they remain subject to the terms of the FIC Act because, unless a contrary intention appears, references in one law to repealed provisions in another law must be construed as a reference to any new provisions which have replaced those repealed (Interpretation Act, s.12(1)). There are, however, 43 licensed financial service providers which give investment advice and which do not fall within the category of "accountable institution". Additionally, the following financial institutions are not accountable institutions for the purpose of the FIC Act: finance companies, leasing companies, collective investment scheme custodians, money lenders other than banks, and securities custodians licensed under the FAIS Act (collectively referred to as Uncovered Financial Institutions).

385. These exclusions create a scope issue. Since they are not accountable institutions, the Uncovered Financial Institutions are not subject to the customer due diligence (CDD), record keeping and internal control requirements of the FIC Act. These exclusions have not been justified based on demonstrated low risk for ML/FT. However, as "businesses", they are still subject to the reporting obligations of the FIC Act. These gaps in the scope of the AML obligations affect the ratings relative to some of the Recommendations discussed in Section 3 of this report.

3.2 Customer due diligence, including enhanced or reduced measures (R.5 to 8)

3.2.1 Description and Analysis

386. Uncovered Financial Institutions are not subject to the CDD obligations of the FIC Act. This affects the ratings for Recommendations 5, 6 and 8. Uncovered Financial Institutions do not, however, engage in correspondent banking activity, so the rating for Recommendation 7 is not affected.

Recommendation 5

387. Section 21 of the FIC Act creates obligations for accountable institutions to take certain steps to establish and verify the identity of a customer prior to establishing a business relationship or concluding a single transaction with that customer. This Section also prohibits accountable institutions from concluding transactions with existing customers without first taking certain steps to establish and verify the identity of the customer and to trace all accounts held by the institution that are involved in transactions concluded in the course of that business relationship. The MLTFC Regulations set out in detail the measures to be taken by accountable institutions when establishing and verifying their customers' identities. The regulations are organised in respect of the following categories of customers:

- South African citizens and residents;
- foreign nationals;
- close corporations and South African companies;
- foreign companies;
- legal persons other than a company, close corporation or foreign company;
- partnerships; and
- trusts.

388. There are 17 exemptions to the provisions of the FIC Act and the MLTFC Regulations which are listed in the Exemptions in Terms of the Financial Intelligence Centre Act 38 of 2001.

389. There are general exemptions as well as exemptions that apply specifically to insurance companies, investment providers, members of the exchanges, attorneys and administrators of property, real estate agents, banks and gambling institutions. They permit financial institutions the flexibility of applying reduced or simplified customer due diligence, or in many cases no due diligence, in situations where the ML/FT risk is lower, where information on the identity of the customer and the beneficial owner of the customer is publicly available, or where adequate checks and controls exist elsewhere in the national system. While the provisions of some of the exemptions fit within the FATF framework for reduced or

simplified due diligence, other exemptions are overly broad and have reduced the overall effectiveness of the provisions of the FIC Act and the MLTFC Regulations.

390. The Centre has also issued three guidance notes under Section 4(c) of the FIC Act to provide interpretations in relation to certain aspects relating to the obligations to establish and verify customers' identities. As explained above in the preamble to Section 3, these Guidance Notes do not constitute "other enforceable means" as defined by the FATF.

- Guidance Note 1 "Guidance Concerning the Identification of Clients" issued in April 2004 focuses on the application of the risk-based approach to the identification and verification of customers. It encourages accountable institutions to accurately assess money laundering risks associated with their customer base, products and transactions and develop and implement appropriate identification and verification procedures to mitigate those risks.

- Guidance Note 2 "Guidance to Financial Services Industries Regulated by the Financial Services Board Concerning the Meaning of the Word 'Transaction'" issued in June 2004 provides guidance regarding the definition of transaction with respect to customer identification and verification.

- Guidance Note 3 "Guidance for Banks on Customer Identification and Verification And Related Matters" issued in July 2005 provides additional guidance with respect to client identification and verification and risk management. It also addresses the treatment of politically exposed persons (PEPs) and corresponding banking relationships.

391. Guidance Note 3 is of particular importance to the implementation of CDD requirements. It addresses key issues such as PEPs and correspondent banking. It does so by referencing international standards such as the FATF, the Wolfsberg Principles and the Basel Committee. While language used in the discussion suggests that the application of these standards is mandatory (*i.e.* the use of "should"), it is difficult to determine if the application of the standards cited is mandatory or if they are being provided as "best practice."

Anonymous accounts

392. While there is no specific prohibition against the maintenance of anonymous accounts, Section 21(1) of the FIC Act prohibits an accountable institution from establishing a business relationship or concluding a single transaction with a customer before the accountable institution has taken the prescribed steps to establish and verify: (a) the customer's identity; and (b) as appropriate, the identity of the person acting on behalf of the customer or on whose behalf the customer is acting. In addition, Part 1, Section 2 of the MLTFC Regulations explicitly prohibits accountable institutions from establishing or maintaining a business relationship or conducting a single transaction with a customer who is entering into that business relationship or transaction under a false name. The MLTFC Regulations lay out detailed steps in Sections 3 through 18 for implementing customer identification and verification requirements. The consistent and thorough application of these requirements of the FIC Act and the MLTFC Regulations should effectively prevent the maintenance of anonymous accounts or accounts in fictitious names.

When CDD is required

393. Section 21 of the FIC Act requires that accountable institutions establish and verify the identity of customers before a business relationship can be established or a single transaction concluded with those customers. This would also include occasional transactions above the 15 000 USD/EUR threshold and wire transfers in the circumstances covered by SR VII.

394. There is an exemption to this general rule under Exemption 17 which permits the application of reduced CDD (no address verification) on accounts that enable a customer to withdraw or transfer or make payments of an amount not exceeding ZAR 5 000 per day. Exemption 17 applies only to banks, mutual banks, Post Bank, the Ithala Development Finance Corporation, foreign exchange dealers and money remitters on transactions conducted within the borders of South Africa. This exemption was designed to cover the Mzansi accounts which were introduced to expand financial services to all segments of the population. Given the restrictions on Mzansi accounts generally, this type of account is considered low risk for ML.

395. There is no explicit legal obligation for an accountable institution to undertake customer due diligence measures when there is a suspicion of money laundering or terrorist financing. While the FIC Act requires that a customer be fully identified and verified at the outset of a business relationship or single transaction and the customer's identity will have been already established and verified at the time when a suspicion of money laundering or terror financing arises, there is no specific requirement for the institution to undertake additional CDD. However, the Regulations do require an accountable institution to obtain additional information whenever such information is reasonably required to identify a business relationship or single transaction which poses a particularly high risk of facilitating ML activities or to enable the accountable institution to identify the proceeds of unlawful activity, including ML (MLTFC Regulation 21). This additional information must be adequate to reasonably enable the accountable institution to determine whether these transactions conducted by the customer are consistent with the accountable institution's knowledge of the customer and the customer's business activities.

396. With respect to identification verification, accountable institutions are required to take reasonable steps with respect to an existing business relationship to maintain the correctness of particulars collected under the requirements of Chapter 1 of the FIC Act that are susceptible to change (MLTFC Regulation 19). This implies that accountable institutions are required to ensure that the information obtained and maintained by them with respect to customer verification is correct and take steps to verify customer particulars before continuing with the business relationship or transaction. If the institution is unable to establish and verify the customer's identity to its satisfaction, the further implication is that it will continue its efforts to meet the requirement or take the decision not to engage with the customer. However, there is no explicit obligation under the FIC Act that an accountable institution conduct CDD when it has doubts about the veracity or adequacy of previously obtained customer identification data.

Customer identification and verification

397. Accountable institutions are required to verify the identity of customers (s.21 FIC Act). For South African citizens and residents, the national identification document is an important means of establishing and verifying a customer's identity. Customers wishing to open Mzansi accounts are required to provide them and they are generally the only form of documentation that is utilized by banks and other financial institutions that offer these products. The national identification document has a photograph and a bar code that relates back to the information on the person which is collected and maintained by the National Population Registry. Government authorities are in the process of introducing an updated form of the national identification document. The details of this obligation are expanded by MLTFC Regulations 2 to 18. MLTFC Regulations 4, 6, 8, 10, 12, 14 and 16 set out in detail the various source documents an accountable institution must refer to in order to verify the above mentioned categories of customers.

398. For natural persons, accountable institutions must collect the full name, date of birth, identity number and residential address (MLTFC Regulation 3). These particulars must be verified by reference to a government issued identification document (official ID document for South African citizens/residents; passport for non-citizens/residents) that confirms the person's name, date of birth and identity number. Where an identification document cannot be produced, another document bearing the person's photograph,

full name (or initials and surname), date of birth and identity number may be acceptable, taking into account any relevant guidance notes on the verification of identification (MLTFC Regulation 4). The residential address must also be verified.

399. For legal persons that are companies or close corporations, accountable institutions must collect the following information: the entity's registered name, address and registration number of incorporation; name under which it conducts business; legal form; address of operation or, if it operates from multiple addresses, the address of the head office or office seeking to do business with the accountable institution; and the full names, dates of birth and identity numbers and country (in the case of foreign nationals) of each natural person authorized to act on behalf of the legal person as well as their residential address and contact particulars. The accountable institution is also required to obtain the full names, dates of birth, identity number and residential addresses of: the manager (in the case of a company) or manager of the company's South African operations (in the case of a foreign company); the members (in the case of a close corporation); each natural or legal person, partnership or trust holding 25% or more of the voting rights at a general meeting of the company; and each natural person authorised to conduct business on behalf of the company (MLTFC Regulations 7 and 9). For other legal persons, accountable institutions must collect similar types of identification information (MLTFC Regulation 11).

400. Accountable institutions are required to verify the identification information collected on companies and close corporations, and their legal status as follows. For South African companies, the identification information must be verified by comparison with the most recent versions of the Certificate of Incorporation (form CM1) and the Notice of Registered Office and Postal Address (form CM22) which are certified by the Registrar of Companies and signed by the company secretary (collectively referred to as Valid Incorporation Documents). For close corporations, the identification information must be verified by comparison with the most recent versions of the Certificate of the Founding Statement and Certificate of Incorporation (form CK1) and the Amended Founding Statement (form CK2), if applicable, bearing the stamp of the Registrar of Close Corporations and signed by an authorised member or employee of the close corporation (collectively referred to as Valid Founding Documents). For foreign companies, the identification information must be verified by comparison with official documents of incorporation that were issued by the appropriate authority in the company's country of incorporation (MLTFC Regulations 8 and 10). Accountable institutions are also required to verify any particulars collected against information obtained from any other independent sources if it is believed to be reasonably necessary and, in the case of foreign and domestic companies, to take steps to verify the trade name and business address with information which "can reasonably be expected to achieve such verification" and is "obtained by reasonably practical means" (MLTFC Regulations 8, 10 and 14).[10] However, although the Companies Act, as administered by the Companies and Intellectual Property Registration Office (CIPRO), requires that domestic and foreign companies provide information on each director, including full names, nationality, occupation, residential and business address and date of appointment (form CM29), and lodge copies of the company's memorandum and articles of association, the FIC Act does not require accountable institutions verify the identification information relating to directors and senior management by comparison with the CM29 form filed with CIPRO. For other legal persons, the identification information must be verified by comparison with the entity's constitution or other founding document (MLTFC Regulation 12).

401. For partnerships, similar information is required for every partner including: every member of a partnership; the person who exercises control over the partnership; and each natural person who is authorized to act on behalf of the partnership. Accountable institutions are required to verify the

[10] Guidance Note 1 indicates that the use of the language "can reasonably be expected to achieve such verification" and "is obtained by reasonably practical means" in the Regulations indicates that in these specific instances, the accountable institution must assess what information may be necessary in order to achieve the verification of particulars and the means by which it can be obtained.

identification information collected by comparison with the partnership agreement (MLTFC Regulations 13 and 14).

402. For trusts, accountable institutions must obtain: the identifying name and number of the trust; the address of the Master of the High Court where the trust was registered; and identification information on any legal or natural persons serving as trustees as well as each natural person authorised to act on behalf of the trust, beneficiaries and the founder of the trust. Accountable institutions must verify the identification information received by comparison with the trust deed (or other founding document). Additionally, authorisation provided by the Master of the High Court to each trustee to act in that capacity is required. For trusts created outside of South Africa, accountable institutions are required to obtain an official document issued by an authority in the country where the trust was created which oversees laws relating to trusts in that jurisdiction (MLTFC Regulations 15 and 16).

403. Although the MLTFC Regulations[11] also require accountable institutions to collect and verify the income tax registration numbers[12] of natural and legal persons (regardless of form), and trusts, all accountable institutions are exempted from doing so (Exemption 6(2)). In the case of trusts, Exemption 6(2) also exempts all accountable institutions from verifying the address of the Master of the High Court where the trust was registered.

404. Where another person is acting on behalf of a customer (whether natural or legal), the accountable institution must establish and verify the identity of that person and that person's authority to act on behalf of the customer (s.21(1)(b) FIC Act). Additionally, the accountable institution must obtain proof of the person's authority to act (MLTFC Regulation 17). Guidance Note 3 gives guidance on the types of identifying documents that could be obtained by accountable institutions to meet these requirements, such as power of attorney, mandate, resolution executed by authorised signatories or a court order authorising the third party to conduct business on behalf of the other person (s.12).

Beneficial owner

405. There is no specific requirement in law or regulation that requires accountable institutions to identify beneficial owners (*i.e.* the natural persons who ultimately own and control the customer) or to verify their identities. Although, in some cases, the MLFTC Regulations require the identification of a variety of persons who own, control or are beneficiaries of a customer (as described below), these persons may not be the beneficial owner as that term is defined by the FATF.

406. Accountable institutions are required to establish and verify the identity of any person on whose behalf the customer is acting (s.21 FIC Act) and obtain proof of the customer's authority to so act (MLTFC Regulation 17). However, if the person on whose behalf the customer is acting is a legal person, the accountable institution need not go further to identify the natural person(s) behind that legal person.

407. For companies, an accountable institution must identify and verify the identity of the natural or legal person, partnership or trust holding 25% or more of the voting rights at a general meeting of the domestic or foreign company concerned (MLTFC Regulations 7(f)(ii) and 9(j)). However, if the 25% shareholder is owned by another legal person, the accountable institution is not required to go further (*i.e.* continue identifying parties) with a view to identifying the natural person(s) who is the beneficial owner of that legal person, except on a risk-basis as recommended under Guidance Note 4. Discussions

[11] MLTFC Regulations 3(d), 4(b), 5(e), 6(2), 7(h), 8(d), 9(h), 10(c), 11(d), 12(b) and 15(c).

[12] Official registration numbers, such as tax registration numbers for legal persons, is an example of the type of customer information that could be obtained as suggested in the Basel Committee's General Guide to Account Opening and Customer Identification.

with the private sector indicate that the general practice is not to go beyond the identification of the 25% shareholder at the first level as required by the legislation.

408. For partnerships, every member of the partnership, including so-called "silent partners" and "anonymous partners" must be identified (MLTFC Regulation 13(b)(i)). Likewise, for trusts, the trustees, named beneficiaries and the founder must be identified (MLTFC Regulation 15(d), (e) and (f)). For trusts, an accountable institution is required to identify the founder, trustee and each named beneficiary of the trust (MLTFC Regulation 15). However, if any of these parties is a legal person, there is no further requirement to go further and identify the natural person(s) who own or control that legal person.

409. Members of the JSE Equities Market are required to obtain and maintain sufficient information on each client account and each account operated by a client so as to be able to identify: *(a)* the customer; *(b)* the beneficial owner of a "controlled customer" account if the account holder is not the customer of the member but is the person on whose behalf the customer is acting as agent; and *(c)* the person(s) responsible for placing instructions on the account (JSE Equities Rules 8.6).[13] Members are required to obtain for each customer and beneficial owner of each controlled account of the account holder on whose behalf a customer is acting as agent: *(a)* full name; *(b)* identity or registration number; *(c)* physical and postal address; *(d)* telephone number; and *(e)* customer's legal status.

410. There is no specific requirement to understand the ownership and control structure of a customer that is a legal person or arrangement, beyond the requirements described above to identify: the manager and 25% shareholders of a company; the members of a close corporation; the partners in a partnership; and the founders, trustees and beneficiaries of a trust.

411. The FIC Act does not explicitly require that information on the purpose of a business relationship be obtained. However, under Section 22 (1)(*e*) of the FIC Act, accountable institutions are required to keep a record of the nature of the business relationship established with a customer which would imply an obligation to obtain such information. This requirement covers only the nature of the business relationship but does not address its purpose.

Ongoing due diligence

412. There is no explicit requirement in the FIC Act that accountable financial institutions conduct on-going due diligence on business relationships although elements of such a requirement can be found in the MLTFC Regulations. MLTFC Regulation 19 does require an accountable institution to maintain the correctness of a customer's particulars with respect to customer identification and verification which is susceptible to change. The application of this regulation is discussed further in Guidance Note 3 which recommends that banking institutions consider:

- Applying their know-your-customer (KYC) procedures to existing customers on the basis of materiality and risk, and conducting due diligence reviews of such existing relationships at appropriate times.

- Undertaking regular reviews of their existing customer records. An appropriate time to do so is when a transaction of significance takes place or when there is a material change in the way the account is operated.

[13] Controlled clients have their assets or funds administered by the JSE member. Non-controlled clients are those customers that have appointed their own Central Securities Depository Participant (CSDP) to administer their assets or funds. These customers are usually large institutions or JSE-listed companies or their subsidiaries and as such are considered by the South African authorities to present a lower risk of ML/FT. In addition, they are adequately covered by controls and checks elsewhere in the national system.

- If a bank were to become aware at any time that it lacked sufficient information about an existing customer, taking steps to ensure that all relevant KYC information is obtained as quickly as possible (s.14).

413. Even though meeting these requirements may require some on-going due diligence on the business relationship to maintain the accuracy of customer particulars, the update requirements relate only to customer identification and verification particulars and not to CDD on the overall relationship in general. Furthermore, although Guidance Note 3 suggests a broader application, its application is limited to banks, mutual banks, the Post Bank and the Ithala Development Finance Corporation Ltd. There is also an issue of its enforceability since Guidance Notes, although authoritative, are provided for general information only and there are no specific sanctions associated with non-compliance of their provisions.

414. For banks and controlling companies, "any money laundering activity in which the bank was involved and which was not identified in a timely manner and reported as required by law" is a reportable offense (Regulation 47(3)(*e*) Banks Act). Meeting the requirements of Regulation 47(3)(*e*) of the Banks Act suggests that on-going due diligence would be necessary to identify any reportable offenses that would cover ML activities in which the accountable institution was involved but did not report under the FIC Act requirements in a timely fashion. However, the requirements under the MLTFC Regulations and the Banks Act relate to the identification and reporting of suspicious activities and are not specifically intended to apply to ongoing CDD on the overall business relationship.

415. The Registrar of Banks circulated Guidance Note 3 to the banks as Banks Act Circular 4/2005. While the Circular is not enforceable, the Registrar of Banks has been examining for compliance with Guidance Note 3 as part of its FIC Act compliance reviews, and issuing letters to banks recommending the establishment of guidelines for addressing relationships with PEPs and verifying identities.

Risk

416. There is no specific requirement that accountable institutions apply enhanced due diligence for higher risk categories of customers, business relationships or transactions but South African accountable institutions are required to identify high-risk clients, relationships and transactions and take appropriate steps to manage them accordingly.

417. MLTFC Regulation 21 deals with customer profiling and requires accountable institutions to obtain additional information pertaining to a customer's source of income when this appears necessary concerning a business relationship or single transaction which poses a particularly high risk of facilitating ML activities, or in order to enable the institution to identify the proceeds of unlawful activity or ML. Accountable institutions are required to obtain sufficient information to determine if transactions involving a customer are consistent with the institution's knowledge of that customer and the customer's business activities, including particulars concerning the source of the customer's income and the source of funds which that customer expects to use in conducting a specific transaction or a series of transactions in the course of the business relationship. These requirements relate only to situations where a business relationship or a single transaction poses a high ML risk or the information is needed by the accountable institution to identify the proceeds of unlawful activity or ML; they are not required as part of an on-going CDD program. Although MLTFC Regulation 21 requires accountable institutions to identify high-risk clients as defined in the Regulation, it does not contain specific requirements for performing enhanced due diligence with respect to these customers beyond collecting additional information regarding the source of the customer's income (s.21.3.a) and the source of funds the customer expects to use (s.21.3b).

418. The treatment of high-risk customers is addressed primarily in Guidance Notes 1 and 3 which are issued under Section 4(c) of the FIC Act and considered authoritative, but are provided only for general information. Even though these Notes have been reissued as Circulars by the Registrar of Banks, there are questions regarding their enforceability and there are no specific sanctions associated with a failure to comply with their provisions. Guidance Note 1 applies to all accountable institutions; however, Guidance Note 3 applies only to banks, mutual banks, Ithala Development Finance Corporation Limited and Post Bank.

419. Guidance Note 1 advises accountable institutions of the scope of applying a risk-based approach in respect of the verification of certain information and encourages accountable institutions to organise business relationships and transactions by the level of risk they present and apply measures that are appropriate to address those risk levels (*i.e.* to implement a risk framework). However, the guidance stops short of encouraging the application of ongoing enhanced due diligence in such cases once the customer's identity has been established and verified. The decision to do so therefore becomes risk-based. Where business relationships or transactions are identified as high-risk, the Guidance Note advises that a first step in the process is for the accountable institution to conduct a risk assessment in order to correctly classify risks associated with business relationships and single transactions. In doing so consideration should be given to how the reasonable manager in a similar institution would: (a) rate the risk associated with a particular customer, product and transaction; and (b) what likelihood, danger or possibility can be foreseen of ML occurring with respect to that specific customer profile, product type or transaction. The Guidance views the ultimate risk rating applied to a particular business relationship or transaction as being a function of a broad number of factors relating to a combination of the customer profile, product type and transaction, and recommends that accountable institutions apply a systematic approach to determining different risk classes and identifying criteria to characterise customers and products in conducting their assessments. In particular, the Guidance Note encourages accountable institutions to develop a risk matrix to assist in this effort and notes that where there is the use of language in the MLTFC Regulations such as "can be reasonably be expected to achieve such verification" and "is obtained by reasonably practical means" may be taken as an indication that in those specific instances, a risk-based approach to the verification of customer particulars may be applied. Thus, if the level of risk is high, accountable institutions should apply a higher level of verification and more secure methods.

420. For banks, Guidance Note 3 contains a list of indicators that could be considered unexpected if they relate to certain categories of businesses or have no apparent business purpose given the particular customer's business. Accountable institutions are encouraged to obtain additional information to develop a broad customer profile in these cases to facilitate the identification of suspicious activities or business relationships and transactions that pose a risk of ML/FT (s.4). The issue of PEPs and the Wolfsberg Principles that apply to the identification and treatment of PEPs is also discussed. Guidance Note 3 notes the FATF standards for applying due diligence measures to PEPs such as: obtaining senior management approval for establishing business relationships; applying enhanced on-going monitoring of PEP relationships; and taking reasonable steps to establish sources of wealth and funds of customers and beneficial owners identified as PEPs (s.26). However, beyond this guidance, there is no enforceable obligation for accountable institutions to identify PEPs which are considered by the FATF to be of significant importance as a category of high-risk customers.

Reduced due diligence

421. The application of reduced or simplified CDD is addressed by exemptions made by the Minister of Finance under Section 74 of the FIC Act.

422. Exemption 6(1) permits all accountable institutions to apply reduced CDD to business relationships or single transactions concluded with a public company whose securities are listed on a stock exchange listed in the Schedule to the Exemptions. Listed companies are generally subject to their exchange's regulatory disclosure and AML/CFT requirements, and information on such companies is generally publicly available. In such cases, accountable institutions may apply reduced CDD. In particular, they are exempt from having to collect and verify: the business name; registered address of the company; and name, date of birth, ID number, nationality or residential address of managers, members, authorised representatives and 25% shareholders. This exemption does not apply in circumstances that give rise to the accountable institution considering whether to file an STR (s.18 Exemptions).

423. Exemption 9 permits securities market participants to conduct simplified CDD in relation to business relationships or transactions with legal persons who are non-controlled clients. In such cases, the accountable institution does not need to conduct CDD (ID or verification) on the managers, members, authorised representatives and majority (25%) shareholders of the customer (name, date of birth, ID number, nationality, residential address), or conduct associated record keeping. Non-controlled clients, which account for the majority of broker business, process payments for share trades through the banking system while the underlying shares (script) is held by a bank (securities depository). This means that the broker never physically handles the transaction and the JSE sees the entire trade. This type of securities transaction differs significantly from transactions involving controlled clients (the customer physically brings the shares to the broker who stores them, finds a buyer, collects the money and physically hands the shares to the buyer). In the case of a non-controlled client, a JSE member never receives funds or securities from the client. The client deposits funds and securities with its Central Securities Depository Participant (CSDP) and all settlement takes place through the CSDP. The bank is therefore the only party that sees the flow of funds and securities and is able to identify the source of those funds and securities. As an accountable institution, the bank acting for the non-controlled client is responsible for complying with all the requirements of the FIC Act in relation to that client.

424. Exemption 17 permits the application of reduced CDD to special accounts such as the Mzansi accounts. The Mzansi account was launched by the South African Government in 2004 as part of a national effort to increase access to financial services. Mzansi accounts have no management fees and there are limits on the balance held in the account as well as on the amounts that can be transferred out of the account on a daily and monthly basis, in keeping with the requirements of Exemption 17. In order to make these accounts available to more customers, accountable institutions are only required to establish the customer's identity and verify it by using the South African identification document. However, they are not required to verify addresses. Government authorities believe that the ML/FT risks associated with this product is low because of the limits placed on account activity and the fact that the customers using these accounts present a low risk of ML/FT. As of November 2007, there were 4.24 million such accounts held by South African accountable institutions.

425. Exemption 17 applies only to banks, mutual banks, the Post Bank, the Ithala Development Finance Corporation Ltd and money remitters but only in respect of transactions where both the sending and receiving of funds takes place in South Africa (*i.e.* the accountable institutions to which Exemption 17 applies). This exemption applies to business relationships (such as Mzansi accounts) and single transactions that enable the customer to withdraw, transfer or make payments of an amount not exceeding ZAR 5 000 per day and not exceeding ZAR 25 000 in a monthly cycle, and does not enable the customer to transfer funds to any destination outside of South Africa (except for point-of-sale payments or cash withdrawals in a country in the Rand Common Monetary Area). The accounts that qualify for this exemption must not have a balance exceeding ZAR 25 000 at any time and the same person cannot hold two or more of these accounts at the same time. Customers holding an account with a balance exceeding the threshold or holding more than one account with the same institution are subject to the full customer

identification and verification requirements, and the related recordkeeping provisions of Sections 21 and 22 of the FIC Act.

426. The Mzansi Account, a basic bank account with limited functionality was developed in the context of the Financial Sector Charter (FSC). The FSC is a joint effort by Government and the financial industry to provide financial services (banking/insurance/credit etc) to the previously excluded population. This product is tailored to meet specific needs of a particular income group, requiring limited functionality of deposit taking,withdrawals and domestic remittance services.

427. The features of the account reflect the following risk parameters that are considered by the authorities to constitute low risk:

- **Type of customer**: the product is only available to natural persons.
- **Nationality of the customer**: the customer must be a South African Citizen or resident.
- **Limited to domestic transactions:** cross border transfers are not permissible, except for point of sale payments or cash withdrawals in the Rand Common Monetary Area.
- **Monetary limits**: There is a daily limit on withdrawals, transfers and payments. A capped monthly limit also applies. In addition there is a limit on the balance that maybe maintained in this account. The customer is restricted from maintaining more than one such account at an institution.

428. In order to ensure the successful implementation of this product, an exemption from certain measures required by the FIC Act (Exemption 17) was carved out based on the risk parameters discussed above. It was recognised that full CDD, in particular, obtaining and verifying a residential address was not feasible given that most people in the intended target market typically did not have residential addresses that could be confirmed by reference to formal documentation. Such a requirement would have precluded most individuals in the intended target market from accessing this product.

429. This exemption does not absolve institutions from other obligations such as establishing and verifying the customer's identity based on the official bar-coded South African ID book and requiring the institution to request other information such as the source of income and funds. Furthermore, in cases where a customer exceeds the account limits, the accountable institution is then required under the exemption to conduct full CDD in accordance with the FIC Act before completing any additional transactions associated with that customer's account.

430. Mzansi accounts can only be obtained through banks and the Postbank and transactions can only be conducted through the banking system or the country's network of post offices. This permits authorities to effective track activities associated with these accounts and enforce established limits. The advent of this product has brought millions of new customers into the formal banking system and has, in effect, expanded the reach of South Africa's AML/CFT regime.

Full exemption from CDD

431. The FATF Recommendations allow for simplified or reduced CDD measures where there are low ML/FT risks. However, parts of the following exemptions do not comply with the FATF Recommendations in that they fully exempt certain accountable institutions – which should be subject to the FATF Recommendations – from all CDD requirements (as well as some or all record keeping requirements). Moreover, there appears to be no research, typologies or analyses that would justify these full exemptions on the basis of a proven low ML/FT risk. One such exemption applies to all accountable

institutions, two such exemptions apply to the banking sector (Exemptions 15 and 16), two apply to securities market participants (Exemptions 7(2) and 8) of which only parts are problematic, and one applies to the insurance sector and investment providers (Exemption 7(1)).

432. Exemption 4 applies where two accountable institutions located in South Africa are doing business. Exemption 4 fully exempts an accountable institution (the "secondary" institution) from all CDD and associated record keeping requirements on business relationships/single transactions that are established with another accountable institution (the "primary" institution) acting on behalf of its customer, provided that the primary institution confirms in writing to the satisfaction of the second institution that it has established and verified the customer's identify in accordance with Section 21 of the FIC Act, or in accordance with its own internal rules and procedures for implementing Section 21. Since Exemption 4 applies only to institutions located in South Africa, the implication is that the secondary institution can be assured that the primary institution is regulated in accordance with South African MLTFC Regulations and that the measures established by the primary institution comply with the FIC Act. Exemption 4 implies that if the secondary institution is not satisfied with the written confirmation provided by the primary institution, it should undertake its own customer identification and verification pursuant to Section 21 of the FIC Act. In this case, the customer of the secondary institution is the primary institution which is acting on behalf of its own customer.

433. Exemption 15 and 16 exempt banks (including mutual banks, Postbank and the Ithala Development Finance Corporation Limited) from conducting any CDD and related record keeping in relation to the following types of business:

(a) Unsecured loans not exceeding ZAR 15,000 which are made to a customer with whom that accountable institution has a business relationship (Exemption 15). South African authorities explained that this was a way to allow accountable institutions to compete with microfinance institutions, which provide this service and are not yet covered under the FIC Act.

(b) Business relationships with another financial institution that provides similar services and is located in a country where, to the satisfaction of the relevant supervisory body, it is subject to equivalent AML regulation and supervision. Although the relevant supervisory bodies have not formally designated any such countries as "equivalent" in terms of this exemption, in practice accountable institutions are applying Guidance Note 3 and treating FATF countries as having equivalent AML/CFT regulatory regimes, thereby fully exempting them from CDD and related record keeping requirements.

434. Exemption 7(1) exempts insurance agents and brokers, investment advisers and brokers and management companies (unit trusts) from conducting any CDD and related record keeping in relation to certain products. Several situations in this Exemption (reinsurance policies issued to another accountable institution, and long-term insurance or assistance policies which only pay out benefits upon death, disability, or injury to the beneficiary) fall outside of the category of "financial activity' as defined by FATF. However, the following Sections of this Exemption are problematic:

- Long term insurance policies, annuities or unit trusts/linked product investments held by pension/retirement funds, where the policy holder is approved in terms of the Income Tax Act.

- Contractual agreements to invest unit trusts/linked product investments with recurring payments which do not exceed ZAR 25 000 (EUR 2 145) annually or a once-off consideration not exceeding ZAR 50 000 (EUR 4 300), provided that full CDD and associated record keeping is done in respect of every client who liquidated whole/part of the investment within one year of making the first payment.

- Long term insurance policies for which the surrender value does not exceed 20% of the value of the premiums paid in respect of that policy within the first three years.

- Long term insurance policies with recurring premiums which do not exceed ZAR 25 000 (EUR 2 145) annually or in respect of which a single premium not exceeding ZAR 50 000 (EUR 4 300) is payable, provided that full CDD and associated record keeping is done in respect of every client who: increases the recurring premiums beyond this threshold; or borrows from the accountable institution against the security of the policy; or surrenders the policy within three years. It should be noted that these annual and single premium thresholds greatly exceed the examples cited in the FATF methodology of the types of insurance policies that may be considered low risk, and there is no research, typology or other documentation that would support the conclusion that these types of policies are, nevertheless, also low risk.

435. Exemption 7(2) fully exempts securities market participants that are accountable institutions from conducting any CDD and related record keeping in relation to transactions in securities listed on a stock exchange, performed on behalf of a pension, provident or retirement annuity fund.

436. Exemption 8 fully exempts securities market participants that are accountable institutions from conducting any CDD (ID or verification) in the following circumstances. When an accountable institution enters into a relationship with a person (natural or legal) who is located abroad and is acting on behalf of a client, the accountable institution is fully exempt from performing any CDD (ID or verification) in respect of the person's client if: (a) the person is located in a country where the national AML regulation and supervision is considered by the relevant South African supervisory body to be equivalent to South Africa's regime; and (b) the person confirms in writing to the satisfaction of the accountable institution that the person obtained and recorded the identities of all such clients in the manner required by that country's AML legislation.

437. A further concern is that the full exemptions from CDD and related record keeping in Exemptions 7, 8, 15 and 16 would also apply in cases where an accountable institution is considering filing a suspicious transaction report. This is in contrast to Exemptions 5, 6, 9 and 13 which explicitly do not apply in any circumstances where an accountable institution is considering filing a report pursuant to Section 29 of the FIC Act which deals with suspicious and unusual transactions (unless to do so would prejudice an investigation) (paragraph 18, Exemptions). Nevertheless, Exemption 5 still impacts the ability of an accountable institution to detect a suspicion of ML/FT which, pursuant to R.5, should trigger the obligation to undertake CDD measures. This is because the accountable institution is impeded in its ability to detect suspicious transactions since there is no requirement for the institution abroad (which conducted the CDD) to provide it with the CDD information and the accountable institution is not subject to a requirement to conduct ongoing due diligence. See Section 3.3 of this report for a full discussion of Exemption 5.

Timing of verification

438. Accountable institutions are required to establish and verify a customer's identity before establishing a business relationship (s.21 FIC Act). Nevertheless, Exemption 2 allows some flexibility around the timing of verification. An accountable institution may accept a mandate (or take similar preparatory steps) from a prospective customer, with a view to establishing a business relationship or concluding a single transaction, before the customer's identity has been verified on condition that the accountable institution will have completed all necessary steps to verify the customer's identity before concluding a single transaction. However, there is no obligation to identify the beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers.

Failure to satisfactorily complete CDD

439. Accountable institutions in South Africa are not permitted to establish a business relationship, open an account, conduct transactions or otherwise allow a customer to utilise a business relationship before the customer's identity has been verified in accordance with Section 21 of the FIC Act. However, once a business relationship has been established, there is no specific requirement to terminate the business relationship or to consider filing an STR if doubts about the veracity or adequacy of previously obtained customer identification data arise.

440. Guidance Note 4 suggests that accountable institutions should consider the following circumstances as indicators of suspicious activity that should be considered when determining whether to file an STR: customers opening accounts with false or fictitious documents; providing doubtful or vague identification information; refusing to produce personal identification documents; providing supporting documents that lack important details such as contact particulars; or presenting foreign documentation that cannot be checked (s.4.1). However, this Guidance Note is unenforceable.

Existing customers

441. An accountable institution is required to establish and verify the identity of all customers with whom it had entered into a business relationship before the FIC Act took effect (so-called "existing customers"). In particular, accountable institutions are not permitted to conclude transactions for existing customers unless the accountable institution has taken the prescribed steps to: *(a)* establish and verify the identity of the customer; *(b)* establish and verify the identity of a person acting on behalf of the customer, including verifying the person's authority to act; *(c)* establish and verify the identity of anyone on whose behalf the customer may have been acting, including verify the customer's authority to act; and *(d)* trace all the accounts at the accountable institution that are involved in transactions concluded in the course of that business relationship (s.21(2) FIC Act).

442. In addition, Guidance Note 3 (which is unenforceable and only applies to banks) sets out the following procedures which may be applied based on an institution's risk framework:

- Banks should apply their KYC procedures to existing customers on the basis of materiality and risk, and conduct due diligence reviews of such existing relationships at appropriate times.

- Banks need to undertake regular reviews of their existing customer records. An appropriate time to do so is when a transaction of significance takes place or when there is a material change in the way the account is operated.

- If a bank becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant KYC information is obtained as quickly as possible (s.14).

Recommendation 6

443. There is no enforceable obligation for accountable institutions to identify politically exposed persons (PEPs) or take other such as measures as indicated in Recommendation 6.

444. In July 2005, the Centre issued Guidance Note 3 "Guidance for banks on customer identification and verification and related matters" under Section 4(c) of the FIC Act in 2005. Guidance Note 3 is only applicable to banks, mutual banks, Post Bank and the Ithala Development Finance Corporation Limited. Discussions with representatives of security firms and insurance companies confirmed their understanding

that this Guidance only applies to banks. Although Guidance Note 3 is comprehensive, it cannot be considered to be either law, regulation or other enforceable means. Its preamble states that "the guidance provided by the Centre in this Guidance Note although authoritative, is provided as general information only." The language used in Section 25 which relates to PEPs cites the Wolfsberg Principles best practice guidance rather than any South African legal authority as the basis for the practices discussed in the Section. In addition, the Guidance discusses the application of practices for the identification and treatment of PEPs as beneficial owners in the absence of a legal or regulatory requirement within the jurisdiction to identify beneficial owners. There are no specific sanctions associated with a failure to comply with this Section of the Guidance.

445. The Registrar of Banks circulated Guidance Note 3 to the banks as Banks Act Circular 4/2005. However, the Circular is not enforceable either. Even so, the Registrar of Banks has been examining for compliance with Guidance Note 3 as part of its FIC Act compliance reviews, and issuing letters to banks recommending the establishment of guidelines for addressing relationships with PEPs and verifying identities.

446. Guidance Note 3 defines a PEP and describes the best practice guidance provided under the Wolfsberg Principles with respect to the identification of domestic and foreign PEPs, including paying special attention to family members and close associates of PEPs (*e.g.* spouses, children, parents, siblings, and other blood relatives and relatives by marriage) (ss.25-27). The guidance note encourages banks to: establish appropriate risk management systems to determine whether a customer, potential customer or beneficial owner is a PEP; treat PEPs as high-risk clients; and conduct proper due diligence on PEPs, persons acting on their behalf, family members and close associates. In addition, banks should: *(a*) obtain senior management approval for establishing a business relationship with a PEP and, in cases where a relationship already exists, banks should obtain senior management approval to continue the relationship; *(b)* take reasonable measures to establish the source of wealth and the source of funds for customers and the beneficial owners identified as PEPs; and *(c)* conduct enhanced ongoing monitoring of a relationship with a PEP. The guidance note further indicates that it is crucial for banks to address the issue of PEPs in their risk framework and group AML policy. As a higher-risk customer, a PEP should be subject to enhanced due diligence and heightened scrutiny whenever PEPs, their family members or close associates are contracting parties, beneficial owners of assets, or have control over the disposal of assets by virtue of power of attorney or signature authorisation.

Additional elements

447. South Africa signed and ratified the United Nations Convention Against Corruption (UNCAC) in 2004. South Africa has implemented all of the mandatory requirements of the UNCAC through promulgation of the Prevention and Combating of Corrupt Activities Act, 2004 (PRECA Act).

Recommendation 7

448. There is no specific obligation in law or regulation for accountable institutions to conduct enhanced due diligence on cross border correspondent banking and other similar relationships.

449. Guidance Note 3 (which is not enforceable) encourages banks to avoid doing business with shell banks and pay particular attention to relationships with respondent banks located in jurisdictions that have weak KYC standards or have been identified by the FATF as being "non-cooperative". In particular, Guidance Note 3 refers banks to the requirements of FATF Recommendation 7:

- to gather sufficient information about a respondent bank to understand fully the nature of its business and to determine from publicly available information its reputation and the quality of its

supervision, including whether the respondent bank has been subject to ML/FT investigation or regulatory action;

- to assess the respondent bank's AML/CFT controls;
- to obtain approval from senior management before establishing new correspondent relationships;
- to document the respective responsibilities of each bank; and
- with respect to "payable-through accounts", to be satisfied that the respondent bank: has verified the identity of and performed on-going due diligence on the customers having direct access to its accounts; and is able to provide relevant customer identification data upon request to the correspondent bank.

450. Banks are also encouraged to take into account the Basel Committee Core Principles which recommend that banks only establish correspondent relationships with foreign banks that have effective customer acceptance and KYC policies in place, and are subject to effective AML supervision by relevant authorities (s.28). The Guidance Note also refers banks to the Wolfsberg Principles on risk indicators, encouraging reasonable due diligence and enhanced due diligence on the correspondent banking customer's domicile, ownership and management structures, business and customer base.

451. Although Guidance Note 3 provides a comprehensive discussion of the measures to be taken by banks in South Africa to ensure that their correspondent banking relationships are in keeping with international standards as defined FATF Recommendation 7, the Basel Committee on Banking Supervision's Core Principles and the Wolfsberg Principles, none of these requirements are based in law, regulation or other enforceable means (see Recommendation 6 above for more details). Additionally, Exemption 16 suggests that a full exemption from conducting CDD or related record keeping may be available with respect to correspondent banking relationships if they are established with financial institutions that are located in countries designated by the relevant supervisor – the SARB in this case – as being subject to equivalent AML regulation and supervision (see Recommendation 5 above for more details).

Recommendation 8

452. There are no specific legal or regulatory requirements for accountable institutions to have policies in place to address the potential abuse of new technological developments for ML/FT. Although the Electronic Communications and Transactions Act of 2002 makes it an offence to obtain unauthorized access to, interfere with or unlawfully and intentionally intercept data (s.86), this and other related provisions in the Act are focused only on the general protection of consumers and do not focus on AML/CFT vulnerabilities specifically.

453. With respect to non face-to-face transactions generally, accountable institutions are required to take reasonable steps to establish the existence of the customer, or to establish or verify the identity of the customer (MLTFC Regulation 18). However, this requirement does not extend to when conducting on-going due diligence, as is required by Recommendation 8. Additionally, there is no elaboration of how this general requirement should be applied, other than in the context of the banking sector and in relation to cell phone products, as described below.

454. Guidance Note 3 (which only applies to banks and is not enforceable) expands on the provisions of MLTFC Regulation 18 by citing the Basel Committee Core Principles encouraging banks to apply equally effective customer identification procedures and on-going monitoring standards for non-face-to-

face customers. It encourages banks accepting customers on a non face-to-face basis to apply: *(a)* customer identification procedures to non face-to-face customers that are as effective as those applied to customers with whom personal contact has been made; and *(b)* specific and adequate measures to mitigate the higher risks presented by such customers (s.9). The Guidance cites examples of risk mitigating measures from the Core Principles such as: certification of documents presented; third party introduction; independent contact with the customer by the bank; and requirement for documents in addition to those normally required from face-to-face customers. Faxed documents which are certified true copies of the originals are acceptable, but an accountable institution would be required to take appropriate steps to confirm that the documents do indeed relate to the particular customer (s.10).

455. Circular 2006/6 provides further guidance for banks in relation to cell phone banking products, noting that these products have the potential to be abused since they are opened primarily through a non face-to-face process (although as discussed above in Recommendation 6, banking circulars are also not enforceable). Cell phone banking products in South Africa meet the requirements of Exemption 17 (*i.e.* single transaction limits of ZAR 5 000 per day, not exceeding monthly transaction limits of ZAR 25 000; and no funds transfers outside of South Africa, except for point-of-sale payments or cash withdrawals in a country in the Rand Common Monetary Area).[14] As described above in Recommendation 5, Exemption 17 allows banks to apply reduced CDD – in particular, the residential address of the customer does not need to be verified. To mitigate the particular risks of applying Exemption 17 to the non-face-to-face context of cell phone banking, Circular 2006/6 suggests that banks apply a minimum set of criteria to minimise the risk of ML/FT abuse. Such criteria include: ensuring that all of the conditions for Exemption 17 are met; making the product available only to South African citizens and residents with South African identity numbers; and ensuring that the account opening procedure includes adequate steps to verify the identity of the customer by cross referencing third-party databases which include the names and identity numbers of persons sourced from the Department of Home Affairs. The process must enable the bank to establish: if the identity number provided by the customer is valid and relates to the customer's name; that the person to whom the identity number relates is not deceased and has not emigrated from South Africa; and that the name and identity number of the applicant does not appear on a database of fraud convictions. The Circular further advises accountable institutions to apply enhanced due diligence measures with respect to transaction activities associated with cell phone banking products in terms of identifying and reporting suspicious activities.

456. Circular 2006/6 further states that an accountable institution may open an account without face-to-face contact and verification of the customer's identity during the account opening process where low-value transactions and debits from the accounts are limited to ZAR 1 000 per day (which is below the threshold established by Exemption 17). If an account opened in a non face-to-face process exceeds this threshold, the accountable institution must apply the requirements of Exemption 17 and conduct face-to-face customer identification and verification. The customer identification and verification requirements of the FIC Act apply in full in cases where the customer exceeds the thresholds established under Exemption 17.

457. In conjunction with Exemption 17, Circular 6/2006 imposes limits on transaction sizes and types of eligible customers, restrictions on destinations and requirements for enhanced due diligence on these relationships for reporting purposes. By restricting the number of accounts that can be used by customers, the Circular is addressing the potential for breaking large transactions into smaller amounts and transferring them from multiple accounts.

[14] The Common Monetary Area (CMA) includes South Africa, Lesotho, Swaziland and Namibia.

458. It should also be noted that, in terms of implementation, South Africa went beyond the FATF requirements in that they imposed a requirement to reidentify all existing customers (not just on the basis of materiality and risk). This work is completed and was a significant undertaking that positively contributes to South Africa's overall implementation of CDD measures. For further information on the results of the inspection process to verify compliance with CDD measures, refer to Section 3.10 of this report.

3.2.2 Recommendations and Comments

459. While South Africa has taken some substantial measures to address the FATF requirements related to Recommendations 5 through 8, South African authorities are recommended to take the following measures to enhance the effectiveness of the existing AML/CFT regime:

- Apply adequate CDD requirements to financial institutions that are not currently "accountable institutions" under the FIC Act.

- Institute a primary obligation to identify beneficial owners (including the natural person that ultimately owns or controls the customer, as well as understanding the ownership and control structure of customers that are legal persons) of accounts beyond the current requirement of identifying 25% shareholders of legal persons.

- Review the provisions of the current Exemptions to ensure that current practices of exempting full CDD requirements in situations where the application of simplified or reduced due diligence would be more appropriate are addressed.

- Institute explicit requirements to conduct enhanced due diligence when there is a suspicion of ML or FT, if there are doubts about previously obtained CDD data, and with respect to high-risk customers and transactions.

- Establish an explicit obligation for accountable institutions to conduct general on-going due diligence on business relationships and reducing the existing reliance on the obligations under the FIC Act to file an STR and the Regulations to update customer identification and verification particulars to serve this purpose.

- Introduce a primary obligation for accountable institutions to identify PEPs and to apply enhanced due diligence with respect to these relationships and transactions conducted as a result of them.

- Establishing a specific, enforceable requirement for a bank to perform CDD measures on its respondent institutions and gather sufficient information to fully understand the nature of its respondents' business, the respondents' reputation and the quality of AML/CFT supervision being applied to those institutions.

- Introduce explicit requirements for accountable institutions to have policies in place or take measure as needed to prevent the misuse of technological developments by money launderers and terrorist financiers. While, the SARB's issuance of a Circular with respect to cell phone banking products represents progress in this area, establishing an explicit requirement applicable to all accountable institutions is still necessary.

3.2.3 Compliance with Recommendations 5 to 8

	Rating	Summary of factors underlying rating
R.5	PC	• No specific legal obligation for an accountable institution to undertake CDD when there is a suspicion of money laundering or terrorist financing or when it has doubts about the veracity or adequacy of previously obtained customer identification data. • The FIC Act does not require accountable institutions to verify the identification information relating to directors and senior management by comparison with the CM29 form filed with CIPRO. • No specific requirement in law or regulation that requires accountable institutions to identify beneficial owners (*i.e.* the natural persons who ultimately controls and owns the customer) or to verify their identities. Therefore, there is no obligation to identify the beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. • No specific requirement to understand the ownership and control structure of a customer that is a legal person or arrangement, beyond the requirements described above to identify: the manager and 25% shareholders of a company; the members of a close corporation; the partners in a partnership; and the founders, trustees and beneficiaries of a trust. • No explicit requirement that information on the purpose of a business relationship be obtained. • There is no explicit requirement to conduct on-going due diligence. • There is no specific requirement that accountable institutions apply enhanced due diligence for higher risk categories of customers, business relationships or transactions. • Certain exemptions do not comply with the FATF Recommendations in that they fully exempt certain accountable institutions from all CDD requirements (as well as some or all record keeping requirements). In addition: o For insurance exemptions, the annual and single premium thresholds greatly exceed the examples cited in the FATF methodology of the types of insurance policies that may be considered low risk. o A further concern is that the full exemptions from CDD and related record keeping in Exemptions 7, 15 and 16 would also apply in cases where an accountable institution is considering filing a suspicious transaction report. • Once a business relationship has been established, there is no specific requirement to terminate the business relationship or to consider filing an STR if doubts about the veracity or adequacy of previously obtained customer identification data arise. • Uncovered Financial Institutions are not subject to the CDD obligations of the FIC Act.
R.6	NC	• No enforceable obligation for financial institutions to identify politically exposed persons (PEPs) or take other such as measures as indicated in Recommendation 6.
R.7	NC	• There is no specific obligation in law or regulation for accountable institutions to conduct enhanced due diligence on cross border correspondent banking and other similar relationships.
R.8	PC	• There are no specific legal or regulatory requirements to have policies in place to address the potential abuse of new technological developments for ML/FT. • The general requirements for non face-to-face customers do not extend to when conducting on-going due diligence. Additionally, there is no elaboration of how this general requirement should be applied other than in the context of the banking sector and in relation to cell phone products. • Uncovered Financial Institutions are not subject to the CDD obligations of the FIC Act.

3.3 Third parties and introduced business (R.9)

3.3.1 Description and Analysis

460. Uncovered Financial Institutions are not subject to the CDD obligations of the FIC Act. This affects the rating for Recommendation 9. In addition, there is one exemption that relates to reliance on third-party customer identification and/or verification.

461. Exemption 5 provides that a South African institution may, for verification purposes, rely on a confirmation of a customer's identity by a regulated institution in a foreign jurisdiction. This applies where a foreign customer engages directly with a South African institution and the South African institution is assisted in the verification process by obtaining confirmation of the customer's identity from a foreign institution.

462. Specifically, Exemption 5 exempts the South African accountable institution from the requirement to verify the CDD information collected pursuant to Section 21 of the FIC Act where: *(a)* the customer is located in a country where the national AML regulation and supervision is considered by the relevant South African supervisory body to be equivalent to South Africa's regime; *(b)* a person/entity subject to the other country's regime confirms in writing, to the satisfaction of the secondary institution, that it has verified the customer's particulars in accordance with Section 21 of the FIC Act; and *(c)* the person/entity undertakes to forward all the documents obtained in the course of verifying the customer's particulars to the South African accountable institution. While this exempts customer *verification*, this does not exempt the accountable institution from establishing the customer's identity as required in Section 21 of the FIC Act – *i.e.* the customer must still supply identification information.

463. No official determinations have been made by any South African supervisory authority with respect to countries whose AML regulation and supervisory regimes can be considered to be equivalent to South Africa's, which according to South African authorities indicates that accountable institutions cannot apply the exemption. Nevertheless, the private sector appears to be applying Exemption 5 in terms of Guidance Note 3 which suggests that all FATF members are considered to have adequate AML legislation and supervision of compliance with such legislation (s.29). Some accountable institutions are thus applying Exemption 5 and fully exempting from verification all customers from FATF membership countries, without any requirements to satisfy themselves of the adequacy of applicable AML/CFT measures. However, Guidance Note 3 only applies to the banking sector and is not binding in any event because it does not fall within the FATF's definition of "other enforceable means". Therefore, the voluntary application of this Guidance by the private sector does not affect the rating. A further problem is that Exemption 5 does not require the foreign institution to forward the relevant customer identification information immediately. There is also no requirement for the accountable institution to ensure that copies of customer identification data and other relevant documentation relating to CDD requirements will be made available from the foreign primary institution without delay. Guidance Note 3 (which, as noted above, is unenforceable) only suggests that this should occur "in due course" (s.30). The division of obligations of the two institutions in terms of Exemption 5 should be clarified.

3.3.2 Recommendations and Comments

464. South Africa should adopt specific measures to implement the requirements of Recommendation 9, and these measures should extend to all financial institutions, including Uncovered Financial Institutions. The institution relying on third-party identification and/or verification should be required to immediately obtain from the third party the relevant information and satisfy itself that copies of the customer identification and verification information are made available to it by the primary institution.

465. In addition, there should be a more definitive timeline attached to the "undertaking" to forward the appropriate information in Exemption 5(*c*) to ensure that the accountable institution relying on the third-party verification obtains the relevant CDD documentation immediately and that the other accountable institution be under an obligation to provide that information within that time frame.

466. South African authorities should include a specific obligation on accountable institutions relying on customer identification and verification undertaken by third parties (whether those third parties are other South African accountable institutions or foreign institutions) indicating that they are ultimately responsible for customer identification and verification even though they may be satisfied by the services provided by the third parties.

3.3.3 Compliance with Recommendation 9

	Rating	Summary of factors underlying rating
R.9	NC	• Exemption 5 does not require the institution relying on third-party verification/identification to immediately obtain the relevant CDD information. • Exemption 5 does not require the accountable institution 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." • For Exemption 5, there is no explicit requirement that the financial institution satisfy itself of the adequacy of applicable AML/CFT measures applicable to the foreign financial institution. • Despite the lack of determinations by relevant supervisory bodies, some accountable institutions are applying Exemption 5 and fully exempting from verification requirements all customers from FATF membership countries. • Uncovered Financial Institutions are not subject to the CDD obligations of the FIC Act.

3.4 Financial institution secrecy or confidentiality (R.4)

3.4.1 Description and Analysis

467. South Africa does not have secrecy laws pertaining to the information held by financial institutions. In terms of common law, the standard terms of a contract between a customer and a financial institution include an obligation on the financial institution to hold the customer's information confidential. Case law confirms that this contractual obligation is not absolute. For example, see the cases of G S George Consultants and Investments (Pty) Ltd and Others v Datasys (Pty) Ltd 1988 (3) SA 726 (W) (at 736 G) which apply the principle laid down in the English case of Tournier v National Provincial and Union Bank of England [1924] 1 KB 461 (CA).

468. The obligation of confidentiality can therefore be overridden by, among others, due process of law, court order, a number of statutory provisions and the interests of the institution itself. In particular, the CPA, POCA and FIC Act all enable investigators to access a customer's financial records. Legislation also allows supervisory bodies to access information held by financial institutions in client records. Secrecy provisions do not inhibit the sharing of information between financial institutions where this is required by R.7, R.9, or SR.VII.

3.4.2 Recommendations and Comments

469. This Recommendation is fully observed.

3.4.3 Compliance with Recommendation 4

	Rating	Summary of factors underlying rating
R.4	C	This Recommendation is fully observed.

3.5 Record keeping and wire transfer rules (R.10 & SR.VII)

3.5.1 Description and Analysis

Recommendation 10

Transaction and customer identification records

470. Uncovered Financial Institutions are not subject to the record keeping obligations of the FIC Act. This affects the ratings for Recommendation 10.

471. Accountable institutions are required to keep records of information pertaining to customer identification and transactions whenever they establish a business relationship or conclude a transaction, including single transactions or transactions conducted in the course of the business relationship (s.22 FIC Act). Such records must be kept for at least five years from the date on which the business relationship is terminated (in the case of a business relationship) or transaction was concluded (s.23 FIC Act). Although it is implied in the FIC Act that records can be kept for longer than five years, there is no specific allowance for records to be maintained for a period longer than five years if requested by a competent authority.

472. In particular, accountable institutions are required to keep the following information and documentation related to CDD and the particulars of transactions:

- the identity of the customer;
- the identity of any person on whose behalf the customer is acting, including the customer's authority to so act;
- the identity of any person who is acting on behalf of the customer, including that person's authority to so act;
- the manner in which the identities of these persons were established;
- the nature of the business relationship or transaction;
- the amounts involved and the parties to transactions;
- all accounts involved in transactions concluded by the accountable institution in the course of the business relationship and/or all accounts involved in single transactions;
- the name of the person who obtained the above information the accountable institution’s behalf; and
- any document or copies obtained by the accountable institution in order to verify a person’s identity in terms of Sections 21(1) or (2) of the FIC Act (s.22(1) FIC Act).

473. There is no specific requirement that the transaction records include the date of the transaction or the address of the customer. Regulation 50 of the Regulations Relating to Banks requires that a "bank shall implement and maintain policies and procedures to guard against the bank being used for purposes of market abuse and financial fraud, including insider trading, market manipulation and money laundering. As a minimum, the policies and procedures implemented by the bank shall be adequate…to provide an audit trail." This should adequately cover the reconstruction of individual transactions. However, outside of the banking sector, there is no general obligation on accountable institutions to keep transaction records sufficient to permit the reconstruction of account activity.

474. Effective application of the record keeping provisions of Section 22 of the FIC Act are further eroded by Exemptions 4, 6, 7, 8, 9, 14, 15, 16 and 17 which exempt accountable institutions from maintaining records of customer identification and verification. Nevertheless, even in circumstances where these Exemptions apply, the relevant accountable institutions are still required to retain the following transaction records: the amount involved, parties to the transaction and all accounts involved (ss.22(f) and (g) FIC Act). However, in the absence of a requirement to retain underlying CDD records, the reconstruction of transactions conducted under some of the Exemptions may be difficult.

475. Additionally, there is no requirement for accountable institutions to maintain account files or business correspondence as part of the recordkeeping obligation under Section 22, which may be a shortcoming to the extent that such records are needed to reconstruct a transaction. However, this deficiency is mitigated by the additional and specific record keeping requirements that apply in the securities sector. Members of the JSE are required to maintain "proper, accurate and secure records in relation to the services rendered to its clients" (s.8.10.4 JSE Equities Rules, s. 16.10.5 Derivatives rules and s.10.220.5 Yield-X rules). They are also required to have procedures and systems in place to store and retrieve, "in a manner safe from destruction", a record of all communications given to a client, including: instructions given by the client to the member; transaction documents; and contractual arrangements between the member and its clients, including mandates prescribed by the rules and client particulars required to be provided in terms of the rules or which are necessary for the effective operation of client accounts. The accountable institutions to which the JSE Rules apply would thus seem to required to maintain business correspondence as part of their record keeping obligations. Records may be kept in electronic, printed or voice-recorded format. JSE members are not required to maintain the records themselves, but are required to make them available for inspection within seven days. JSE members are also required to maintain client instructions for executing transactions for six months and other records for at least five years.

Access to information

476. Representatives of the Centre are authorised to examine, make extracts from or copies of any records kept by or on behalf of an accountable institution pursuant to the record keeping obligations under Sections 22 and 24 (s.26 FIC Act). Except in the case of records which the public is entitled to have access to, authorised representative of the Centre exercise their authority to review records by virtue of a warrant issued in chambers by a magistrate, regional magistrate or judge of an area of jurisdiction within which the records (or any of them) are kept or within which the accountable institution conducts business. Such a warrant can only be issued on the basis of information provided on oath or affirmation that establishes reasonable grounds to believe that the records referred to may assist the Centre to identify the proceeds of unlawful activities or to combat ML. Such a warrant may contain whatever conditions regarding access to the records as the issuing official may deem appropriate to include. An accountable institution must without delay give an authorised representative of the Centre all the assistance necessary to enable that representative to exercise the authority granted under the Act to access records.

477. Accountable institutions are permitted to outsource the maintenance of records to third parties on their behalf as long the accountable institution has free and easy access to the records, and provides the Centre with that third party's particulars (s.24 FIC Act). In particular, the accountable institution must provide the Centre with: the third party's full name (for a natural person), or registered name and name under which it conducts business (for a legal person); the full name and contact particulars of the individual who exercises control over access to those records; the address where the records are kept; the address from where the third party exercises control over the records; and the full name and contact particulars of the individual who liaises with the third party on behalf of the accountable institution regarding the retention of the records (MLTFC Regulation 20). Ultimate responsibility for compliance with the record keeping provisions of Section 22 remains with the accountable institution which will be liable for any breach of the requirements.

478. The results of the inspection process show a good level of compliance with record keeping obligations in the banking sector and among authorised dealers who provide foreign exchange and international remittance services. Likewise, no noteworthy problems were identified in the securities, FSP or insurance sectors in relation to compliance with the record keeping obligations. The results of the inspection process are further elaborated in Section 3.10 of this report.

Special Recommendation VII

Overview

479. South Africa implements components of SR VII through requirements in its National Payment System (NPS). Following the last FATF mutual evaluation of South Africa (2003), a project team was established, under the auspices of the SARB and comprised of representatives from the payments industry, to implement changes to South Africa's NPS to enable full originator information to accompany wire transfers (domestic and cross-border) being transmitted using the SWIFT messaging formats.

480. Only banks that are subject to the FIC Act are currently allowed to participate in the NPS. The NPS was established under the National Payment System Act (the NPS Act), which provides for the management, administration, operation, regulation and supervision of payment, clearing and settlement systems in South Africa. Section 3 of the Act authorises the SARB to recognise a payment system management body to manage, organise and regulate the payment system. The management body recognised by the SARB is the Payment Association of South Africa (PASA).

481. The National Payment System is comprised of some 14 different payment streams which are supervised by Payment Clearing Houses (PCHs). The PCHs specifically applicable to wire transfers include:

- the Electronic Funds Transfer (EFT) Debit PCH;
- the EFT Credit PCH;
- the Immediate Settlement (IMMS) PCH (being the RTGS environment);
- the Real Time Credit (RTC) PCH; and
- the old South African Payment System (ZAPS) PCH.

482. PASA requires that each member (participant bank) sign a bilateral, binding agreement with the other participants in its payment stream. These agreements, known as PCH Agreements, require adherence with the rules and standards governing the compilation and processing of payment instructions in the respective payment streams.

483. Each one of these PCH Agreements contains a Section 5 (concerning compliance and responsibilities) which contractually obliges the participant banks to abide by the respective PCH and Straight Through Processing (STP) Rules as set out in the NPS Straight Through Processing Automation Guide. By entering into PCH Agreements, PASA members agree to abide by the relevant PCH rules when processing wire transfers including adherence to prescribed standards in the clearing rules that ensure the accuracy, legality and integrity of payment instructions. Failure to comply with these obligations could result in action being taken by PASA if it considers that the particular member's actions constitute an unacceptable level of risk to the system and/or other PCH participants.

484. Wires are also executed for non-members such as Postbank member banks, and two PASA member banks serve as agents for MoneyGram in South Africa where the value transfer service product offered by MoneyGram is licensed by ExCon. MoneyGram agent banks collect and verify customer information as required under the FIC Act. Some of this information along with related payment instructions is then transferred by MoneyGram's office in South Africa to a central database using MoneyGram's proprietary messaging system. Payment instructions transferred using MoneyGram are not processed through the NPS and therefore are not subject to the PASA contractual obligations described in the paragraph above. Since cross-border remittance services can be legally provided only by Authorised Dealers, pursuant to Regulation 2 of the Exchange Control Regulations 1961, cross-border MoneyGram payments instructions accepted by its agent banks are subject to these Regulations.

485. Uncovered Financial Institutions are not authorised to conduct wire transfers, so the scope issue identified above (see Section 3.1) does not affect the Special Recommendation VII.

Obligations on ordering financial institutions to collect and maintain information

486. Accountable institutions (including all PASA members, Authorized Dealers and Postbank) are required to obtain, verify and maintain full originator information (name, address and account number) for all domestic and cross-border transactions, regardless of the amount of the transaction (s.21 and 22 FIC Act). Since transactions using the MoneyGram are also conducted through its agents which are accountable institutions, complete originator information for those transactions is also collected for each of these transactions. Under Exchange Control regulations, this information is also sent to and maintained by ExCon.

Information that must accompany the wire transfer

487. The contractual obligation to include originator information in wire transfers is limited only to wire transfers processed through the NPS. Even though there is a legal requirement for accountable institutions to collect and verify originator information, there is no generalised legal requirement that all wire transfers/payment instructions be accompanied by full originator information. Consequently, in practice, the amount of information that accompanies a wire transfer depends on whether the transfer is being sent by a PASA member through the NPS or by a MoneyGram agent through MoneyGram's own proprietary messaging system.

Transfers through the NPS

488. Wire transfers through banks may only be executed in South Africa by any one of the 21 banks that are members of the NPS using SWIFT messaging standards.[15] The Electronic Funds Transfer (EFT) systems are primarily used to process low value wire transfers (*i.e.* credit payment transfers of up to ZAR 5 million and debit payment transfers of up to ZAR 500 000). Payments processed through the EFT for domestic purposes are batched. The batches contain "trace numbers" which can be traced back to originators. The SWIFT system is primarily used to process high value transactions (meaning any payments in excess of these thresholds) which most likely include cross-border transfers originating or terminating in jurisdictions outside South Africa.

489. Cross-border payment instructions in cases where either the beneficiary or, the sender or both are non-financial institutions are processed singly using the SWIFT Message Type (MT) 103 formats.

490. PASA's PCH Clearing Rules for IMMS and ZAPS (Section 2.16) – which banks have contractually agreed with each other to adhere to--indicates that "all domestic transfers will be populated by the ordering bank with a unique reference number (see FATF Interpretative Note to Special Recommendation VII: Wire Transfers paragraph 8 and 9), which will allow the ordering bank to trace and identify the originating customer. The ordering bank must be able to make this information available within three business days of a request to do so from the authorities" (Section 2.16.1). While South African authorities explained that "domestic transfers" applies to all transfers originating in South Africa, including those that will be sent cross-border, the reference to the Interpretative Note to Special Recommendation VII creates possible confusion by referring to those paragraphs in the interpretative note that apply only to domestic transfers and not to the paragraphs relating to cross-border transfers.

491. Section 2.16.2 indicates that beneficiary institutions must take reasonable care as part of its risk management processes, to determine that the transfer instruction has been populated with originator information. Transfers should not be returned on the basis that the originator information is missing, but the lack of such information must be considered in assessing whether the transfer is suspicious and should be reported.

492. In order to implement this contractual obligation on a technical level, changes were made to the STP Rules to make mandatory the use of Tag (Field) 20 (*i.e.* to include a *unique reference number*) in the SWIFT message type (MT) 103 (the single customer credit transfer) and MT 205 (the financial institution transfer execution). SWIFT message formats are used by PASA participants to clear and settle payments through the NPS.

493. Under contractual obligations to comply with the PCH Clearing Rules for IMMS and ZAPS, banks are required to complete certain message fields ("Tags") in the SWIFT message when processing payment instructions. Banks sending or receiving MT 103s are required to ensure that the mandatory fields in these message types meet the standards set by PASA and validate the mandatory fields in the two message types including the MT 103s which are used for single customer transfers (s.3.1). In this case where the originator or beneficiary (or both) are not financial institutions, the ordering financial institution (Ordering FI) can send a SWIFT MT 103 message type on behalf of the originator, either directly or indirectly through a correspondent(s). In such cases, it is mandatory to complete Field 50a (Ordering Customer) and Field 20, requiring a *unique reference number* to allow the sender to unambiguously identify the message. For a normal customer-to-customer transactions, the originator's *account number* should be entered into the first line of Field 50a, where applicable, and the originator's *name and address* in the following lines or the Business Entity Identifier (BEI) in the second line (s.3.4(3)(a) and (b)). Where

[15] The SARB is a member of the NPS as a user.

the payment instruction originates from the Ordering FI's EFT system, both the account number, and name and address or BEI are mandatory.

494. The complete omission of characters in fields that are mandatory for MT 103 and 205 messages is automatically detected by the system and results in the rejection of the wire transfer. However, the wire transfer will not be rejected as long as there are some characters in the mandatory fields – regardless of whether those characters constitute full, accurate and meaningful originator information.

Transfers through MoneyGram

495. In addition to funds transfers by banks using the SWIFT messaging through the NPS, a large percentage of money/value transfers are effected using MoneyGram services through two South African banks serving as MoneyGram agents. These payment instructions are not transmitted via the NPS and therefore do not utilise SWIFT message formats nor are subject to PASA rules and contractual obligations. Furthermore, in the absence of a general legal requirement, there is no enforceable obligation for MoneyGram to transmit full originator information with its payment instructions. In the event that payment settlement services are required by MoneyGram, wire transfers are sent by the PASA member banks where MoneyGram is the originator and the beneficiary is another MoneyGram agent/office. In these cases, full originator information would be required in order for the member bank to utilise the NPS. However, the information would relate to MoneyGram and would not permit the identification of the underlying MoneyGram customers unless the unique reference in the MT 103 (Tag 20) message format allowed the originator bank to make such identification.

496. Although MoneyGram's agent banks collect full originator information in accordance with the FIC Act requirements with respect to both existing and occasional customers who wish to transfer funds overseas, in practice, not all the information that is collected is transferred to the receiving MoneyGram agent or office outside of South Africa. It is, however, transferred by MoneyGram's agents to the MoneyGram Office in South Africa and entered into the central MoneyGram database located in the United States for further processing and settlement. The assessment team was informed that, for privacy reasons, addresses are not sent with payment instructions from South Africa and recipient agents/offices are provided only with the first and last names of the customer, the country of origin and a transaction identifier. However, MoneyGram is subject to South Africa's exchange control regulations which require its agent banks to report outgoing transfers to ExCon. ExCon requires, as mandatory fields, for reporting purposes, the name of the ordering customer as well as his/her address. The bank's system processing the transaction automatically generates a transaction reference number (TRN) which is linked directly to the customer's profile which includes account numbers.

Transfers through Postbank

497. In addition to the transfer services offered by the banks and MoneyGram, South African citizens also have access to money/postal orders provided by SAPO through its Postbank. Postbank sells both domestic and international money transfer services (Money/Postal Orders), and provides both services to its account holders and interested customers. There is a limit on each domestic and outbound money transfers/postal order of ZAR 2 000 and a ZAR 5 000 limit on Mzansi Money Transfers. While there is no limit to the numbers of money/postal orders that can be sent to countries in the Rand common monetary area (CMA), there is a ceiling on the amount that can be sent by money order to countries outside of the Rand CMA, which is ZAR 2 000 per month per person up to an annual limit of ZAR 24 000. Both the postal orders and Mzansi transfers fall below the threshold of EUR/USD 1 000 for the collection and verification of originator information and SR VII requirements. However, originator information is captured and is available to South African law enforcement authorities. It can also be made available to any foreign post office upon request. Postbank is also subject to exchange control laws that have

mandatory requirements with respect to name and address and this information is also available upon request from ExCon.

498. As an accountable institution, Postbank is subject to the FIC Act requirements, and the information collected from customers is entered into a database. For domestic and international money transfer services (Money/Postal Orders), ordering customers are provided with a reference and/or pin number which is used by beneficiaries to retrieve the funds at the Post Office or Retail Postal Agencies. These numbers can also be used by law enforcement authorities to identify originating customers. Less frequently used are Mzansi transfer services which are processed through the NPS where there is an established Mzansi PCH. Since Postbank is not a member of the NPS, wire transfers sent on behalf of its customers are executed by a "sponsoring" bank that is a PASA member. As is the case with other transfers, originator information related to Mzansi transfers is also organized in a database which is accessible by the NPS system operator.

Ability of the competent authorities to access full originator information

499. For "domestic transfers" (which South African authorities define as being all transfers originating in South Africa) being processed through the NPS, the PASA Payment Clearing Rules for Immediate Settlement (IMMS) and ZAPS contractually oblige an Ordering FI to enter a unique reference number which will permit it to trace and identify the originating customer. The Ordering FI must be able to make this information available within three business days of a request to do so from the authorities (s.2.16.1). The PCH Agreements also contractually obligate members to adhere to the STP standards which require them to enter the name and address of the ordering customer in Field 50a (s 3.4.3). These requirements do not apply to MoneyGram transfers although, in practice, MoneyGram reports that it is able to make full originator information available to the authorities within a few days.

500. Making originator information readily available to the authorities is also facilitated by the Cross-Border Foreign Exchange Transaction Reporting System of the ExCon which requires comprehensive information on all cross-border foreign exchange and foreign remittance transactions (except inter-bank transactions) to be reported. This reporting system captures the name and address (but not the account number) of any South African resident who is the originator or beneficiary of such a transaction, irrespective of the amount involved. Law enforcement authorities would also have access to the Postbank databases which contain originator information relative to customers who have purchased cross-border money/postal orders or conducted transfers from their Mzansi accounts.

501. Although the information captured by these systems can be easily retrieved upon proper authority and provided to foreign authorities upon appropriate mutual legal assistance requests, they are not substitutes for requiring full originator information to be transmitted in the message or payment form accompanying the cross-border wire transfer, as is required by SR VII. One of the main objectives of SR VII is to ensure that full originator information is immediately available in the jurisdiction of the beneficiary financial institution, without having to undertake (often lengthy) mutual legal assistance processes.

502. In the case of domestic transfers through Mzansi accounts, verification of the address is not required pursuant to Exemption 17 (see Section 3.2 of this report for more details). However, the limits on single transfers through Mzansi accounts is ZAR 5 000 (EUR 423) which is well below the EUR 1 000 threshold for the collection and verification of originator information, and in line with the requirements of Special Recommendation VII.

Obligations on intermediary financial institutions

503. Intermediary institutions are contractually obliged to ensure that they pass originator information received from the ordering financial institution to the beneficiary financial institution (s.2.16.3 of the PCH Rules for Immediate Settlement and ZAPS). If there is a technical reason for why they are unable to do so, the intermediary financial institution must store the originator information received for a period of not less than five years and must make that information available within three business days of a request from authorities to do so. There are no similar requirements or guidelines for MoneyGram transfers not processed through the NPS.

Obligations on beneficiary financial institutions

504. There is no obligation on beneficiary institutions to consider restricting or terminating the business relationship with financial institutions to meet the requirements of SR VII.

505. In relation to wire transfers being processed through the NPS, a beneficiary financial institution is not expected to validate originator information provided by the Ordering FI, but is required to "exercise reasonable care, as part of its risk management processes" to determine whether the transfer instruction contains originator information as required (s.2.16.2 PCH Clearing Rules for Immediate Settlement and ZAPS). Transfers that do not contain full originator information should not be returned on that basis and the beneficiary financial institution should consider the absence of full originator information in determining whether such a transfer is suspicious and where appropriate file a report to the Centre. There are no similar requirements or guidelines for MoneyGram transfers.

506. Additionally, the ExCon Department issued a notice to all Authorised Dealers on 3 April 2003 indicating that, in the event that an incoming international wire transfer does not contain adequate information pertaining to the originator's name, the receiving Authorised Dealer is required to contact the originating correspondent bank and request it to supply the required information. Postbank and MoneyGram's agent banks are required to report any cross-border transactions that involve foreign exchange under the ExCon requirements as is the Postbank.

Monitoring for compliance

507. As the PASA Rules contractually oblige full originator information be included by users of the NPS in SWIFT messages utilised to process cross-border payment instructions, the absence of full originator information would contravene both the PASA rules and signed PCH Agreements.

508. Compliance with the PASA Rules and PCH Agreements is implemented by PASA members/users on a self-regulating basis. The financial institutions that use the NPS are responsible for ensuring its integrity. Failure to comply with the PASA Rules and Standards could be deemed as causing unacceptable harm to the system and to the other participants. In such cases, financial institutions are required to report such compliance failures to the chair of the relevant PCH and are authorised by the PASA STP standards to take actions themselves. Section 2.3.3 of the STP guide permits a PASA member to levy repair charges against another member of ZAR 1 000 per payment where a payment has failed automatic processing in the receiver's system due to incorrect formatting and the receiver is required to manually intervene in order to process the payment. Such interventions could be necessary in cases of missing or incomplete originator information, but would also be necessary in any number of other situations including incorrect formatting, systems failures or other circumstances unrelated to SR VII.

509. PASA's monitoring of compliance with its rules and standards relies on its members (the banks) to report irregularities. There is no indication that PASA specifically checks for compliance with Rule 2.16 to ensure that financial institutions are indeed entering a reference number in Field 20 of their MT 103

messages or account number, name and address in Field 50(a). There is also no indication that compliance with the requirement on beneficiary financial institutions to file an STR in situations where originator information is missing is being tested or that the requirement under Section 5.2.1 of the PCH Agreement for the clearing of EFT Debit Payment Instructions to ensure that the information entered into the fields is accurate and complete. To the extent that the failure by a member to comply with these and other PASA rules results in other members having to make manual interventions, these violations will be addressed by repair charges. South African authorities are aware that PASA members have levied charges against each other and indicate that these have generally been for failure to complete non-mandatory fields and that very rarely, if ever, has there been a need to penalise a bank for incomplete information in the mandatory fields.

510. A failure to comply with PASA rules and standards – included repeated failure on the part of one bank to adequately complete the originator information, could result in a referral by another bank to PASA for investigation. PASA would initially work with the member through its PCH to resolve the problem, or if necessary would issue warning letters. Should the member continue with this practice, PASA can refer the matter to the SARB, who can also take action based on its responsibility to maintain the safety and soundness of the system. The SARB may issue a Directive to a PASA member under Section 12(3) of the NPS Act after consulting with PASA for several reasons including preserving the integrity, effectiveness, efficiency or security of the payment system and ensuring national financial stability. In addition to these specific objectives, Section 12.2(f) also permits the SARB to issue directives for any other matters it considers appropriate, which could include a violation of the PASA requirements to include full originator information in a wire transfer. Any person who fails to comply with a directive is guilty of an offence (s.12(8)). Ultimately, the most severe enforcement actions that the SARB can take against a PASA member are the suspension or termination of access to the system.

511. However, the basis for monitoring and sanctions – the initial reporting by other South African banks – can only be applied to domestic wire transfers. There is no system to monitor, detect, or sanction in cases where complete originator information is not included in cross-border wire transfers, which is a main component of SR.VII.

512. Therefore, for a variety of reasons, the evaluation team could not conclude that the PASA rules and standards developed by South Africa to implement its SR.VII obligations could be considered "other enforceable means", as that term is defined by the FATF. As the payment system management body authorised under the NPS Act with power delegated to it by the SARB, PASA could certainly be considered a competent authority. However, while both the SARB and PASA have some sanctions available to it under the provisions of the NPS Act, and the members themselves can impose fines for violations in the form of repair charges, the links between the requirements under the PASA rules to include sender references and to enter accurate originator information in the MT 103 message fields and these sanctions are not clear. And while these sanctions could be applied for such violations, they are primarily intended to address general concerns such as preserving the integrity, efficiency and effectiveness of the NPS. Finally, the system for sanctions cannot be applied for cross-border wire transfers since in practical terms, a foreign beneficiary may not report a South African sending bank's for a failure to include full originator information nor is it under any obligation to do so not being a party to a PCH Agreement.

513. In the absence of clearer links between the range of available sanctions and the requirements, and a system for applying sanctions to cross-border transfers, it is difficult to determine if these sanctions are effective, proportionate and dissuasive. An argument can be made that repair charges levied by one financial institution against another for manual interventions in the processing of payments could be effective, proportionate and dissuasive for a failure to include complete/accurate information in wire transfer. However, this sanction can only be applied with respect to domestic wire transfers. An argument can also be made that considerations of reputational risk and the threat of removal from the NPS are

dissuasive. However, without that link or examples of enforcement actions, it is difficult to assess proportionality or dissuasiveness.

514. Overall, this means that there is no generalised legal requirement that all wire transfers/payment instructions be accompanied by full originator information. Nevertheless, South Africa's approach appears to be generally effective in practice. The PASA rules constitute relevant "drivers" that have been issued by a competent authority and address the specific issues required under the essential criteria for SR VII. These drivers are understood by the financial sector in South Africa to have directional effect and, at the domestic level, there is some monitoring of compliance by PASA relying on its members to report irregularities. There are also general enforcement powers which may be invoked on the basis of non-compliance and which the authorities indicate have been applied for failure to complete mandatory fields. In these particular circumstances, an upgrade of the rating is justified on the basis of effectiveness.

515. Finally, it should be noted that the obligations and sanctions described do not apply to MoneyGram. However, this gap is mitigated because the total value of MoneyGram transfers represents a very small percentage of the total value of wire transfers being sent in South Africa, and the value of the average MoneyGram transaction is less than EUR 350 which falls well below the EUR 1 000 *de minimus* threshold applicable to SR VII.

3.5.2 Recommendations and Comments

516. For financial institutions outside the banking sector, there should be a specific obligation to collect sufficient information to reconstruct financial transactions; there should also be a general obligation to keep account files and business correspondence.

517. The record keeping obligations should be extended to Uncovered Financial Institutions.

518. South African authorities should establish a general, enforceable obligation (in law, regulation or other enforceable means) to require: all wire transfers to be accompanied by full originator information (or, in the case of domestic transfers, full originator information to be made available to the authorities within three business days of receiving the request), for the intermediary financial institutions to ensure that all originator information that accompanies a wire transfer is transmitted with the transfer, and for beneficiary financial institutions to consider restricting or terminating business relationships with financial institutions that fail to meet the requirements of Special Recommendation VII and/or consider filing an STR. Effective systems for monitoring compliance with these obligations should be implemented, including the possibility of imposing more effective, proportionate, and dissuasive sanctions where appropriate.

3.5.3 Compliance with Recommendation 10 and Special Recommendation VII

	Rating	Summary of factors underlying rating
R.10	PC	• There is not a specific requirement that the transaction records include the date of the transaction or the address of the customer. • Outside of the banking sector, there is no general obligation to keep transaction records sufficient to permit the reconstruction of account activity. • No requirement to maintain account files or business correspondence as part of the record-keeping obligation. • Effective application of the record keeping obligations is eroded by Exemptions 4, 6, 14, 16 and 17 which exempt accountable institutions from maintaining records of customer identification and verification. • Uncovered Financial Institutions are not subject to the record keeping obligations of the FIC Act. This affects the ratings for Recommendation 10.

	Rating	Summary of factors underlying rating
SR.VII	PC	• There is no general legal requirement for all wire transfers to be accompanied by full originator information. • For domestic transfers, there is no general requirement that, where full originator information does not accompany the wire transfer, such information can be made available to the appropriate authorities within three business days of receiving the request. • No general requirement on intermediary financial institutions to ensure that all originator information that accompanies a wire transfer is transmitted with the transfer. • No obligation on beneficiary financial institutions to consider restricting or terminating the business relationship with financial institutions that fail to meet the requirements of Special Recommendation VII. • No indication that PASA specifically checks for compliance with Rule 2.16 to ensure that financial institutions are indeed entering the originator's name and address (in Field 50a), and account number (in Field 57a in the case of debit transfers) or a reference number (in Field 20) as required. • No indication that compliance with the requirement on beneficiary financial institutions to file an STR in situations where originator information is missing is tested or that any tests are conducted to ensure that the information entered into the fields is accurate and complete. • No specific sanctions associated with failing to include full, accurate and meaningful originator information in a message conveying payment instructions across borders. • Although MoneyGram's agent banks collect full originator information, in practice, not all the information that is collected is transferred to the receiving MoneyGram agent or office outside of South Africa.

Unusual and Suspicious Transactions

3.6 Monitoring of transactions and relationships (R.11 & 21)

3.6.1 Description and Analysis

519. Uncovered Financial Institutions are not subject to the transaction monitoring requirements of the FIC Act, so the scope issue identified above (see Section 3.1) does affect the ratings for Recommendations 11 and 21.

Recommendation 11

520. The FIC Act does not contain a provision which expressly requires institutions to pay special attention to transactions based on complexity, size or unusual patterns. However, Section 29(1) (which also establishes the obligation to report suspicious transactions) requires transactions with no apparent business or lawful purpose to be reported to the Centre.

521. The information that must be included in such a report to the Centre includes information identifying the property, accounts and parties involved (see Section 3.7 of this report for more details). Providing this level of detail detailed must require significant examination of transactions and collected information; however, these requirements, are only applicable if a person or institution is considering filing an STR and is required to obtain this information for purposes of preparing a report in accordance with MLTFC Regulation 23. There is no general requirement to undertake these activities for complex and unusually large transactions or unusual patterns of transactions, or to prepare written findings and to maintain them.

522. Although accountable institutions are required to keep records for at least five years (s.22 FIC Act), since there is no requirement to prepare any written findings concerning the background and purpose of transactions with no apparent business of lawful purpose, there can be no requirement to keep them available for competent authorities and auditors for at least five years.

Recommendation 21

523. There is no specific requirement for financial institutions to give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations. Although Guidance Note 3 recommends that accountable institutions apply more careful scrutiny to AML/CFT systems in non-FATF countries to determine if they are equivalent to South Africa's, this guidance is not enforceable and is applicable only to banks.

524. There are some mechanisms in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries. For instance, supervisory bodies and the Centre can communicate such during compliance reviews, or by issuing letters, guidance or circulars to the industry. For instance, in June 2008, the Registrar of Banks issued a letter from the Centre as Guidance Note 8/2008 under Section 6(5) of the Banks Act alerting banks and controlling companies to the FATF call for enhanced scrutiny of transactions with certain jurisdictions that the FATF had identified as posing a risk due to their lack of AML/CFT regimes and the United Nations sanctions in relation to weapons of mass destruction. The letter noted the FATF call on its members to implement enhanced due diligence with respect to the Northern part of Cyprus, the Republic of Uzbekistan and the Islamic Republic of Iran, and urged South African banks to "take account of the vulnerabilities identified by the FATF and to ensure that the due diligence applied in relation to any transactions that might involve financial institutions identified in the FATF statement." Banks were also urged to ensure that such due diligence is commensurate with the increased risk presented by those deficiencies. Additionally, the SARB requested banks to provide it with information regarding the extent of their exposure with respect to Iran, and details regarding their activities and client relationships. This information was then provided to the Centre. This Circular applied only to banks and controlling companies, and is not enforceable. There is no indication that similar efforts were undertaken to inform the securities firms, insurance firms, non-bank money remitters and foreign exchange dealers.

525. The general requirement to report any transaction or series of transactions that is known or suspected to have no apparent business or lawful purpose would equally apply to transactions involving parties from or in countries which do not or insufficiently apply the FATF Recommendations (s.29(1) FIC Act). This implicitly requires institutions to examine these transactions and prepare reports for submission to the Centre. However, as described above in the discussion of Recommendation 11, there is no explicit requirement for a person to examine such transactions and prepare written findings (other than an STR) that can be made available to competent authorities and auditors.

526. There are no specific provisions in South Africa for financial institutions to apply counter-measures in situations where countries do not sufficiently apply the FATF Recommendations. However, South African banks seeking to acquire banks in other countries, establish branches or increase their shareholding in foreign institutions require approval from the SARB for such activities. The SARB can request information or impose conditions it feels appropriate in order to approve such applications. It can, and has requested South African banks to provide plans for meeting AML/CFT requirements in jurisdictions where AML/CFT systems are weak or non-existent.

3.6.2 Recommendations and Comments

527. South Africa should introduce an explicit requirement that all financial institutions (including Uncovered Financial Institutions) pay special attention to all complex, unusual large transactions or unusual patterns of transactions that have no apparent or visible economic purposes. At the present time, guidance provided under Guidance Note 1 and requirements under the FIC Act and the Regulations imply that accountable institutions should identify and conduct some examination on transactions that are unusual and have no apparent economic purpose. However, these activities are limited only to meeting STR reporting obligations.

528. Authorities should establish requirements to pay special attention to customers and transactions relating to countries that do not, or insufficiently apply, the FATF Recommendations. Authorities should also establish institutionalised mechanisms for routinely advising accountable institutions of concerns about weaknesses in the AML/CFT regimes of other countries. While there are communications of this type with the financial sector by the SARB and the Centre, they are currently conducted on a reactive basis; either through supervisory communications when a specific deficiency is identified or another event occurs such as the submission of an application by an accountable institution to expand its operations overseas. The recent efforts to inform accountable institutions of the actions taken by FATF are a step in the right direction and should be formalised.

529. Authorities should clarify the application of Exemption 5 and Section 29 of Guidance Note 3 with respect to countries with equivalent AML/CFT systems and strengthen the provisions of Section 29 to ensure that accountable institutions are routinely and consistently paying special attention to business relationships and transactions with countries that do not or insufficiently apply the FATF standards.

3.6.3 Compliance with Recommendations 11 & 21

	Rating	Summary of factors underlying rating
R.11	PC	• The FIC Act does not contain a provision which expressly requires financial institutions to pay special attention to transactions based on complexity, size or unusual patterns. • No requirement to make a record that includes customer and transaction information for complex and unusually large transactions or unusual patterns of transactions or to prepare written findings and to maintain them unless it is part of an STR. • Since there is no requirement to prepare any written findings concerning the background and purpose of transactions with no apparent business of lawful purpose, there can be no requirement to keep them available for at least five years. • The obligation to pay attention to transactions with no apparent business or lawful purpose should be extended to Uncovered Financial Institutions.
R.21	NC	• No specific requirement for financial institutions to give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations. • Efforts to inform the financial sector about the risks of certain jurisdictions were directed only to banks. • No explicit requirement for a person to examine such transactions and prepare written findings (other than an STR) that can be made available to competent authorities and auditors. • No requirements to apply counter-measures in situations where countries do not sufficiently apply the FATF Recommendations. • The obligation to pay attention to transactions with no apparent business or lawful purpose should be extended to Uncovered Financial Institutions.

3.7 Suspicious transaction reports and other reporting (R.13-14, 19, 25 & SR.IV)

3.7.1 Description and Analysis

530. The reporting obligations of the FIC Act apply to all businesses (not just accountable institutions). Consequently, the scope issue identified above (see Section 3.1) does not affect the ratings for Recommendations 13, 14, 19, 25 and Special Recommendation IV.

531. The Centre has also issued one guidance note under Section 4(c) of the FIC Act to provide interpretations in relation to certain aspects relating to the reporting obligations. "Guidance Note 4 on Suspicious Activity Transaction Reporting" issued in March 2008 provides guidance to accountable institutions, reporting institutions and any other person on meeting the requirements of Section 29 of the FIC Act which requires them to report suspicious and unusual transactions. As explained above in the preamble to Section 3, this Guidance Note does not constitute "other enforceable means" as defined by the FATF.

Recommendation 13 (Suspicious transaction reporting) and SR.IV

532. South Africa has an STR reporting regime with a broad scope both in terms of reporting entities coverage and the situational bases on which to report. Any person who carries on a business, manages or is employed by such business is required to report to the Centre if he/she knows or ought reasonably to have known or suspected that:

- the business has received (or is about to receive) the proceeds of unlawful activities, or property connected to terrorist financing or related activities;

- a transaction to which the business is a party:
  - facilitated (or is likely to facilitate) the transfer of the proceeds of unlawful activities, or property connected to a terrorist financing offence or related activities;
  - has no apparent business or lawful purpose;
  - is conducted for the purpose of avoiding giving rise to a reporting duty under the FIC Act;
  - may be relevant to the investigation of an evasion or attempted evasion of tax; or
  - relates to a terrorist financing offence and related activities, or

- the business has been used (or is about to be used) in any way for ML purposes or to facilitate a terrorist financing offence (s.29(1) FIC Act).

533. The POCDATARA amended Section 29 of the FIC Act 2001 (as indicated above) to extend the STR reporting obligation to property related to terrorist financing offences or transactions that may facilitate terrorist financing offences. Additionally, POCDATARA amended the FIC Act by introducing a new Section 28A, which requires accountable institutions to file Terrorist Property Reports (TPRs) with the Centre if they have knowledge that property in their possession or control is property owned or controlled by or on behalf of, or at the direction of any entity which has committed, or attempted to commit, or facilitated the commission of a specified offence as defined in POCDATARA or is a specific entity identified in a notice issued by the President under Section 25 of POCDATARA.

Attempted transactions and those related to tax matters

534. Section 29 of the FIC Act does not provide for a monetary threshold as a condition to file a suspicious transaction report; therefore a report should be filed irrespective of the amount involved.

535. In relation to attempted transactions, a person who carries on a business and who knows or suspects that a transaction or a series of transactions about which enquiries are made, may, if that transaction or those transactions had been concluded, have caused any of the consequences referred to above, must report that to the Centre (s.29(2) FIC Act).

536. The fact that a transaction is thought to involve tax matters does not exclude the obligation to report suspicious or unusual transactions. On the contrary, Section 29(1) of the FIC Act includes a reference to transactions that may be relevant to duties to pay taxes, duties and levies.

Additional elements

537. Both the reporting obligation in respect of suspicious and unusual transactions under the FIC Act and ML offences under the POCA include references to proceeds of "unlawful activities". "Unlawful activity" has the same definition in both Acts and includes the proceeds from any crime in South African law.

Recommendation 14

538. No action whether criminal or civil may be brought against an accountable or reporting institution, a supervisory body, SARS or any other person who complies in good faith with the reporting obligations under the FIC Act (s.38).

539. Tipping-off is prohibited. A person involved in making a report may not inform anyone, including the customer or any other person associated with a reported transaction, of the contents of a suspicious transaction report or even the fact that such a report has been made (s.29(3) FIC Act). Likewise, any reporter as well as any other person who knows or suspects that a report has been made is prohibited from disclosing any information regarding that report (s.29(4) FIC Act). Such knowledge or suspicion may however be disclosed under the following circumstances: "within the scope of the powers and duties of that person in terms of any legislation; for the purpose of carrying out the provisions of this Act; for the purpose of legal proceedings, including any proceedings before a judge in chambers; or in terms of an order of court."

540. Contravention of these prohibitions constitutes offences in terms of Section 54 of the FIC Act and carries a maximum penalty of imprisonment for up to 15 years or a fine of up to ZAR 10 million.

Additional elements:

541. No evidence concerning the identity of a person who has made or contributed to such a report is admissible as evidence in criminal proceedings unless such a person chooses to voluntarily testify.

Recommendation 25 (only feedback and guidance related to STRs)

542. In March 2008, the Centre issued Guidance Note 4 to assist accountable institutions, reporting institutions and any other person as described in Section 29 of the FIC Act in meeting their reporting obligations under the Act. Guidance Note 4 provides general guidance on the nature of the reporting obligation and explains reporting timelines, how reports have to be sent to the FIC, what information has to be included in these reports, and how to use the electronic reporting mechanism. It also details a number of possible suspicious activity indicators.

543. The Centre conducts feedback sessions with various stakeholders to discuss past activities, challenges and successes, emerging trends and typologies with a view to improving their AML efforts and future cooperation. During these sessions the Centre discusses matters such as trends, based on information

reported by particular institutions. Information emanating from these reviews is shared with other institutions through these sessions.

544. The Centre provides general feedback, acknowledging receipt of all reports and providing the reporter with a unique reference number which will be used in respect of further communication relating to a particular report. As a general rule, the Centre does not provide case-by-case feedback on the outcomes of analysis and referral processes relating to information reported to it, as this may prompt an institution to change its behaviour towards a customer which may, in turn, alert the customer to the fact that a report has been made in respect of a transaction, or may generate unwarranted suspicious and unusual transaction reports. Nevertheless, in specific instances the Centre may engage with a reporting person/entity subsequent to receiving a report, in order to obtain additional information or to ascertain whether a transaction should be stopped by means of the Centre's intervention powers.

Recommendation 19

545. South Africa has considered the feasibility and utility of implementing a system where financial institutions report all transactions in currency. Provision is made under Sections 28 of the FIC Act for the reporting of cash transactions above a prescribed threshold. This provision will come into operation in January 2009, when the Centre's IT capacity to receive and process such transactions has been fully developed.

Statistics and effectiveness

546. During the 2007/08 financial year, the Centre received 24 585 STRs. This denotes a 15% increase in comparison to the previous year. The financial sector submitted 22 415 STRs to the Centre, which comprises 90% of all reports received. However, this included 64% of all total STRs from one bank, and in particular its foreign remittance business. There was some concern that this could be the result of over-reporting. However, neither the financial institution nor the Centre saw this as an impediment, and the Centre in particular indicated that they particularly welcomed the additional reporting from the one institution and the information provided in these reports. Compared year-on-year, the overall reporting trend appears unchanged.

STRs received by the Centre

	Type and number of entity reporting	2005/06	2006/07	2007/08	Total	%
Financial	Banks(30)	3 802	6 080	6 622	16 504	25%
	Money remitter*	14 712	12 300	15 287	42 299	64%
	Foreign Exchange Entities(9)	94	73	89	256	0%
	Brokers & Investment Entities(21)	99	35	110	244	0%
	Insurance Entities(24)	126	334	307	767	1%

547. There were some initial effectiveness concerns surrounding the multiple obligations to report matters relating to terrorist financing – the general STR obligation (s.29), the TPR obligation (s.28A) and the obligation to report matters to the police that might pertain to terrorism pursuant to POCDATARA. However, the Centre indicated that while this does cause some double reporting, the additional information and reports are welcome and are subject to different kinds of analysis. Financial institutions confirmed that initially there had been some confusion, but this has improved since Guidance Note 4 was issued in March

2008. There has been a marked increase in the number of STRs selected for suspected terrorist-related activity, as noted in the chart below.

STRs selected for suspected terrorist related activity

Financial year	Reporter	Total	Accumulated Totals
2005/06	Bank	1	1
2006/07	Private individual or Bank	28	29
2007/08	Private individual or Bank	161	190

TPRs received by the Centre

Financial year	Total	Accumulated Totals
2005/06	44	44
2006/07	47	91
2007/08	5	96

3.7.2 Recommendations and Comments

548. South Africa has a broad reporting regime in which all financial institutions are required to submit STRs, and overall the regime is being implemented effectively; however, some categories of financial institutions (*e.g.* leasing companies and finance companies) have not yet implemented the reporting obligations.

549. The Centre issued guidelines on reporting requirements and reporting forms, however, the guidelines are very general, not sector specific, and the current guidance and reporting forms are mainly focused on the banking institutions. As a result, other financial institutions and DNFBPs have to modify the reporting forms internally to adapt to the general reporting requirements initially designed for banks. The Centre should consider tailoring reporting forms for non-bank financial institutions and DNFBPs.

550. Though the Centre provides case-by-case paper-based feedback to law enforcement agencies and other supervisory bodies, the Centre should provide general feedback with respect to the current techniques, methods and trends of money laundering, and sanitised examples of actual money laundering cases either in its annual reports or separately in its typology reports.

3.7.3 Compliance with Recommendations 13, 14, 19 and 25 (criteria 25.2), and Special Recommendation IV

	Rating	Summary of factors underlying rating
R.13	LC	• Leasing and financing companies have not yet implemented the reporting obligations.
R.14	C	• This Recommendation is fully observed.
R.19	C	• This Recommendation is fully observed.
R.25	PC	• The current STR reporting guidelines are not sector specific, and the reporting requirements and reporting forms are mainly designed for banks. • The Centre has not provided general feedback on the methods and trends of money laundering, or sanitised ML cases.
SR.IV	LC	• Leasing and financing companies have not yet implemented the reporting obligations.

Internal controls and other measures

3.8 Internal controls, compliance, audit and foreign branches (R.15 & 22)

551. Uncovered Financial Institutions are not subject to FIC Act requirements relating to internal controls, and foreign branches and subsidiaries, so the scope issue identified above (see Section 3.1) does affect the ratings for Recommendations 15 and 22.

Recommendation 15

552. Accountable institutions are required to formulate and implement internal rules to foster compliance with the FIC Act and to make these available to each of its employees involved in transactions to which the FIC Act applies (s.42). The internal rules must address CDD (identification and verification), record keeping, reporting obligations and other matters that may be prescribed. These general requirements are further elaborated in the MLTFC Regulations (25 to 27).

Compliance officers and access to records

553. Accountable institutions are required to appoint a compliance officer who is responsible for ensuring compliance by employees with the FIC Act; however, the FIC Act does not require that the compliance officer be at the management level (s.43(b)).

554. This deficiency is not relevant to the banking sector, however, because Banks Act Regulation 49(4)(a) specifies that, at a minimum, the compliance officer of a bank shall have senior executive status in the bank. Banks Act Regulation 49 also requires that the compliance function for banks must ensure that they continuously manage their regulatory and supervisory risks (*i.e.* the risk that the bank does not comply with applicable laws and regulations or supervisory requirements). This would include the risk of not complying with AML/CFT requirements.

555. Accountable institutions must ensure that their internal rules on record keeping provide for the necessary processes and working methods to ensure that relevant staff members (which would include the compliance officer) have access to those records, as may be required or authorised under the FIC Act (MLTFC Regulation 26(f)).

Independent audit

556. The FIC Act does not specifically address the issue of an independent, internal audit function. However there are requirements for internal audit in some of the separate financial institutions' legislation. For example, banking institutions are subject to a general requirement to maintain an audit function (s.11 SARB Act). In addition, according to Regulation 48 of the Regulations Relating to Banks, banks "shall establish an independent and objective internal audit function that, which internal audit function: … establishes and maintains… appropriate methods in order to monitor the bank's compliance with laws, regulations, and supervisory and internal policies." This would include the AML/CFT rules required under section 42 of the FIC Act and the related MLTFC Regulations. The audit function must be functionally independent, objective and sufficiently resourced (including with appropriately trained staff) so as to be able to provide an independent assessment of the adequacy of and compliance with the bank's established policies, processes and procedures.

557. Long-term life insurers are required to appoint auditors who submit an annual audit report to the FSB (s.19, Long/term Insurance Act (LTI Act)). As part of this return, the auditors report on ALM/CFT compliance. However, this requirement does not address sample testing. An audit committee must also be established (s.23 LTI Act); however, that committee's work is focused mainly on accounting practices,

information systems and auditing and actuarial valuation processes. There are no broad references to ensuring that the institution complies with all applicable laws and regulations.

558. Similar general requirements to establish an audit function apply to FSPs (asset managers, linked investment service providers and financial services providers who collect premiums or receive/hold customers' funds) (s.19 FAIS Act). However, the audit is focused on ensuring that the financial records of the institution are being properly maintained, not ensuring compliance with internal control rules.

559. For collective investment schemes, the Registrar is empowered to direct a manager to have all books of account and financial statements audited, and to submit the results of such an audit to the Registrar (ss.19, 73 and 74 Collective Investment Schemes Act (CISC Act)). However, this is a general obligation that focused on accounting practices, not compliance with relevant laws such as the FIC Act.

Employee screening and training

560. There is no general requirement for financial institutions to put in place screening procedures to ensure high standards when hiring all employees. There are provisions in the various financial sector's legislation for fit and proper tests, although they apply only to executives and senior managers, and compliance staff (see Section 3.10 of this report for more details). However, banks do share an internal database that lists persons who were dismissed on the grounds of dishonesty.

561. Accountable institutions are required to train their employees to enable them to comply with the internal rules and the FIC Act (s.43(a)). However, there is no requirement that such training be conducted on an ongoing basis and in practice some financial institutions only provide such training upon hiring.

Additional elements

562. For banking institutions, the compliance function must be independent. At a minimum, the compliance officer shall function independently from functions such as internal audit and shall be demonstrably independent (Banks Act Regulation 49). The compliance officer shall also have direct access to and demonstrable support from the chief executive officer (CEO) of the bank, and shall in a timely manner report non-compliance with laws and regulations or supervisory requirements to the bank's CEO, board of directors and audit committee (Banks Act Regulation 49(4)(b) and (d)).

Recommendation 22

563. There is no direct requirement for South African financial institutions to ensure that their 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 is there a requirement to apply the higher of the requirements if South African and host country requirements differ. As described below, there are some relevant measures that are specific to the banking sector. However, it should be noted that these only partially meet the requirements of Recommendation 22 and there are no similar measures in any of the other financial sectors (*e.g.* insurance, securities, etc.).

Relevant measures in the banking sector

564. Section 52 of the Banks Act allows the Registrar to impose conditions on those applying for bank licenses. In practice, a normal condition of a banking licence is that a foreign branch or subsidiary adhere to the higher of the AML/CFT standards – those of the host country or those of South Africa. Anyone who contravenes Section 52 (1) or (4) of the banking act shall be guilty of an offence and liable to a fine or to imprisonment for a period not exceeding five years or to both a fine and such imprisonment (s.91, Banks Act). However, there is nothing in the law or regulations that require the Registrar to make this element of

Recommendation 22 a condition of a banking licence and, in fact, it is not clear that all banking licences contain this condition.

565. In practice, when foreign subsidiaries or branches of South African banks are established, in terms of consolidated supervision, the BSD may assess the status of the standards applied in the foreign subsidiaries or branches and may contact the regulator abroad for information to be able to properly assess the situation.

566. The leading South African banking groups have a significant number of subsidiaries abroad, mainly in Africa (Mozambique, Zimbabwe, Botswana, Namibia, Malawi, Zambia, Uganda, Swaziland, Tanzania, Nigeria, Mauritius); the Channel Islands (Jersey, Guernsey, Isle of Man); the United Kingdom; Hong Kong, China; the United States; and The Bahamas. Some of the AML officers of the major banks indicated that they imposed on their subsidiaries in Africa training requirements for, internal controls and procedures and reporting. All major banks indicated that, although not required by law, their policy was to apply the higher standards of home and host jurisdiction. This situation regarding other types of financial institutions is not clear.

567. In terms of the FAIS Act, only entities that render financial services as defined in the Act and conduct business in South Africa are regulated. This means that foreign branches and subsidiaries do not fall within the ambit of the FAIS Act unless they are representatives of authorised financial services providers and render financial services in the Republic.

568. For the supervision of insurers, the FSB requires that the insurers have AML/CFT policies applicable to the group of companies. These policies must be adopted at Board level.

569. There is no specific requirement to inform the South African authorities if a foreign branch or subsidiary is unable to observe appropriate AML/CFT measures because this is prohibited by host country laws, regulations, or other measures.

570. Banks are required to seek approval from the registrar in order to open or acquire a domestic or foreign branch or subsidiary (s.52(1) Banks Act). The conditions are set out in Regulation 56 of the Banks Act Regulations. In the case of an off-shore branch office or subsidiary, the application shall contain an opinion on the ability of the company to submit the required Banks Act form and the following details about host country: the nature of supervisory functions performed by host country and the evaluation of country risk in respect of the host country (Banks Act Regulation 56(2)(b)(xii) and (xv)). While this might address safety and soundness issues, there are no specific requirements relating to the level of AML/CFT controls applying in the foreign country. In addition, there is no specific provision of an ongoing monitoring of the licensing requirement.

571. Consolidated supervision serves as a complement to solo supervision of a bank. Regulation 36 of the Banks Act Regulations relates to minimum standards for consolidated supervision and is aimed at capturing all material risks to which the banking group may be exposed, including credit risk, market risk and operational risk. Regulation 36(17) regulates matters related to corporate governance, risk management and internal controls. Banks are required to have policies and risk-management procedures that include, *inter alia*, "comprehensive know your customer standards that… prevent the bank or controlling company from being used for any money laundering or other unlawful activity."The procedures shall also be sufficient to ensure that the relevant bank or controlling company, achieves effective risk-management, monitors account activity for potential suspicious transactions, establishes an independent internal audit function and independent compliance function, etc.

572. Regulation 37 which pertains to the consolidated supervision of foreign operations of South African banks, aims to ensure that such foreign operations are prudently managed. Regulation 37(4) provides that all the relevant provisions specified or envisaged in Regulation 36(17) in respect of governance, risk management and internal controls shall *mutatis mutandis* apply to any foreign operation of the relevant bank.

Additional elements

573. There are no requirements for financial institutions to apply consistent CDD measures at the group level, although as noted above, for the banking sector, regulations require that group policies contain comprehensive know your customer standards that prevent the bank or controlling company from being used for any money laundering or other unlawful activity.

3.8.2 Recommendations and Comments

574. The FIC Act should be amended to specify that compliance officers should be at the management level and that employee training be on-going. There should also be more specific requirements for financial institutions to screen all employees and, for non-bank financial institutions, to maintain internal audit procedures to ensure compliance with AML/CFT policies and procedures. The requirement to implement internal controls should extend to Uncovered Financial Institutions.

575. Regulations for consolidated supervision require group policies that address certain AML/CFT issues such as ensuring KYC policies to ensure the institution is not used for money laundering and procedures to adequately monitor for suspicious activity. However, there should be more specific requirements that foreign branches and subsidiaries apply AML/CFT measures consistent with the FATF Recommendations, and apply the higher of either domestic or South African standards, and inform the home supervisor if it is unable to do so. These requirements should also extend to Uncovered Financial Institutions.

3.8.3 Compliance with Recommendations 15 & 22

	Rating	Summary of factors underlying rating
R.15	PC	• For financial institutions other than banks, there is not a requirement that the compliance officer be at the management level. • Other than for banks, there is no requirement for accountable institutions to maintain an adequately resourced and independent audit function to test compliance (including sample testing) with AML/CFT procedures, policies and controls. • There is no general requirement for financial institutions to put in place screening procedures to ensure high standards when hiring all employees. • There is no requirement that training be conducted on an ongoing basis. • Uncovered Financial Institutions are not subject to FIC Act requirements relating to internal controls.
R.22	NC	• There is no direct requirement for South African financial institutions to ensure that their 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 is there a requirement to apply the higher of the requirements if South African and host country requirements differ. • There are serious deficiencies in South Africa's framework for preventative measures for financial institutions, so applying the South Africa standards would not be consistent with the FATF Recommendations. • There is no specific requirement to inform the South African authorities if a foreign branch or subsidiary is unable to observe appropriate AML/CFT measures.

	Rating	Summary of factors underlying rating
		• Uncovered Financial Institutions are not subject to FIC Act requirements relating to foreign branches and subsidiaries.

3.9 Shell banks (R.18)

3.9.1 Description and Analysis

576. South African licensing requirements effectively prevent the establishment of shell banks.

577. An entity wishing to act as a bank or a branch of a foreign bank in South Africa must first be registered as a public company (banks) or an external company (branches), then apply for and receive authorisation from the Registrar of Banks. In assessing such applications the shareholders/parent and the management are evaluated by the Registrar in terms of the Core Principles, including Core Principle 18. The Branch Regulations require that the business operations of a branch of a foreign bank shall at all times be covered and supported by a valid letter of comfort and undertaking from the parent institution confirming, among others, its understanding and acceptance of, and its adherence to, the relevant core principles for effective banking supervision. In addition the Registrar shall be satisfied that, among other things, "the responsible consolidating supervisor of the foreign institution accepts, is committed to and complies with the proposals, guidelines and pronouncements of the Basel Committee on Banking Supervision".

578. Recently, two applications were turned down, one because the Registrar was not satisfied with the origin of the funds to be invested in the capital of the proposed bank and the second because the Registrar was not satisfied with the proposed management profile. Additionally, an institution's registration may be cancelled if it does not carry on satisfactorily the business of a bank (s.25(4)(b)).

579. Although there is no direct prohibition on financial institutions from entering into, or continuing, correspondent banking relationships with shell banks, the Banks Act Regulations require that group polices "shall be sufficiently robust to ensure that the relevant bank or controlling company… does not enter into or continue a correspondent banking relationship with a shell bank located in a foreign jurisdiction" (Regulation 36(17)(c)). However, there is concern that, as this Section pertains only to banking groups, there might be some banks outside of groups where these requirements do not apply.

580. Guidance Note 3 indicates a number of factors which banks should take into account when establishing correspondent banking relationships, including matters such as the correspondent bank's domicile, the location and structure of its ownership and the nature of its business and customer base.

581. There is no requirement that financial institutions satisfy themselves that respondent financial institutions in a foreign country do not permit their accounts to be used by shell banks.

3.9.2 Recommendations and Comments

582. South Africa should create a more direct and specific prohibition on financial institutions entering into or continuing correspondent banking relationships with shell banks and requirements for financial institutions to satisfy themselves that respondent financial institutions in a foreign country do not permit their accounts to be used by shell banks.

3.9.3 Compliance with Recommendation 18

	Rating	Summary of factors underlying rating
R.18	PC	• There is no direct prohibition on financial institutions from entering into, or continuing, correspondent banking relationships with shell banks. • No requirement that financial institutions satisfy themselves that respondent financial institutions in a foreign country do not permit their accounts to be used by shell banks.

Regulation, supervision, guidance, monitoring and sanctions

3.10 The supervisory and oversight system – competent authorities and SROs Role, functions, duties and powers (including sanctions) (R.23, 29, 17 & 25)

3.10.1 Description and Analysis

Authorities/SROs roles, duties, structures and resources R. 23, 30

Financial Intelligence Centre (the Centre)

583. The Centre is responsible for monitoring and giving guidance to accountable institutions, supervisory bodies and other persons regarding the performance by them of the duties and compliance with the provisions of the FIC Act (s.4). It does not, however, have official supervisory functions or powers.

584. The following supervisory bodies are designated as being responsible for supervising financial institutions which are accountable institutions for compliance with the FIC Act:

- the Financial Services Board (FSB);
- the South African Reserve Bank (SARB); and
- the JSE Securities Exchange of South Africa (JSE) (s.45 and Schedule 2 FIC Act) (collectively referred to as Designated Supervisors).[16]

585. There is an over arching scope issue in that financial institutions which are not accountable institutions are not subject to AML/CFT supervision: finance companies; leasing companies; collective investment scheme custodians; money lenders other than banks; and securities custodians licensed under the FAIS Act (collectively referred to as Uncovered Financial Institutions) (see Section 3.1 of this report for more details). A further scope issue is that there is no designated supervisory authority for the following accountable institutions: Postbank and members of the Bond Exchange. These gaps in the scope of the supervisory framework affect the ratings relative to Recommendations 17, 23 and 29.

South African Reserve Bank (SARB)

586. The SARB is established pursuant to the South African Reserve Bank Act (SARB Act). In addition to being a designated supervisor pursuant to the FIC Act, SARB is responsible for supervising

[16] Also listed in Schedule 2 of the FIC Act are supervisors for certain DNFBP sectors and companies: the Public Accountants and Auditors Board (PAAB), National Gambling Board (NGB) and Law Society of South Africa (LSSA) which will be discussed in section 4.3 of this report and the Registrar of Companies (CIPRO) which will be discussed in section 5.1 of this report.

banking institutions, and overseeing South Africa's exchange control regime. It exercises these powers through its Banking Supervision Department (BSD) and Exchange Control Department (ExCon), as described below.

587. *Banking Supervision Department (BSD):* Banks are registered and supervised for prudential purposes by the Registrar of Banks who performs this function through the BSD of the SARB, pursuant to the Banks Act and the Mutual Banks Act. In practice, BSD also carries out the responsibility of overseeing compliance of banking institutions with the FIC Act.

588. *Exchange Control (ExCon) Department:* The ExCon department of the SARB administers South Africa's exchange control regime and supervises so called "Authorised Dealers" in foreign exchange (*bureaux de change* and banks which are also authorised to deal in foreign exchange) for compliance with the exchange control requirements pursuant to the Currency and Exchanges Act (CE Act) and Exchange Control Regulations (FX Regulations). In terms of an internal arrangement within the SARB, ExCon is responsible for supervising compliance with the FIC Act by the Authorised Dealers in foreign exchange with limited authority (ADLAs) which may only perform travel-related *bureau de change* functions (*i.e.* convert currencies and redeem travellers' cheques.)

Financial Services Board (FSB)

589. In addition to being a designated supervisor pursuant to the FIC Act, the FSB is an independent regulator that was established in 1990 in terms of the Financial Services Board Act (FSB Act). It is responsible for supervising the following providers of financial services for compliance with FSB legislation: financial advisors and intermediaries including investment managers (collectively referred to as financial services providers (FSP)), the insurance industry, retirement funds, friendly societies, collective investment schemes, exchanges, central securities depositories (CSDs) and clearing houses. It exercises these powers through an Executive Officer (the Registrar)[17] who in turn has four Deputy Executive Officers each immediately responsible for a Division of the FSB, *i.e.* Capital Markets Department, Insurance Department, Pensions Department and the Financial Advisory and Intermediary Services Department (FAIS), as described below.

590. *Registrar of Long-term Insurance:* Long-term insurers are supervised by the Registrar in terms of the Long-term Insurance Act, 1998 (LTI Act).

591. *Registrar of Collective Investment Schemes:* The Registrar supervises the following entities in terms of the Collective Investment Schemes Control Act, 2002 (the CISC Act): collective investment schemes in securities, including fund of fund and feeder fund structures, collective investment schemes in property and in participation bonds and foreign collective schemes approved to market their products in South Africa. Managers of Collective Investment Schemes are registered with the Registrar under the CISC Act.

592. *Financial Advisory and Intermediary Services Department (FAIS):* The FAIS is responsible for supervising Financial Services Providers (FSPs) (investment advisers) in terms of the Financial Advisory and Intermediary Services Act, 2002FAIS Act. An FSP is any person who as a regular feature of their business furnishes advice and/or renders an intermediary service. There are currently 14 568 FSPs licensed in terms of the FAIS Act.

---

[17] The Executive Office of the FSB carries the following titles: *Registrar of Long-term Insurance, Registrar of Collective Investment Schemes, Registrar of Securities Services, Registrar of Financial Services Providers and Registrar of Pension Funds*.

593. *Registrar of Pension Funds:* Pension funds are supervised by the Registrar in terms of the Pension Funds Act, 1956 (PF Act).

594. *Registrar of Securities Services*: The Registrar of Securities Services supervises Exchanges, CSD and Clearing Houses in terms of the Securities Services Act, 2004.

JSE

595. In addition to being a designated supervisor pursuant to the FIC Act, the JSE is a licensed exchange which operates four markets: the Equities Market (EM), Equity Derivatives Market (EDM), Agricultural Products Market (APM) and Yield-X. The JSE is responsible for supervising authorised users of the exchange for compliance with the Securities Service Act, 2004, (SS Act) and the JSE rules. The JSE Rules are exchange rules that the JSE is required to maintain pursuant to the SS Act (s.18). Section 18(2)(bb) specifically requires the JSE rules to provide for supervision for compliance with the FIC Act. The JSE is licensed as a self-regulatory organisation (SRO) in terms of the SS Act.

Recommendation 30: Structure, funding, staffing, resources, integrity standards, and training

The Centre

Structure, funding, staffing, and other resources for AML/CFT compliance

596. The Centre's Compliance and Prevention Department has been reaching out and working with the financial sector regulars of the various accountable institutions to help bring institutions into compliance with the FIC Act. Please see Section 2.5 of this report for more details of the structure, function, staffing, and resources of the Centre.

Confidentiality, integrity, skills and training

597. Though it is not mandatory, it is common practice for staff of the Centre to register for the postgraduate diploma in compliance management through the University of Johannesburg (see the above description of this program in relation to the FSB). The Centre also provides funding and encouragement to staff members who further their education by pursuing ongoing skills development courses, or pursue undergraduate and postgraduate degrees. Employees of the Centre are subject to strict standards of confidentiality (see Section 2.5 of this report for further information).

SARB – BSD and ExCon

Structure, funding, staffing, and other resources.

598. The SARB Act provides for a 14-member Board of directors: the Governor; three deputy governors and three other directors appointed by the President of South Africa for five-year and three-year terms respectively; and seven directors elected by shareholders for three-year terms. Since its establishment, the SARB has always been privately owned.

599. Each department of the SARB submits to the Board an annual budget of its staff and resource needs. The structure of the BSD is designed to create the most efficient method to achieve its objectives. The bank through its operations is self financing and the commitment from the budget is generated from these funds and no reliance for financing is placed on any body or person.

600. The BSD has 110 personnel, none of which are dedicated AML/CFT staff. AML/CFT responsibilities are held among various "Teams." The supervisory program and hence most AML work is

run by the Relationship Team (with approximately 60 staff). SARB explained that this approach is useful because the Relationship Team is responsible for managing specific relationships with the banks, and therefore has a better understanding of their structures and risks. Supervisory plans are arranged at the beginning of they year, including which banks should be inspected and whether to include an AML/CFT component. If issues arise, the Relationship Team can bring in the Review Team (which mainly deals with credit risk and has 6 staff) or the Market Risk team (with three staff.) BSD can organise its supervisory program along product lines or profile lines, depending on how the bank is organised. The Review team's complement of 6 staff does not seem adequate given the size of the financial sector.

601. This issue is being addressed, however, in consultation with the management of the SARB. A Deputy Registrar of the Bank Supervision Department (BSD) of the South African Reserve Bank responsible for the unit which performs on-site inspections has submitted a proposal to the BSD executive that this unit should be enlarged with a team which will be dedicated to the supervision of AML/CFT. The team will be staffed with specialists in AML/CFT and will comprise a manager and four senior analysts. The team will receive appropriate training based on the level of skills and to keep it abreast of new developments. The team will be the repository of AML/CFT knowledge within BSD and will receive and analyse AML/CFT returns submitted by the banks and perform on-site inspections of AML/CFT practices and procedures.

602. Seven ExCon staff members are responsible for the execution of the supervisory function. Given the number of entities that the ExCon is responsible for supervising – 130 branches of the seven ADLAs.

Confidentiality, integrity, skills and training

603. Directors, officers and employees of the SARB are subject to strict duties of confidentiality concerning any information acquired in the course of their work (s.33 (SARB Act)) or during the course of an inspection (s.8 Inspection of Financial Institutions Act).

604. The BSD requires its staff to be educated, at a minimum, to the graduate level. BSD has its own code of conduct and applies these standards at all times. ExCon staff responsible for supervising ADLAs are being specially trained and structured to enable effective performance of their duties in accordance with the FIC Act.

605. All new employees must undergo a comprehensive training programme which includes an AML component and the requisite legislation. The SARB College offers an in-depth one day course on AML measures. As part of their performance appraisal, all staff members must complete the e-learning course of the Financial Stability Institute (FSI connect) which has very specific AML modules. The Banking Sector Education and Training Authority, which was established to assist in the training of people working in the banking environment, also has specific AML training modules.

FSB

Structure, funding, staffing, and other resources

606. Currently, the workload of the Executive Officer (Registrar) is divided between four Deputy Executive Officers, each immediately responsible for one of the following divisions: FAIS, Insurance, Investment Institutions (Capital Markets, Collective Investment Schemes and Directorate of Market Abuse) and Pension Funds (including Friendly Societies).

607. The FAIS Department consists of three units which are resourced in the 2008/09 financial year as follows: Registration (responsible for new licences, changes in licensing condition and related information) has 29 staff; Supervision (responsible for analysing financial statements and compliance reports, and

conducting onsite visits) currently has 55 staff members which is expected increase to 60 in January 2009; Enforcement (responsible for complaints, debarment of representatives, investigations and oversight inspections, and regulatory action) has 18 staff.

608. The Supervision Department is also responsible for supervising compliance with the FIC Act and has adopted a risk-based supervision approach. This framework requires the department to focus more on FSPs that pose more risk to the FSB's objectives. Of the 14 568 FSPs currently licensed under the FAIS Act, approximately 11 000 category I FSPs are considered low impact entities.

- These investment advisors and intermediaries are mostly sole proprietors and small scale entities that operate one-man businesses.

- They all submit annual compliance reports to the FAIS Department and are required confirm in such reports as having internal rules and other AML/CFT policies and procedures in place.

- These low impact FSPs are predominantly represented by external compliance officers who assist them in interpreting and implementing AML/CFT legislation. The compliance officers also monitor the FSPs' compliance with AML/CFT legislation and provide regular reports to management and the annual compliance report to the FSB.

609. They are visited under the risk-based supervision approach but not regularly as with the other FSPs. As these entities are small it is possible during each visit to perform detailed procedures on compliance with AML/CFT legislation. The risk based onsite visits to all entities include a Section on assessing FSP's AML/CFT compliance and scrutinizing samples of clients' records and transactions. This is done for high, medium and low impact FSPs. The risk-based approach enables the Supervision Department to visit high impact FSPs on a one to three year cycle, medium impact FSPs on a three to seven year cycle and at least 500 small FSPs per year. This coupled with reliance on monitoring performed by compliance officers is adequate to ensure close and ongoing monitoring of the business of FSPs. FAIS has enough facilities and resources to carry out its responsibilities.

610. The Insurance Department has a Prudential Section (with 24 staff members), a Registration department (with 11 staff members), and a Compliance department (with 15 staff members).

611. The Collective Investment Schemes Department (CIS Department) has a Supervision unit (one Manager and two analysts), and a Registration department (two Managers, one senior analyst, five analysts and one registration clerk).

612. The Inspectorate department has 17 professional staff members.

613. The FSB is funded entirely from the levies and fees it charges regulated industries.

Indicators	**Performance**					
	Prior years			**Forecast**	**Projected**	
	2004/05	**2005/06**	**2006/07**	**2007/08**	**2008/09**	**2009/10**
Revenue (R'000)	139 670	210 731	245 087	285 000	287 000	310 000
Revenue increase year on year (%)	33%	51%	16%	16%	0.7%	8%
Accumulated funds & reserves	147 044	217 250	252 074	250 000	306 000	330 000
Operational expenditure (R'000)	30%	48%	16%	(0.8%)	22%	8%

Indicators	Performance					
	Prior years			Forecast	Projected	
	2004/05	2005/06	2006/07	2007/08	2008/09	2009/10
Operational increase year on year (%)	46 754	86 697	151 948	185 000	160 000	165 000
Number of employees	251	309	322	380	441	450

614. The increase in revenue of 33% for the 2004/05 year, 51% for the 2005/06 year and 16% for the 2006/07 year is mainly due to the expansion of the mandate of the FSB necessitated by the implementation of the FAIS Act, which saw about 14 000 entities being incorporated into the FSB's regulatory net. In 2007/08, the expected increase in revenue is about 16% due to the significant growth in the levy base of various industries. Operational expenditure has mirrored revenue growth over the past three years in that it grew by 30% in 2004/05, 48% in 2005/06 and 16% in 2006/07. During these years the FSB had to increase its capacity particularly in the FAIS department as the department was now migrating from the registration phase of FSPs to the next phase of supervising these entities.

Confidentiality, integrity, skills and training

615. The FSB employs staff with relevant legal, commercial and actuarial qualifications. All staff must undergo a fit & proper test, including security clearances and credential vetting. FSB staff members are subject to strict duties of confidentiality (s.22 FSB Act). Failure to do so constitutes an offence.

616. A Post Graduate Diploma by University of Johannesburg was made compulsory for all FAIS staff members. It includes modules on Compliance Certificate in Money Laundering, Compliance Management, Corporate Governance as well as Ethics and Interpretation of statues. Twenty-three staff have completed the training and fourteen more are still in training. Staff also receive internal training.

JSE

Structure, funding, staffing, and other resources

617. The JSE Board of Directors has delegated the responsibility for the supervision of JSE members' compliance with the SS Act, the JSE Rules and the FIC Act to the Director: Surveillance. The Surveillance division has a current staff compliment of 24 who are organised into five teams with each team being responsible for the supervision of compliance in respect of members' regulated activities either within a particular market or across markets. The Trading, Market Conduct & Conduct of Business Team has five staff covering the EDM, APM and Yield-X markets. The Trading & Markets Conduct Team has three staff covering the EM market. The Capital Adequacy Team has five staff covering the EM EDM, APM and Yield-X markets. The Client Asset Protection team has five staff covering the EM market. The Conduct of Business and FIC Act Team covers all four markets of the JSE (EM, EDM, APM and Yield-X) in respect of FIC Act compliance and the EM in respect of business conduct.

Confidentiality, integrity, skills and training

618. The staff members of the JSE are required to maintain high professional standards, including standards concerning confidentiality. These requirements are incorporated into the JSE's policies and procedures and in its employment practices. The JSE also performs criminal record and credit checks on all prospective employees. All employees are required to sign a contract of employment, which includes a confidentiality clause and binds the employees to the JSE's code of conduct.

619. Staff of the JSE responsible for the supervision of members' compliance with the FIC Act and the Regulations are provided relevant in-house training and attend various AML/CFT conferences.

Authorities Powers and Sanctions – R.29 & 17

620. The FIC Act does not provide any of the supervisory authorities designated pursuant to Schedule 2 of the Act with specific powers of supervision or enforcement to be exercised in this regard. Consequently, supervisors must rely on their general statutory powers of supervision, as defined by their constituting or other legislation, when supervising for compliance with AML/CFT requirements. This raises a concern since, in many cases as described below, the supervisory authority has limited legal basis to inspect and/or enforce compliance with the FIC Act.

The Centre

621. The FIC Act does not provide the Centre with any official powers of supervision or enforcement. The Centre has, however, been able to participate jointly with other supervisory authorities in AML/CFT inspections. In such cases, the supervisor uses its general power to inspectors for the purpose of appointing employees of the Centre to the inspection team (for example, see ss.11 and 12 of the SARB Act for the general authority of SARB to appoint inspectors). This provides a legal basis for the employees of the Centre as individuals (not the Centre as a body) to participate in inspections.

SARB – BSD and ExCon

Powers to monitor, including conducting on-site inspections and compelling production of information

622. The supervisory powers of the SARB are derived from Section 11 of the SARB Act which provides that inspections by the SARB shall be conducted in terms of the Inspection of Financial Institutions Act (IFI Act). The inspection powers under the IFI Act are extremely broad, and allow the SARB to inspect any part of the "affairs" of a banking institution or associated institution (s.3 IFI Act). The inspector may, at any time without prior notice, enter and search any premised occupied by the bank and require the production of any document relating to its affairs (s.4). The Registrar may issue a directive to a bank requiring production of any related information or documents, or the production of an independent auditing report (ss. 6(6)(b)(iii) and 7 Banks Act). It is an offence to give false information to an inspector or, without lawful excuse, refuse to comply with an inspector's request or otherwise hinder the inspection (s.12 IFI Act). Such an offence is punishable by a fine and/or imprisonment for up to two years. Any document which may afford evidence of an offence or irregularity can be seized and retained for as long as it may be required for any criminal or other proceeding. The SARB has no additional inspection powers pursuant to the Banks Act.

623. The definition of financial institution in the IFI Act does not cover ADLAs. Consequently, for ADLAs the ExCon Department must rely on its powers of inspection as contained in the Exchange Control Regulations (s.19). Pursuant to these provisions, ExCon has broad powers to enter any premises (business or residential), inspect books or documents, and obtain statements. These powers are further elaborated in the Exchange Control Rulings which provide that ExCon may, at any time, inspect an ADLA and its books, in a form and manner determined by ExCon, with a view to establishing the ADLA's compliance with any laws which apply to its business, including the FIC Act (Subsection E of Section A.4). Additionally, every director, official or staff member of an ADLA is obligated to produce to the ExCon inspector all books, accounts and other documents in the ADLA's custody and to furnish the inspector with such statements or information relating to the affairs of the ADLA as that inspector may require. Failure to comply with this obligation is an offence punishable by a fine of ZAR 250 000 and/or imprisonment for up

to five years. In case of suspected malpractice or fraud, the inspector has the right of seizure of documents and records.

624. These powers enable the SARB (BSD and ExCon) to access and inspect financial institutions within its jurisdiction for compliance with the FIC Act and to obtain relevant documents and information without a court order.

Powers of enforcement and sanction

625. The SARB has no specific authority to sanction the financial institutions within its jurisdiction for failing to comply with the FIC Act. For banking institutions, including Authorised Dealers, the SARB's enforcement powers (exercised through the Registrar of Banks) are derived from the Banks Act. Although a range of sanctions is available, they may only be applied to contraventions of the Banks Act itself (s.91A). For ADLAs, the SARB's enforcement powers are derived from the FX Regulations; however, the range of sanctions available may only be applied to contraventions of the Exchange Control Regulations made pursuant to the Currency and Exchanges Act. This means that there is no specific authority for SARB to apply administrative sanctions for breaches of the FIC Act. Should an ADLA be found to be non-compliant with its obligations under the FIC Act, the ExCon will consider recommending to the National Treasury the withdrawal of the authority granted to the company to act as an ADLA. This note is contained in the "Guidelines for the submission of an application for authorisation to conduct the business of an Authorised Dealer in foreign exchange with limited authority" (Section A.4 of the Exchange Control Rulings). Nevertheless, overall, the SARB's powers of enforcement and sanction are inadequate to induce compliance with the AML/CFT requirements.

FSB

Powers to monitor, including on-site inspections, and compel production of information

626. The supervisory powers of the FSB are derived from the various pieces of legislation administered by the FSB: the LTI Act, CISC Act, FAIS Act, PF Act, and the SS Act. All four of these Acts provide that inspections by the FSB may be conducted in terms of the IFI Act (see the above discussion of SARB's inspection powers). These powers enable the FSB to inspect financial institutions within its jurisdiction for compliance with the FIC Act and to obtain relevant documents and information without a court order. The FSB's inspectorate has used its powers under s.4 of the IFI Act many times to search and seize documents.

627. However, during the on-site visit, FSB officials indicated that inspections are not conducted under the IFI Act on a regular basis; generally, they are only carried out when there is already a suspicion of something wrong. On a regular basis, the FSB says that it relies on the powers in the LTI Act, CISC Act, FAIS Act and PF Act to obtain documents and information without a court order and to conduct regular compliance visits (the FSB calls these "on-site reviews"). However, these powers are limited to the context of ensuring compliance with the FSB legislations and do not extend to ensuring compliance with other applicable legislation, such as the FIC Act. Moreover, only the CSIC Act and PF Act authorise the FSB to enter a premises to conduct a review, so it is not clear what legal basis (other than the IFI Act itself) is being used to conduct such visits.

628. There are additional powers that do require a court order – the provisions of the FI Act (Sections 5 and 6) empower the Registrar to apply to Court to compel an institution to comply with any law or a lawful request, directive or instruction issued by the Registrar under any law. Furthermore failure to comply with a request for documentation or information or where the exercise of monitoring duties by FSB personnel are frustrated or interfered with will be considered to amount to a contravention of the law

and may render a financial institution subject to the suspension or withdrawal of its licence or authorisation.

629. *Long-term Insurance Act (LTI Act):* The Registrar may by notice direct a long-term insurer to provide any specific information or documents required for the purposes of the LTI Act (s.4). Failure to comply with such a notice or directive is punishable with a fine of up to ZAR 100 000 (s.67). The Registrar does not, however, have any powers under the LTI Act to physically inspect the business premises. The FSB indicated that, should it experience resistance in allowing an on-site visit, the powers under the IFI Act would be invoked.

630. *Collective Investment Schemes Control Act (CISC Act):* The Registrar has the power to investigate the business of a person, whether registered or authorised or not, who is involved in the administration of a collective investment scheme or the soliciting of investment in a collective investment scheme (s.14). Inspectors are empowered to demand documents (s.14(2)(a)). Any person who fails to comply with any direction or notice is guilty of an offence (s.115).

631. *Financial Advisory and Intermediary Services Act (FAIS Act):* The Registrar may direct by notice an authorised financial services provider to furnish any specified information or documents (s.4). If there is reason to believe that a person is contravening or has failed to comply with a provision of the FAIS Act, the Registrar may furthermore direct a person to appear before him to discuss the matter and to make arrangements for the discharge of the person's obligations in terms of the FAIS Act (s.4(4)(a)). At the time of the on-site visit, the Registrar did not, however, have any powers under the FAIS Act or FIPF Act to physically inspect the business premises.[18]

632. *Pension Funds Act (PF Act):* The Registrar has the power to conduct a compliance visit of the business premises during which he/she has the right of access, at any reasonable time, to all documents or records as may reasonably be required, and may require persons to provide other information and explanation as necessary (s.25(2)-(3)). Administrative penalties apply for failing to comply with these provisions (s.37).

633. *Financial Institutions (Protection of Funds) Act (FI Act):* Additionally, the Registrar has powers to obtain documents and information without a court order in relation to all of the institutions that it supervises for the purpose of ensuring compliance with the LTI Act, CISC Act, FAIS Act and PF Act and SS Act (s.6(2)(a)) FI Act). Failure to comply with these provisions is an offence (s.10).

Powers of enforcement and sanction

634. The FSB has no specific authority to sanction the financial institutions within its jurisdiction for failing to comply with the FIC Act. Although a range of sanctions is available pursuant to the LTI Act, PF Act, and SS Act, these may only be applied to contraventions of those Acts themselves.

635. Additionally, the Registrar of Securities Services can refer matters of market abuse, insider trading and false reporting to an administrative tribunal, in the form of the enforcement committee, which

[18] An amendment bill was signed into law on 23 September 2008 which provides specifically for on-site (compliance visits). Section 4(5) which empowers the Registrar to "authorise any suitable person in the employ of the Board or any other suitable person to conduct an on-site visit of the business and affairs of a provider or representative, to determine compliance with this Act." Provisions also allow inspectors to size any document. Institutions that fail to comply with a request for information or documentation may be referred to the Enforcement Committee. However, these and most other provisions of the act only enter into force on 1 November 2008. This is outside of the 2-month period following the on-site visit and, therefore, cannot be taken into account in the rating.

was established pursuant to the SS Act (s.97) and may impose administrative penalties on persons who have contravened the SS Act. During 2007, the Enforcement Committee imposed administrative penalties of ZAR 2 million on a discretionary financial services provider and an authorised user for prohibited practice (price manipulation).[19] However, the Enforcement Committee has no jurisdiction in relation to violations of the FIC Act.

636. This means that there is no specific authority for FSB to apply administrative sanctions for breaches of the FIC Act. Overall, the FSB's powers of enforcement and sanction are inadequate to induce compliance with the AML/CFT requirements.

JSE

Powers to monitor, including on-site inspections, and compel production of information

637. The supervisory powers of the JSE are derived from the SS Act and JSE Rules. The JSE has powers to supervise compliance by its members with the FIC Act 2001 (Equities Rules 12.10.1.3 and 12.10.2.1.2; Derivatives Rule 3.275.1.2; and Yield-X Rule 4.10.1.3). The JSE may require any person who is subject to JSE jurisdiction to produce any book, document, tape or electronic record or other object in order to facilitate such an investigation (Equities Rule 12.10.2.1.5; Derivatives Rule 3.275.2.1.5; and Yield-X Rule 4.10.2.5). These powers are sufficiently broad to allow access to all records and conduct on-site inspections, including sample testing, without the need for a court order. These powers enable the JSE to inspect financial institutions within their jurisdiction for compliance with the FIC Act and to obtain relevant documents and information without a court order.

Powers of enforcement and sanction

638. Although the JSE may check for compliance with the FIC Act, the JSE does not currently have powers to enforce compliance (i.e. apply sanctions for non-compliance). The JSE indicates that if there were significant problems and members did not comply with requests for remedial actions (through corrective letters), the JSE would have to forward its concerns to the Centre for possible application of criminal sanctions pursuant to the FIC Act. However, no administrative sanctions could be applied for such breaches of the FIC Act. When changes to the FIC Act enter into force in 2009, this should provide more enforcement powers for the FSB, to which the JSE will refer problematic cases for administrative action. In the meantime, the JSE's powers of enforcement and sanction are inadequate to induce compliance with the AML/CFT requirements.

Recommendation 17 (Sanctions)

639. The FIC Act only provides for criminal sanctions in relation to breaches of the Act. The criminal sanctions apply equally to legal and natural persons. In cases where the directors and/or senior management of an institution are responsible for the institution's contraventions or failures, the directors and managers in question will be held liable as co-accused with the institution. The maximum penalties for offences relating to violations of CDD, record keeping and reporting requirements are imprisonment for 15 years or a fine of ZAR 10 million. The maximum penalties for offences relating to the failure to formulate internal rules, provide training to staff or appoint a compliance officer are imprisonment for five years or a fine of ZAR 1 000 000. As criminal sanctions, these penalties would be applied by the courts.

[19] The FSB has prepared draft legislation which is currently considered by Parliament and which will establish a general enforcement committee for all institutions which fall under the regulatory and supervisory functions of the FSB. Once established, this enforcement committee will provide the FSB with an effective administrative sanction to refer matter to the committee for the imposition of administrative penalties.

Criminal sanctions in respect of breaches of the FIC Act have been applied in one matter, namely S v Maddock SH7/17/08, where the accused were convicted of several contraventions of the FIC Act in respect of the identification of customers, record keeping, failure to report suspicious transaction, failure to appoint a compliance officer and failure to formulate and implement internal rules. There is no possibility to apply administrative sanctions directly for breaches of the FIC Act.

640. There are other sanctions available to certain regulators that can be applied directly for violations of the sector-specific legislation. The Banks Act authorises the Registrar of Banks to issue a directive requiring a bank, controlling company, or an eligible institution within a period specified in such a directive to: cease or refrain from engaging in any act, or perform such acts necessary to comply with the directive or to effect the changes required to give effect to the directive (s.6(6)(b)).

641. The Registrar of Banks may also cancel the registration of a Bank in certain circumstances e.g. where false information was supplied in the Bank's application for registration as a bank. In other circumstances the Registrar may apply to a High Court to have the registration of a bank cancelled on grounds such as that a director or executive officer has been convicted of an offence under the Banks Act, or that the bank does not carry on satisfactorily the business of a bank, has failed to comply with a requirement of the Banks Act, continues to employ an undesirable practice or has in a material respect misrepresented the facilities which it offers to the general public, or if the Registrar convinces the court that it is not in the public interest to allow the institution to continue its activities as a bank (s.25).

642. With regard to directors and senior managers, the Registrar of Banks may also object to an appointment or continued employment of a chief executive officer, director or executive officer of a bank if the Registrar believes that it is not in the public interest for the person concerned to hold that appointment, or that the person concerned is not a fit and proper person to do so. Such an objection would initiate a process which could result in the termination of the person's position as chief executive officer, director or executive officer of a bank (s.60(5) and (6)).

643. The Executive Officer of the FSB may also, on good cause shown, apply to court to appoint a curator to take control of and to manage the whole or part of the business of an institution (s.5 FI Act). "Good cause" is not defined in the FI Act and calls for a consideration by a court of the particular facts of each case and could in theory include contraventions of the AML/CFT legislation, although this power to enforce the FIC Act has not yet been used.

644. Section 6 of the FI Act authorises the Registrar to institute proceedings to compel any institution to comply with any law or to cease contravening a law and to compel any institution to comply with a lawful request, directive or instruction made, issued or given by the Registrar under a law. The Registrar may also publish statements that an institution has contravened a law or failed to comply with a directive, instruction or request issued or made by the Registrar. The Registrar utilises the "name and shame" provisions as the method to "blacklist" institutions that contravene the law. "Law" in this regard is not limited to the specific Acts administered by the FSB but includes all laws of the Republic of South Africa. Section 7 of the FI Act empowers the Registrar to declare a specific practice or method of conducting business an "irregular or undesirable practice" or an "undesirable method of conducting business" for a specific category or categories of financial institutions or for all such institutions.

645. An FSP licence may be suspended at any time if the Registrar is satisfied that a licensee no longer meets the licensing requirements, which include fit and proper requirements. (ss.9-10, FAIS Act). With regard to long-term insurance, the Registrar may vary the licensing conditions under certain circumstances such as, that the insurer: has made a material misrepresentation to the public; has failed to comply with a material condition subject to which it was registered, has contravened or failed to comply with a material provision of the Act. With regard to collective investment schemes, the Registrar may in

writing direct any person who employed an irregular or undesirable practice or undesirable manner of administration, to rectify in a manner required by the Registrar anything which was caused by or arose out of the employment of that practice or manner of administration (s.21(3)).

646. While there are some administrative sanctions available to regulators, they are not directly applicable for AML/CFT violations and can generally only be applied if those AML/CFT deficiencies rise to the level of undesirable business practices, safety and soundness issues, or fit and proper criteria. The current range of sanctions available for institutions and their directors and senior managers for AML/CFT is not sufficiently broad to be effective, proportionate, to the severity of a situation, and dissuasive. In particular, none of the supervisory authorities designated pursuant to the FIC Act have the power to impose disciplinary and financial sanctions, or the power to withdraw, restrict or suspend the financial institution's licence, where applicable, for FIC Act violations. This is a serious deficiency; however, it will be addressed when the FIC Amendment Act comes into force in 2009.

Market Entry – R.23

SARB-BSD

647. The Banks Act provides for the Registrar to consider the eligibility of directors and senior managers of banks, and may object to an appointment or continued employment of a chief executive officer (CEO), director or executive officer of a bank if the Registrar believes that it is not in the public interest for the person concerned to hold that appointment, or the person is not a fit and proper (s.60).

648. Section 37 of the Banks Act can be invoked to prevent criminals from holding or being beneficial owners of a significant or controlling interest. Shareholding – total nominal value and/or voting right – totalling more than 15% requires approval. If that person chooses to acquire additional shareholding up to 24%, additional approval is required. Proposed shareholdings up to 49% may only be approved upon the recommendation of the Registrar, and those above 49% require the direct approval of the Minister. The conditions at each level are that permission for the proposed acquisition shall not be granted unless the Minister of Finance is satisfied that the proposed acquisition will not be contrary to the interest of the public, the bank concerned, the depositors or the controlling company concerned (s.37(4)). The Minister also is required to consult and take into account the views of the Competition Commission concerning the acquisition. Nevertheless, one concern is that adequate measures are not taken to determine beneficial ownership. Legal persons may be shareholders and an offshore company could hold up to 49%. However, SARB indicated that it authorises ownership only after face-to-face meetings with the applicants.

649. Section 60(5) read with Section 1(1A) of the Banks Act together with Regulation 42 of the Regulations relating to Banks, can be invoked to prevent criminals or their associates from holding a management function or directorships of banks, and also directors and senior management, who need the approval of the Registrar. The applicants are required to complete a detailed application form (BA 020), where the criteria of fitness and propriety are carefully considered. Questions 19 to 27 of the BA020 questionnaire delve into the personal probity of the applicant.

FSB

650. There are varying requirements to prevent ownership/control by criminals and their associates and fit and proper tests in the various FSB-supervised entities.

651. *LTI Act:* The registrar must approve all shareholdings that: directly or indirectly alone or with a related party exercise control over the long-term insurer (s.26(1)); or represent over 25% of the total nominal value of all the issued shares of the long-term insurer (s.26(2)). There is no legal requirement to submit perspective directors and senior management of long-term insurers to fit and proper tests, although

South African authorities indicate that, in practice, this occurs and complies with the corresponding IAIS core principles to which the FSB subscribes. The FSB has the statutory power to terminate the appointment of a director or senior manager if "the person or firm is not fit and proper to hold the office concerned" (s.22).

652. *FAIS Act*: The FAIS Act applies a set of detailed criteria when applying the fit and proper test to applicants, including personal character qualities of honesty and integrity, competence and operational ability to fulfil the responsibilities imposed by the Act, and the applicant's financial soundness (s.8). All "key individuals" (persons who manage and oversee the rendering of financial services) of FSPs must comply with characteristics of honesty and integrity in terms of paragraph 2 of the Determination of Fit and Proper Requirements for Financial Services Providers. Specific questions are asked in the application (FAIS application form FSP4). This information is verified on a random basis through consumer credit checks and criminal record verification. Credential verification is performed by external service providers. However, fit and proper tests do not apply to all directors of FSPs.[20] If a key individual (person who manages and oversees the rendering of financial services) no longer meets fit and proper criteria, including qualities of honesty and integrity, the Registrar may instruct the FSP to remove that key individual and appoint a new person (s.8 FAIS Act) or may suspend the FSPs licence (s.9) An FSP must debar a representative should he/she no longer comply with the fit and proper requirements (s.13).

653. *CISC Act*: In order to administer collective investment scheme, a person must be registered as the manager by the registrar or its authorised agent (s.5). A company that applies to manage a collective investment scheme must apply to the register and supply any relevant information (s.42(2)). The application will be approved if, *inter alia*, the registrar is satisfied that the proposed directors, management, trustee or custodian and auditors are qualified as required by or under the CISC Act, the manger is fit to assume the duties and responsibilities of a manager, and the registration will be in the public interest. In addition, to *inter alia* avoid conflicts between his/her interests and the interests of investors, a manager of a CIS must disclose to investors the interests of directors and management, organise and control the scheme in a responsible manner, employ adequately trained staff and ensure that they are properly supervised (s.4 CISC Act).

JSE

654. In order to trade listed securities on an exchange a person must be an authorised user in terms of the rules of the exchange (s.19 SS Act). The SS Act (Section 18) provides for the matters which must be dealt with in the rules of an exchange. These include the criteria for authorisation and exclusion of authorised users and, the supervision by an exchange of compliance with the duties imposed on its authorised users by the FIC Act. Section 18(2) of the SS Act requires the JSE Rules to provide criteria for authorising and excluding authorized users (member firms) who do not (or no longer) meet the following requirements:

- is of good character and high business integrity or, in the case of a corporate body, is managed by persons who are of good character and high business integrity; and

- complies or, in the case of a corporate body, is managed by persons or employs persons who comply with the standards of training, experience and other qualifications required by the exchange rules.

[20] Amendments to the FAIS Act are proposed which would give the Registrar the power to consider also the fitness and proprietary of all directors of FSPs.

655. The Registrar of Securities Services approves the rules or any amendments thereto of licensed exchanges. (s.61 SS Act).

656. All authorised users of the JSE must comply with the specific JSE Rules regarding market entry. Officers (dealers/traders and compliance officers), directors and shareholders (natural persons) who own, directly or indirectly, in excess of 10% of issued shares of a member must meet fit and proper requirements (JSE equities rule 4.10.1; derivative rule 3.20, yield-X rule 3.30). This requirement does not cover beneficial ownership or go beyond the 10% if the shareholder is a legal person. Fit and proper criteria cover, inter alia, financial solvency, no convictions or being held liable for fraud, theft, or market abuse, a formal investigation by any regulatory or government agency, dishonesty or deliberate omission in an application to the JSE. The JSE Rules do not currently specify that persons holding a management function meeting the fit and proper criteria, and they do not currently include "expertise" as a criteria, although JSE intends to cover this in the next version of the JSE Rules.

Foreign exchange dealers

657. Natural and legal persons providing money or currency changing services must be licensed in South Africa, pursuant to the Exchange Control Regulations (ss.1 and 2). These take the form of "authorised dealers" (registered banks in South Africa) or "authorised dealers with limited authority" (ADLAs) (currently 27 business providing currency exchange for tourists). In terms of Section 3 of the Orders and Rules under the Exchange Control Regulations certain banks have been appointed as authorised dealers.

658. Only authorised dealers may buy or borrow any foreign currency or any gold from, or sell or lend and foreign currency or any gold to any person not being an authorised dealer (except with the permission granted by the Treasury, in accordance any conditions as the Treasury may impose) (s.1(2) Exchange Control Regulations). An authorised dealer may only buy, borrow or receive or sell, lend or deliver any foreign currency or gold for such purposes or on such conditions as the Treasury may determine. Normal day-to-day banking business between residents of South Africa is dealt with under the Banks Act and therefore not in the domain of the ExCon.

659. The ExCon scrutinises the curriculum vitae (CVs) and experience of staff who work in the exchange control environment of the Authorised Dealers and ADLAs. Additionally, the following market entry requirements apply.

660. *Authorised dealers:* Authorised dealers which are subject to the Exchange Control Regulations are also licensed banks or branches of foreign banks which are regulated by the Registrar of Banks (see above for more details about the licensing requirements for banks).

661. *ADLAs:* Directors and senior management of ADLA are subjected to "fit and proper" tests. Only South African residents (*i.e.* a natural or legal person) who are deemed to be "fit and proper" may, directly or indirectly, have or take up a shareholding or an equity stake in an ADLA. This test is applied as part of a licensing procedure which must be renewed every year (subsections D.(iv)(d), (e) and (v)(a) of Section A.4, Exchange Control Rulings). Individuals who are holding (or are proposing to hold) the office of a director of or shareholding in an ADLA are required to complete a questionnaire which deals with aspects of beneficial ownership (significant or controlling interest in the ADLA). The applicant must also provide a certified copy of a statement of criminal convictions from the SAPS.

662. As part of the conditions for doing business, the applicant must confirm in writing that it is conversant with the provisions of the FIC Act and submit its draft internal AML/CFT control rules and the name of the compliance office to the ExCon (s.42 FIC Act). The ExCon will, in consultation with the

Centre, indicate whether the draft internal rules are sufficient to enable the ADLA to comply with its obligations under the FIC Act. After it commences business operations, the ADLA is required to confirm in writing to ExCon that its draft internal rules have been implemented unchanged. An ADLA must inform ExCon in writing of any subsequent changes to its internal rules prior to their implementation, supported by a copy of the amended internal rules. Should an ADLA be found non-compliant with its obligations under the FIC Act, ExCon will consider recommending to the National Treasury that the ADLA's authority to act be withdrawn.

Money/value transfer service businesses

663. Money/value transfers services are provided by authorised dealers, Postbank and through informal (underground) systems. The international remittance providers are, primarily, authorised dealers (including the agents of MoneyGram) and Postbank. International remittances are tightly controlled by the Exchange Control Regulations, although there may be a very small gap in relation to certain types of remittances conducted through informal systems. Domestic money/value transfers are not subject to the Exchange Control Regulations and, therefore, can be performed by persons other than authorised dealers and Postbank. No registration/licensing requirements apply to natural or legal persons conducting a purely domestic money/value transfer business.

664. *Authorised dealers:* Authorised dealers are subject to the Exchange Control Regulations are also licensed banks or branches of foreign banks which are regulated by the Registrar of Banks (see above for more details about the licensing requirements applicable to banks). Authorised dealers may take or send out of South Africa bank notes, gold, securities or foreign currency, or transfer any securities from the South Africa elsewhere (s.3(1) Exchange Control Regulations). Foreign currency is defined as "any bill of exchange, letter of credit, money order, postal order, promissory note, traveller's cheque or any other instrument for the payment of currency payable in a currency unit which is not legal tender in the Republic."

665. *Postbank:* Postbank is not an authorised dealer. Its authority to provide international remittance services is derived from the Postal Services Act 1998 (PS Act) which provides that money may be remitted through the postal company either within or outside the Republic (s.47). Postbank provides two types of money transfer services: money orders and postal orders.

666. The ***money order service*** operates in a similar manner to a bank transfer. The teller is provided with cash by a client, a once-off account is opened and the cash is deposited therein. The teller provides the client with a unique reference number which is passed on to the recipient of the funds. The recipient of the funds can then collect the funds at another branch by providing the teller with his identification document as well as the unique reference number. The identification document will be verified against the details submitted by the client. Money can be transferred to or from certain Southern African Development Community (SADC) countries (Botswana, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, South Africa, Swaziland, Tanzania, and Zambia).

667. The ***postal order service*** operates in the following manner. The teller is provided with the cash and a postal order (receipt) is given to the client. The client then posts the postal order to the intended recipient. The postal order is then redeemed at the Post Office or any other South African Bank. Money can only be redeemed within the borders of South Africa or certain SADC countries (indicated in the paragraph above). The use of the denomination postal orders (on which the value has been pre-printed) was discontinued on 30 April 1998. They were replaced by postal orders on which the value is computer printed or written by hand.

668. *Informal systems:* Certain types of remittances conducted through informal systems would not be covered by the Exchange Control Regulations (*e.g.* where the transfer is effected by telephone, without any instrument for payment being taken out of the country). However, this is a small gap since, in the South African context, most informal money remittance is effected through physical cross-border transportation of cash (*e.g.* by taxi and bus drivers).

Other financial institutions

669. Financial leasing and financing companies that are not subject to licensing or registration requirements, and this exclusion has not been based on any risk assessment.

Ongoing supervision and monitoring – R.23 & 32

670. For financial institutions that are subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes and which are also relevant to money laundering, apply in a similar manner for AML/CFT purposes. This includes requirements for: *(a)* licensing and structure; *(b)* risk management processes to identify, measure, monitor and control material risks; *(c)* ongoing supervision; and *(d)* global consolidated supervision where required by the Core Principles.

Banking sector – Ongoing supervision and monitoring by BSD

671. Banks are monitored and supervised by the SARB through the BSD. Since 2005, the BSD has used Section 6 of the Banks Act to conduct its own compliance visits and Section 7 of the Banks Act to appoint inspectors to carry out specific audits.

672. The inspection regime is determined using a risk-based approach, but BSD aims to cover each bank every 12-18 months. Each person in the BSD's Relationship Team is generally responsible for two banks, and the BSD evaluates each relationship, including the associated risks. BSD discusses with the CEO the bank's short/medium/long term strategy and control environment, and continues to engage with the bank throughout the year. A wide range of risk factors are considered, including quantitative risks (solvency, market, operational, credit, technological) and qualitative risks (corporate governance and AML). BSD then prioritises those banks considered to be riskier, and considers what the riskier areas of each bank are.

673. At the beginning of each year, banks are advised of the assessment schedule. The intensity of the inspection is also based on risk. The total inspection time for a large bank might take six people and several months, whereas for a smaller bank it could be one or two weeks. Generally, AML/CFT components are part of a larger inspection, accounting for approximately 10-15% of the total inspections conducted. However, BSD also conducts specifically targeted AML/CFT inspections when warranted.

674. During 2005 and 2006, the Registrar of Banks commissioned two firms of auditors (appointed using its Section 7 authority) specifically to verify compliance with the FIC Act requirements by the five largest banks (which hold over 80% of total assets). This was the second AML/CFT review of the banks. In particular, the audit covered verification of the client-verification data. At the time, this was deemed to be the most significant area on which to focus inspection work, since the FIC Act required verification of existing customers. In practice, banks had to essentially freeze accounts until customers provided additional CDD information. The audits also aimed to ensure that board-approved policies were in place (*e.g.* specific procedures, internal controls, training, and reporting lines for STRs) and had been filtered down to the rest of the organisation. In general, the audits found that banks' internal audit functions were robust, although the reports noted that in some cases KYC documentation was not being kept. In 2007, SARB made its own follow-up visits to banks where particular problems had been identified. These follow-up visits also covered the internal audit functions of the bank.

675. During 2006, the BSD's review team performed a similar review of the remaining banks and selected branches of foreign banks. The review comprised an analysis of the policies and procedures of the banks concerned, coupled with the testing of sample files to assess whether or not each bank's policies and procedures complied with the implementation of best practice. BSD provided the following statistics which set out the overall results of inspections including AML/CFT that were conducted between November 2004 and January 2007.

TYPE OF BANK	MOSTLY COMPLIANT	MOSTLY COMPLIANT (SOME ITEMS NEED IMPROVING)	IMPROVEMENT REQUIRED	NOT COMPLIANT	TOTAL
Registered banks Locally controlled	8	1	3	0	**12**
Registered banks Foreign controlled	3	2	1	0	**6**
Mutual banks	0	1	1	0	**2**
Branches of foreign banks	1	4	0	0	**5**
TOTALS	**12**	**8**	**5**	**0**	**25**

676. During the course of these inspections, the following FIC Act breaches were noted:

Statistics on AML/CFT breaches found in the eight banks which were set report back deadlines in their closing letters	Total
Know-your-client (KYC) policies and procedures not approved by the board	3
KYC and anti money-laundering policies and procedures not consolidated into one set of integrated documents	6
Clients not classified into risk categories as required by the FIC Act	3
Risk framework as required by the FIC Act not developed	2
KYC files not produced when requested from the bank	3
Acceptable ID document not defined	1
Procedures for verification of foreign nationals not specified	1
Procedure for verification of politically exposed persons not specified	2
Procedure for verification of correspondent banks not specified	1
Procedure for verification of organs of state not specified	3
Procedure for verification of provident and pension funds not specified	3
Procedure for non face-to-face verification of clients not specified	2
Procedures for freezing and unfreezing of non-cooperative accounts not specified	5
Procedure for ongoing monitoring of clients details not specified	3
Account opening procedures need modification to include KYC	1
Procedures for acceptance of faxed copies not specified	2

Statistics on AML/CFT breaches found in the eight banks which were set report back deadlines in their closing letters	Total
Four eyes principle not applied in the KYC process	2
Copies of verification documents not marked original sighted	3
Controls weakness in verification procedures for trusts, close corporations and non-listed companies	3
Control weaknesses resulting in classification of non-compliant clients as fully compliant	3
Procedure for suspicious activity reporting to be developed	1
The bank does not control KYC processes and procedures in its associates	1
System modification required to automate KYC monitoring	1
Reverification of all trusts, close corporations and unlisted companies required	3
TOTALS	**58**

677. Following the on-site reviews, BSD sent the banks inspection report letters indicating its findings and recommendations. In each case, it was indicated that the BSD's Relationship Team would follow up on the implementation of the recommendations contained in the letter. It is important to note that, because the SARB has no power to sanction for breaches of the FIC Act, the inspection report letters do not qualify as sanctions pursuant to Recommendation 17. In the one instance where more serious action was taken (a determination as to whether a locally controlled domestic banks should continue to exist in its current form), SARB was able to act because the bank had systemic problems including AML/CFT breaches.

Insurance sector – Ongoing supervision and monitoring by FSB

678. The insurance sector is monitored and supervised by the FSB. A risk-based approach to supervising insurance entities was introduced in 2007, using a risk matrix based on the approach of Canada's Office of the Superintendent of Financial Institutions (OFSI). At the stage of considering licence applications, the risk management systems of the applicant insurer are evaluated. Risk factors include size of entity, market impact, corporate governance, compliance history, financial strength, evaluation of the fit and proper criteria, and any complaints received. All new insurers are visited within the first year, so AML is factored in at that time and through later compliance history. Quarterly and annual reports are required to be submitted by insurers for off-site prudential supervision. An on-site visit with a major insurer generally lasts about a week with a team of eight to nine persons. For a smaller insurance company, two to three staff members would visit the company for one day. About 5-10% of the visit would be focused on AML/CFT issues.

679. In 2007, the FSB conducted a series of dedicated AML inspections on 68 long-term insurers. The inspections lasted one to two days depending on size of institution. The FSB spoke with management, tested KYC records, and reviewed training manuals and processes for internal controls, reporting pursuant to the FIC Act, and appointing staff. The chart below shows the number of entities and inspections conducted.

Financial Services Board-Long-term Insurers Statistics- FIC ACT/FATF Review						
		2003	2004	2005	2006	2007
Number of Institutions		75	78	78	81	82
Size of the type of institutions	Assets ZAR Billion	822	907	1 086	1 302	1 420
Size of the type of institutions	Premiums ZAR Billion	157	157	165	220	226
Number of on-site examinations involving AML/CFT component		0	20	0	14	68
Number of cases involving sanctions for non reporting of money laundering		0	0	0	0	1
Number of cases when sanctions were applied		0	0	0	0	1

680. As in the case of security brokers (see below), the results of these onsite reviews can be summarised as "partially compliant", as some technical breaches were identified. Most of the insurers relied on top management's buy-in for their internal rules, training programmes and processes for establishing and verifying client identification. The FSB requested insurers to escalate approval of these policies to board level with a view to involving the board (including non-executive directors) in the process of AML/CFT compliance. Other issues that were, in some cases, addressed included not conducting ongoing training and examination of staff members, not risk rating clients and not identifying PEPs. Although one instance of money laundering was discovered that had not previously been reported, the other long-term insurers had adequate internal rules and procedures to meet the CDD and reporting requirements. It is important to note that, because the FSB has no power to sanction for breaches of the FIC Act, the action that was taken following inspections does not qualify as sanctions pursuant to Recommendation 17.

Securities dealers – Ongoing supervision and monitoring by JSE

681. Authorised users of the securities exchange are monitored and supervised by the JSE. The JSE Securities Exchange is a licensed exchange in terms of Section 10 of the SS Act and therefore subject to the supervision of the Registrar of Securities Services (the Executive Officer of the FSB) (s.5 SS Act). FSB does not undertake formal reviews of the members (authorised users) of the exchanges.

682. As at 11 August 2008, 188 different legal entities were authorised users (members) of the four JSE markets. JSE uses a risk-based approach to review 108 of its members, being those members for whom the JSE is the supervisor in relation to the FIC Act (the other 80 members, are regulated by either SARB or FSB, are dormant members or proprietary traders that have no clients). In particular, the JSE targeted the equities market, as the equities members hold a significant amount of client assets (cash and securities) on behalf of clients.

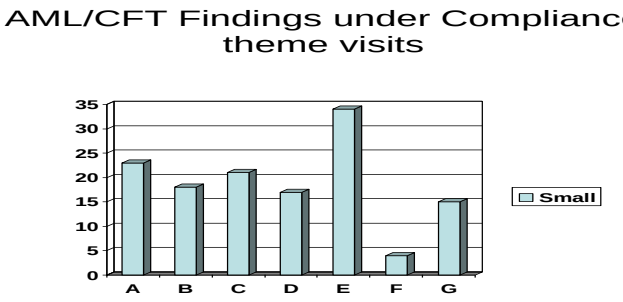
683. Since 2007, the JSE has inspected 19 members (12 conducted jointly with the Centre) who account for 90% of total assets under management. The findings of these reviews can be summarised as "partially compliant". All of the members had internal rules, training programmes, and compliance officers in place. In some instances, however the internal rules had to be amended (*e.g.* to specifically prohibit the application of an exemption where a suspicious transaction had been identified/reported). Another finding was that some members had not implemented procedures to identify high risk clients/transactions and had not implemented enhanced client identification and verification procedures in respect of high risk clients/transactions.

684. Following the reviews, JSE sent letters recommending corrective actions to the members. It is important to note that, because the JSE has no power to sanction for breaches of the FIC Act, these letters do not constitute sanctions pursuant to Recommendation 17. To date, all members have taken the recommended corrective action. The JSE noted that, if a member did not take the recommended corrective action, the JSE would refer the matter to the Centre for possible prosecution. With the new amendments to the FIC Act in 2009, the JSE will be able to refer matters to the enforcement board of FSB for further action.

Financial Service Providers – Ongoing supervision and monitoring by FSB

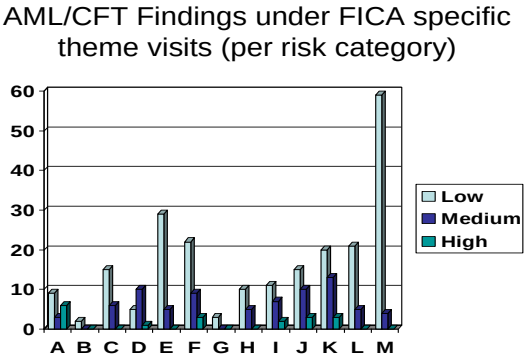
685. Financial Services Providers (FSPs) are monitored and supervised by the FSB. Supervision of FSPs authorised under the FAIS Act is determined on a risk-based approach. Before issuing an FSP license, a risk assessment is conducted. Entities are categorised from low to high impact (risk). Several factors are used to determine the risk, include the size of the entity and whether they handle client funds. Handling client funds is a factor that automatically moves the FSP into the medium or high impact category. For higher-impact FSPs, the FSB conducts an on-site visit prior to issuing a license. Ongoing ratings are determined by compliance reports, which contain specific AML/CFT components (such as control systems and client files). Annual compliance reports and violations can result in a change of the risk category, and if serious violations are found, a formal inspection would be conducted. Regular visits are conducted on the medium and high impact providers, on a three to five year cycle, depending on the risk.

686. A total of 164 small FSPs have been assessed for AML/CFT compliance during normal compliance theme visits. In 2007, the FSB also conducted 170 random AML/CFT specific theme visits for the 170 different FSPs regulated under FAIS. As a result of these visits, the FSB detected few AML/CFT specific concerns; most pertained to general regulatory compliance. The following charts specify the nature of the AML/CFT breaches detected.



A=	Failure to carryout client identification & verification	14%
B=	Failure to verify source if client's funds	11%
C=	Failure to have internal rules in place	13%
D=	Failure to attend training/train employees	10%
E=	Failure to have procedures for dealing with PEPs	21%
F=	Failure to have procedures for dealing with STRs	2%
G=	Failure to risk profile clients	9%

687. The following chart consolidates the findings for all 170 FSPs, broken down by risk category.



A	Full compliance with the FIC Act legislation	11%
B	Non compliance with the FIC Act	2%
C	Failure to establish and verify identities of new clients	12%
D	Failure to establish and verify identities of existing clients	9%
E	Failure to train employees on AML/CFT	20%
F	Failure to provide records of training attended	20%
G	Failure to have procedures for dealing with non face to face clients	2%
H	Failure to have procedures for dealing with and/or generate STRs	9%
I	Failure to verify clients' source of income	12%
J	Failure to risk profile clients	16%
K	Failure to have procedures for dealing with PEPs	21%
L	Failure to formulate and implement internal rules	15%
M	Utilisation of generic documentation	37%

688. Both general regulatory and AML/CFT findings were communicated back to the relevant FSPs by way of letters. The FSPs were requested to rectify the non-compliance issues and to provide confirmation, including copies of documentation, that the findings were indeed addressed. All FSPs confirmed in writing that the requested action was taken within the stipulated time period.

689. The FSB's largest concern was that most of the small FSPs were utilising generic documents provided to them by external agents (*e.g.* compliance officers, industry associations and professional bodies) to assist them in establishing the required FIC Act controls, procedures, systems and processes. The FSB requested these FSPs to customise the documents in line with their business needs. In addition, the FSB met with the above agents and participated in their workshops/seminars to have them take this matter up with their members. The FSB also utilised the FAIS newsletter to communicate its general concerns and findings regarding the onsite visits to the FSPs. The newsletter is published quarterly and is sent to all authorised FSPs. There were only two small FSPs that failed to comply with FIC Act in its entirety. One has since opted to lapse its licence. The other has engaged with the FSB, indicating that many of the findings have been rectified and requesting some exemptions from certain provision of FIC Act. This FSP will be re-visited later in 2008. It is important to note that, because the FSB has no power to sanction for breaches of the FIC Act, none of this action constitutes sanctions for the purpose of Recommendation 17.

690. In 2008, the FSB assessed 16 medium-sized FSPs for compliance with the FIC Act under the new risk-based supervision model. These FSPs, which are all companies in good standing, were selected to be used as test cases for providing practical training to FSB staff. In only one case did FSB find any FIC Act deficiencies. Risk based supervision on-site visits will commence on a full scale from 1 September 2008.

Foreign exchange dealers – SARB (ExCon)

691. SARB's BSD supervises certain foreign exchange dealers (so-called "Authorised Dealers") that are also banks which are also authorised to deal in foreign exchange. However, there were no separate statistics on specific AML/CFT inspections of these banks. ADLAs, which may only perform travel-related *bureau de change* functions (*i.e.* convert currencies and redeem travellers' cheques), are supervised by the SARB through ExCon for compliance with the exchange control requirements and FIC Act.

692. During 2007/2008, ExCon visited 149 ADLA outlets. Thirteen were visited twice and three were visited three times. The reasons for the more frequent visits were due to the fact that these outlets were mostly situated in "tourist attraction" areas and compliance in terms of the FIC Act was poor. A few examples of poor compliance detected are:

- no proof of residence recorded;
- no copies of passports/identity documents attached to the transaction;
- P.O. Boxes address accepted;
- non-compliance with UNSC 1267 lists;
- faxed copies of proof of residence accepted;
- no policy and procedure documents available at the outlet;
- poor knowledge of anti-money laundering in general;
- no anti-money laundering training given to newly employed front-line tellers; and
- poor knowledge on the requirement of the FIC Act evident.

Money remittance

693. Authorised Dealers (which are registered banks authorised to deal in foreign exchange and conduct international remittances) are supervised by the SARB through BSD for compliance with the exchange control requirements and the FIC Act. ExCon is responsible for the supervision of compliance by Authorised Dealers with exchange control requirements.

694. Postbank provides money transfer services, but does not have a designated supervisor. The Centre has been supervising it in the meantime, even though it has no official supervisory powers.

695. It should be noted that the largest provider of money remittance services in South Africa has not yet been visited for an AML/CFT review, despite having reported the vast majority of total STRs.

Joint inspections with the Centre

696. Although not formally designated as a supervisory, the Centre has been building AML/CFT capacity in the other supervisors and in the industry by conducting joint inspections with those supervisors. The Centre has also conducted on-site reviews of Postbank, which does not have a designated AML/CFT supervisor, as indicated in chart below.

On Site Reviews Conducted by the Centre Compliance and Prevention Department during period April 2006 to March 2009				
Supervisory Body (jointly with)	**Accountable Institution sector**	**FY2006/07**	**FY2007/08**	**FY2008/09**
SARB Exchange Control Department	Authorised Dealers in foreign exchange with Limited Authority	**16**	**25**	**9**
Financial Services Board	Insurance Companies	**-**	**52**	**-**
Financial Services Board	Financial Service Providers	**-**	**26**	**-**
Financial Services Board	Collective Investment Scheme Managers	**-**	**24**	**-**
JSE Limited	JSE stockbrokers	**-**	**3**	**9**
The Centre (conducted solely)	Post Office Bank branches	**-**	**27**	**30**

Recommendation 32

697. South African authorities maintain adequate statistics of on-site examinations conducted by supervisors relating to or including AML/CFT and any sanctions applied.

Guidelines – R.25 (Guidance for financial institutions other than on STRs)

698. The Centre has also issued four guidance notes under Section 4(c) of the FIC Act to provide interpretations in relation to certain aspects relating to the obligations to establish and verify customers' identities. As explained above in the preamble to Section 3, these Guidance Notes do not constitute "other enforceable means" as defined by the FATF. In addition, Guidance Note 3 only applies to banks and comprehensive guidance to other financial sectors has not been issued.

- Guidance Note 1 "Guidance Concerning the Identification of Clients" issued in April 2004 focuses on the application of the risk-based approach to the identification and verification of customers. It encourages accountable institutions to accurately assess money laundering risks associated with their customer base, products and transactions and develop and implement appropriate identification and verification procedures to mitigate those risks.

- Guidance Note 2 "Guidance to Financial Services Industries Regulated by the Financial Services Board Concerning the Meaning of the Word "Transaction" issued in June 2004 provides guidance regarding the definition of transaction with respect to customer identification and verification.

- Guidance Note 3 "Guidance for Banks on Customer Identification and Verification And Related Matters" issued in July 2005 provides additional guidance with respect to client identification and

verification and risk management. It also addresses the treatment of politically exposed persons (PEPs) and corresponding banking relationships.

- "Guidance Note 4 on Suspicious Activity Transaction Reporting" issued in March 2008 provides guidance to accountable institutions on meeting the requirements of Section 29 of the FIC Act which requires accountable institutions to report suspicious and unusual transactions.

699. While Guidance Notes 1 and 2 apply to all sectors, they do not comprehensively cover the FIC Act requirements, while Guidance Note 3 comprehensively covers CDD requirements but only for banks. None of this guidance contains a description of ML/FT techniques and methods.

3.10.2 Recommendations and Comments

700. Overall, the supervisory framework should be extended to those financial institutions that are currently not covered: finance companies; leasing companies; collective investment scheme custodians; money lenders other than banks; securities custodians licensed under the FAIS Act, Postbank and members of the Bond Exchange.

701. *R.23:* For financial service providers, fit and proper tests should apply to all directors. Directors of collective investment schemes or long-term insurers should be submitted to fit and proper tests. The JSE Rules should be amended to specify that persons holding a management function meeting the fit and proper criteria, and they do not currently include "expertise." There should also be licensing or registration requirements to natural or legal persons conducting money/value transfer within South Africa.

702. *R.29:* Currently, outside of the Inspection of Financial Institutions Act, there is not clear authority for the SARB and the FSB to inspect for compliance for the provisions of the FIC Act; clearer authority should be provided (and is expected once amendments to the FIC Act enter into force in 2009).[21]

703. *R.17:* Sanctions for non-compliance with the FIC Act are not sufficiently effective and proportionate. Currently the FIC Act only provides for criminal sanctions for breaches of the Act. South Africa should enhance the authority to apply sanctions that are more broadly effective, proportionate, and dissuasive. This is also expected once amendments to the FIC Act enter into force in 2009.

704. *R.25:* South African authorities should issue comprehensive guidance on CDD and other FIC Act measures to the other financial institutions and also issue guidance containing ML/FT trends and methods.

705. R.30: South African authorities should consider expanding the staff for the BSD's review team and FSB compliance areas. Ongoing AML/CFT training for BSD staff should also be enhanced.

[21] The Centre also monitors and gives guidance to relevant entities regarding their compliance with the FIC Act, but it does not have comprehensive supervisory or regulatory powers. However, the *Financial Intelligence Centre Amendment Bill 2007*, which has been passed by the Parliament and in the process for signature by the President to become law and come into effect in 2009, will provide the Centre and supervisory bodies with powers to conduct inspections and impose administrative sanctions on any accountable institutions, reporting institutions or other persons for contraventions of the FIC Act and regulations.

3.10.3 Compliance with Recommendations 23, 29, 17 & 25

	Rating	Summary of factors relevant to s.2.10 underlying overall rating
R.17	PC	• Sanctions are not sufficiently effective and proportionate. Only criminal sanctions can apply for breaches of the FIC Act. • There is no specific authority for SARB, FSB, or JSE, to apply administrative sanctions for breaches of the FIC Act. • Scope issue: The following financial institutions are not subject to AML/CFT supervision: finance companies; leasing companies; collective investment scheme custodians; money lenders other than banks; securities custodians licensed under the FAIS Act , Postbank and members of the Bond Exchange. • Effectiveness: Low level of compliance with AML/CFT requirements in the insurance sector, and among securities market participants. No sanctions have been applied, even though breaches of AML/CFT requirements detected.
R.23	PC	• For financial service providers, insurers and CIS, fit and proper tests do not apply to all directors. • There is no legal requirement to submit directors and senior management of long-term insurers to fit and proper tests. • Market entry (banks, securities market participants): adequate measures not taken to determine beneficial ownership or (for JSE) go beyond the 10% if the shareholder is a legal person. • The JSE Rules do not currently specify that persons holding a management function meeting the fit and proper criteria, and they do not currently include "expertise" as a criteria. • No registration/licensing requirements apply to natural or legal persons conducting money/value transfer within South Africa, financial leasing and finance companies. • There is no designated AML/CFT supervisor for Postbank or the Bond Exchange. • Certain types of remittances through informal systems not covered. • Scope issue: The following financial institutions are not subject to AML/CFT supervision: finance companies; leasing companies; collective investment scheme custodians; money lenders other than banks; securities custodians licensed under the FAIS Act, Postbank and members of the Bond Exchange. • Effectiveness: Low level of compliance with AML/CFT requirements in the insurance sector, and among securities market participants. No sanctions have been applied, even though breaches of AML/CFT requirements detected. The largest provider of money remittance services in South Africa has not yet been visited for an AML/CFT review, despite having reported the vast majority of total STRs. Insufficient resources for SARB (BSD and ExCon) and FSB, given the number of entities that they supervise.
R.25	PC	• Guidance Note 3 only applies to banks and comprehensive guidance on FIC Act requirements to other financial sectors has not been issued. • The guidance does not contain a description of ML/FT techniques and methods.
R.29	PC	• There is not clear authority for the FSB to inspect for compliance, conduct on-site visits, and obtain information to determine compliance with the FIC Act. • For insurers and FSPs, the FSB does not have general authority to conduct visits in relation to AML compliance, and does not use the broad powers under the IFI Act to conduct inspections. There is no specific authority for SARB, FSB, or JSE, to apply administrative sanctions for breaches of the FIC Act. • Scope issue: The following financial institutions are not subject to AML/CFT supervision: finance companies; leasing companies; collective investment scheme custodians; money lenders other than banks; securities custodians licensed under the FAIS Act, Postbank and members of the Bond Exchange.

3.11 Money or value transfer services (SR.VI)

3.11.1 Description and Analysis (summary)

706. Foreign remittance activities can only be provided by Authorised Dealers, pursuant to Regulations 2 and 3 of the Exchange Control Regulations, and Postbank pursuant to the PS Act and Exchange Control Regulations. Authorised dealers are appointed by the Minister of Finance and are licensed banks. No registration/licensing requirements apply to natural or legal persons conducting a purely domestic money/value transfer business. See Section 3.10 above regarding "Market entry" for further details. As banks, Authorised Dealers do not operate through agents; each bank must be licensed as a separate authorised dealer.

707. Authorised dealers are licensed banks and are therefore subject to the provisions of the FIC Act in relation to identification of customers, record-keeping, reporting of information and internal compliance structures and training. Postbank is also subject to these requirements. However, as discussed in Sections 3.2, 3.3, 3.5, 3.6, 3.8 and 3.10 of this report, a number of deficiencies relating to CDD, record-keeping, monitoring of transactions, and supervision have been identified so money/value transfer (MVT) service operators are not subject to the full range of the applicable FATF Recommendations. Moreover, the authorities have not taken any substantial action to address the informal (underground) remittance sector.

708. SARB (through the BSD) supervises authorised dealers (as they are banks) for compliance with applicable AML/CFT requirements. However, as noted above, the systems in place to monitor and ensure compliance for banks are not adequate. Postbank does not have a designated supervisor for compliance with AML/CFT requirements. As well, there are not effective, proportionate, and dissuasive sanctions that can be applied to MVT service operators that fail adequately comply with provisions of the FIC Act (see Section 3.10 above under the discussion of Recommendations 23, 29, and 17).

3.11.2 Recommendations and Comments

709. South African authorities should subject natural and legal persons conducting remittance only within South Africa to licensing or registration. South African authorities should also expand the scope of obligations to comply with the applicable FATF Recommendations.

3.11.3 Compliance with Special Recommendation VI

	Rating	Summary of factors underlying rating
SR.VI	PC	• There is no requirement for an MVT service operator that conducts operations within South Africa to be licensed or registered. • MVT service operators are not subject to the full range of the applicable FATF Recommendations. • The systems in place to monitor and ensure compliance for banks are not adequate and there is no designated AML/CFT supervisor for Postbank. • There are not effective, proportionate, and dissuasive sanctions that can be applied to MVT service operators that fail adequately comply with provisions of the FIC Act. • No substantial action has been taken to address the informal (underground) sector.

4. PREVENTIVE MEASURES – DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

General description

710. The FIC Act, the MLTFC Regulations, Exemptions 2 to 6, Guidance Note 1 on CDD and Guidance Note 4 on STR Reporting generally apply to all accountable institutions in the same way, regardless of whether they are designated non-financial businesses and professions (DNFBP) or financial institutions. Consequently, for DNFBP, this common legal framework suffers from the same deficiencies as for financial institutions (see Section 3 of this report for more details). This Section of the report will focus only on those aspects of the legal framework and implementation which are unique to the DNFBP.

4.1 Customer due diligence and record-keeping (R.12)

(applying R.5, 6, and 8 to 11)

4.1.1 Description and Analysis

711. The following DNFBPs are designated as accountable institutions pursuant to the FIC Act:

- attorneys;
- boards of executors, trust companies or any other person that invests, keeps in safe custody, controls or administers trust property (*i.e.* trust service providers);
- estate agents (*i.e.* real estate agents);
- persons who carry on a business in respect of which a gambling licence is required (*i.e.* casinos, regardless of their form); and
- persons who carry on the business of rendering investment advice or investment broking services, "*including* a public accountant as defined in the Public Accountants and Auditors Act, 1991" (PAA Act). This last category is not limited to public accountants (*i.e.* auditors); any person who carries on such business is covered (including auditors even though the PAA Act is now repealed).

712. As accountable institutions, these DNFBPs are subject to the CDD and record keeping requirements of the FIC Act, the MLTFC Regulations, and Exemptions 2 and 3. See Section 3 of this report for a full description of the deficiencies which have been identified in relation to these aspects of the legislative framework. Additionally, the following sector-specific legal requirements and implementation issues should be noted.

713. Notaries are not a stand-alone profession in South Africa. Notaries are specially qualified attorneys who are also admitted as notaries and may therefore perform the functions of a notary. Therefore, the AML/CFT framework that applies to attorneys also applies to notaries. For the casino sector, it should also be noted that no gambling licences have been issued to ship-based casinos and it is illegal to operate (and therefore impossible to issue a licence to operate) an internet casino.[22] This means that no casinos in these forms are currently authorised to operate legally in South Africa. However, if the National Gambling Board were to issue a licence to a ship-based casino, then the provisions of the FIC Act would apply to it.

Applying Recommendation 5 (CDD)

Casinos (applying R.5)

714. The obligations of the FIC Act apply to casinos only in respect of the gambling activities that it offers and for which it is required to hold a gambling license issued by the provincial licensing authority (PLA). Any other activities that the casino may offer and which could be offered without the gambling licence (*e.g.* hotel, restaurant or entertainment services) are not covered (Exemption 12). This exemption is in line with FATF Recommendation 12.

715. As accountable institutions, casinos are required to perform CDD (identification and verification) in accordance with Sections 21 and 22 of the FIC Act in relation to all business arrangements with customers for the purpose of concluding transactions on a regular basis and every single transaction concluded with a customer in respect of gambling activities where:

- credit is given or chips are sold in excess of ZAR 25 000 (EUR 2 100);
- an amount in excess of ZAR 25 000 (EUR 2 100) is paid in exchange chips, or is received as a deposit for gaming, as repayment of credit, as a wager or for safekeeping;
- an amount in excess of ZAR 5 000 (EUR 430) is received as a wager where chips are customarily used for wagering; or
- cash, a cheque or other negotiable instrument or funds in excess of ZAR 25 000 (EUR 2 100) is exchanged for cash, a cheque or other negotiable instrument or funds which are to be transferred.

716. Transactions below these thresholds are fully exempted from CDD and associated record keeping (Exemption 13). These thresholds are in line with the thresholds for application which are prescribed by FATF Recommendation 12. Exemption 13 does not apply in the case of suspicious and unusual transactions (s.18 Exemptions). It should be noted that most casino business in South Africa is generated by walk-in customers (occasional customers who engage in recreational gambling) who gamble in amounts below ZAR 5 000 (EUR 430) per month, and in fact the norm is closer to ZAR 1 000 (EUR 86).

717. A concern is that, where CDD is required, casinos are permitted to apply reduced CDD in all cases. In particular, casinos are fully exempt from collecting and verifying the residential address and income tax registration number of natural persons (Exemption 14). The FATF Recommendations do permit simplified or reduced CDD to be applied in cases of low ML risk. However, no basis was provided (*e.g.* research, analysis or typologies) to justify all casino transactions as being treated low risk for ML/FT. On the contrary, although most casinos in South Africa do not engage in the gambling junket business, which is considered to be high risk, at least one casino does.

[22] Amendments to the National Gambling Act are currently pending which will allow internet casinos to be licenced in South Africa.

718. Also, in defining the scope of its application, Exemption 14 refers to all transactions which are "not subject to the exemption referred to in paragraph 11 of this Schedule". This cross-reference is incorrect; the exemption in paragraph 11 applies to estate agents. The South African authorities explained that the original draft referred to the transactions which are described in what is now Exemption 12. This drafting error does not seem to be causing confusion in the industry.

719. Implementing CDD requirements effectively poses unique challenges in the casino environment, particularly since it is often impractical to conduct CDD at the gaming tables during play. CDD can, however, be properly performed at the cash desk when chips are purchased and cashed out. In practice, some of the procedures being implemented to address these issues include: (a) not allowing customers to purchase chips or buy into play with a credit card at the gaming tables; (b) referring customers to the cash desk for CDD purposes if they attempt to bet cash (as opposed to chips) in an amount exceeding the ZAR 5 000 threshold or if their cumulative buying of chips exceeds ZAR 25,000; (c) installing only slot machines that pay out redemption cheques (rather than cash) which must be redeemed at the cash desk; (d) employing inspectors to monitor customers for suspicious or anomalous behaviour (*e.g.* movements from table to table with a view to exceeding the ZAR 25 000 threshold for the cumulative buying of chips); (e) requiring full CDD (ID and verification) when cashing out chips, including having the cash desk contact the gaming table to verify that the customer played there; (f) paying special attention to customers who are gambling large amounts of money; (g) ensuring that if someone buys in with a large amount of cash, the cash is stored separately so that the same bills may be returned to the customer upon cashing out; (h) not allowing chips purchased at one casino to be played in another; and (i) uploading the Gazetted list of persons designated pursuant to S/RES/1267(1999) to the casino's electronic transaction surveillance database so matches are automatically flagged. Almost all casinos are equipped with sophisticated customer monitoring and surveillance techniques which, although used primarily for the purpose of detecting cheaters, may also be leveraged for the purpose of ensuring that the casino is not being abused by money launderers or terrorist financiers.

720. CDD measures are easier to implement if the customer enters into a business relationship with the casino. For example, a common practice is to encourage customers to sign up for loyalty cards, which can be used for betting and redeeming rewards. Full CDD can be performed when the customer signs up for the loyalty card. Some loyalty cards include a photograph of the customer which can be checked by the dealer at a gaming table to ensure that the card user is also the subscriber. Additionally, some casinos offer cheque cashing facilities which allow the customer to cash in a cheque for more than the guaranteed amount. In practice, it is the issuing bank which extends the credit; the casino just uses the cheque as security. In such cases, the customer must be required to fill in an application form, provide an ID document, address and employment history.

721. The results of the NGB inspection process in the 12 months prior to the on-site visit show significant improvement in the industry's implementation of CDD requirements.

Accountants (applying R.5)

722. The CDD requirements of the FIC Act only apply to accountants when they are rendering investment advice or investment broking services (Schedule 1, s.12 FIC Act). This is not in line with Recommendation 12 which also requires accountants to be covered when preparing for or carrying out transactions for a client in relation to: buying and selling real estate or business entities; managing bank, savings or securities accounts; organising contributions for the creation, operation or management of companies; and creating, operating or managing legal persons or arrangements. Although, in the South African context, accountant are not involved in real estate transactions and trust asset management, they do engage in the other activities listed above.

723. Another problem is that the industry continues to struggle with the definition of "investment advice" in Schedule 1 of the FIC Act, and would welcome further clarification so as to better understand which members of the profession are considered to be accountable institutions.

Attorneys (applying R.5)

724. The CDD requirements of the FIC Act (s.21) apply to attorneys in respect of every business relationship or single transaction where the attorney:

- assists a client in planning or executing: the purchase or sale of real estate or a business undertaking; the opening or management of a bank, investment or securities account; the organisation of contributions necessary for the creation, operation or management of a company, close corporation or similar structure outside the Republic; the creation, operation or management of a company, close corporation or similar structure, or a trust (other than one established by a testamentary writing or court order) outside the Republic;

- assists a client in disposing of, transferring, receiving, retaining, maintaining control of or in any way managing any property;

- assists a client in managing any investment;

- represents a client in any financial or real estate transaction; or

- receives from a client deposits of ZAR 100 000 or more over a period of 12 months in respect of attorney's fees which may be incurred in the course of litigation.

725. Exemption 10(1) exempts attorneys from performing CDD in relation to all other services they perform. This exemption is not in line with Recommendation 12 which requires lawyers to perform CDD when organising contributions for, creating, operating or managing <u>any</u> legal person or arrangement. Exemption 10(1) allows such activities in relation to legal persons and arrangement within the Republic to be fully exempted from CDD. Exemption 10 is also problematic because it applies even in circumstances where the attorney is considering filing an STR (paragraph 18, Exemptions).

726. Another problem relates to interpretation of Exemption 10(1) in relation to real estate transactions. In practice, when an attorney receives an instruction in relation to a real estate transaction, the client is usually the seller, although it is the purchaser who pays the purchase price. Attorneys have taken the approach that their obligation is to conduct CDD on their client (usually the seller); however, the industry is of the view that the money laundering risk, in fact, lies with the purchaser. In this regard, the industry considers Exemption 10(1) not to be useful.

727. Attorneys are also grappling with how to apply Exemption 10(1) in practice to certain types of legal advice. For instance, if interpreted widely, providing advice to a company on a proposed merger could be interpreted in assisting the client in the management of the company.

Dealers in precious metals and stones (applying R.5)

728. Dealers in precious metals and stones are not accountable institutions and are, therefore, not subject to the CDD and record keeping requirements of the FIC Act. A review is currently underway to bring dealers in precious metals and stones within the full ambit of the FIC Act as accountable institutions.

729. The industry is, however, very committed to the Kimberly process, begun under the auspices of the United Nations, which seeks to improve transparency in the diamond trade. However, only those aspects of the Kimberley Process which have been incorporated into domestic legislation are enforceable. This means that only very limited customer identification requirements apply to a very small segment of the sector.

730. Licensed diamond producers, unpolished diamond dealers and diamond polishers must complete a Note of Purchase/Receipt in respect of Unpolished Diamonds, in the prescribed form, whenever receiving or purchasing an unpolished diamond (s.56 Diamonds Act). These same parties must keep a register, in the prescribed form, of all unpolished diamonds purchased, imported, received or disposed of (s.57 Diamonds Act). The customer identification information captured in this way is very limited. A Note records the names of the purchaser/recipient and the seller/supplier. This information is not independently verified; the purchaser and seller themselves certify the truth of it. A register records only the name and address of the person from whom the diamond was obtained or delivered to. Although the keeper of the register must sign a declaration that this information is true and correct, there are no specific requirements concerning how such names and addresses are to be verified. Both instruments collect limited transaction information (date and description of the goods).

731. Precious metal producers, gold dealers authorised by the National Treasury, and holders of licences to refine or beneficiate precious metals are required to keep a register of dealings in unwrought and semi-fabricated precious metals. The customer identification information captured in this way is also limited. A register contains only the names and addresses of the parties to the transaction. Although this information must be "true and correct", there are no specific requirements concerning how such information is to be verified (s.15 Precious Metals Act; s.33 Precious Metals Regulations). The register also contains limited transaction information (date and description of the goods).

732. Most aspects of Recommendation 5 are not covered and even these limited requirements only apply to a small part of the sector. Dealers in polished diamonds, other precious stones and refined precious metals are not subject to any CDD requirements.

Estate agents (applying R.5)

733. Estate agents may represent either the buyer or seller of property, and are required to conduct CDD on their customers. This is in line with the requirements of Recommendation 5. However, in practice, estate agents usually represent the seller (*i.e.* their customer). The purchaser is generally unrepresented by an estate agent and is not, therefore, subject to CDD requirements, unless the transaction is suspicious and the agent is considering filing an STR. However, the industry regulator (the EAAB) is of the view that the money laundering risk lies with the purchaser. The EAAB has raised this issue with the Centre.

734. Real estate agents are fully exempt from performing CDD when providing services related to property and rental management (Exemption 11). This is in line with the requirements of Recommendation 12.

735. The results of the EAAB inspection process show that, overall, implementation of AML/CFT measures, including CDD requirements, is low. A major issue is lack of awareness of the relevant obligations. For instance, estate agents used to be unaware of the 1267 list. The EAAB is focusing on AML/CFT awareness raising in the industry and notes that the situation is improving.

Trust and company service providers

736. Any person can act as a company service provider; such persons do not fall under the scope of the FIC Act if they are not an entity or person otherwise covered by the legislation. There are, in fact, some

specialised firms of professionals who provide the vast majority of company registrations. These firms may include lawyers and accountants but are not required to and also employ other professionals. Company services are also performed as a business feature by attorneys and accountants providing this as a service to their clients. As noted above, attorneys (whether they are part of a law firm or a specialised company service provider) are subject to CDD requirements to the extent that the legal person involved is outside of South Africa. Accountants are only subject to CDD requirements when they provide investment advice or brokering services, but there is currently an industry debate as to whether company management services would be considered to amount to investment advisory services.

737. Anyone who invests, keeps in safe custody, controls or administers trust property within the meaning of the Trust Property Control Act is subject to the CDD provisions of the FIC Act (s.21). However, these same persons are exempted from the CDD requirements when they are: preparing a testamentary writing; administering a deceased's estate as their executor; administering trust property as the trustee of a trust established by a testamentary writing or court order; or administering trust property as a trustee of a trust established to administer funds payable from an employees' benefit fund for the benefit of a nominated beneficiary or dependant of a deceased member of such an employee's benefit fund (Exemption 10(2)). This does not seem to be in line with the types of activities that should be covered under Recommendation 12.

Applying R.6 (PEPs)

738. There are no enforceable requirements extending any of the specific obligations under Recommendation 6 to any category of DNFBP.

Applying R.8 (Payment technologies and introduced business)

739. There are no enforceable requirements extending any of the specific obligations under Recommendation 8 to prevent the misuse of technological developments for the purpose of ML/FT. Those DNFBP which are accountable institutions pursuant to the FIC Act are, however, subject to MLTFC Regulation 18 which requires them to take reasonable steps to establish the existence, or establish and verify the identity of customers in the context of non-face-to-face dealings. However, this is a very general requirement, and no guidance (enforceable or otherwise) has been provided to DNFBPs to assist them in determining what might constitute "reasonable steps". The only guidance that exists in this area (Guidance Note 3) only applies to banks.

740. There is also a scope issue in that only DNFBP which are accountable institutions are subject to these requirements and not all of the designated activities of accountants, attorneys and TCSP are covered as is required by Recommendation 12. For more details about the scope issue, see above on the application of Recommendation 5 to the DNFBP sector.

Applying R.9 (Third parties and introduced business)

741. *Estate agents:* Property transactions effected in cash are common, particularly in the tourist-inclined areas of the Atlantic seaboard near Cape Town and the game areas. As well, there are no limits on foreign ownership of property; foreign natural and legal persons, and trusts can own property in South Africa. These characteristics make it particularly troubling that the full range of preventative measures required by Recommendation 9 do not apply to non-face-to-face transactions in the real estate sector (see Section 3.3 of the report for a detailed description of these deficiencies).

742. There is also a scope issue. For more details about the scope issue, see above on the application of Recommendation 5 to the DNFBP sector.

Applying R.10 (Record keeping)

743. The scope issue described above (see the application of Recommendation 5 to the DNFBP sector) also applies to record keeping requirements. Additionally, the following sector-specific legal requirements and implementation issues should be noted.

744. *Dealers:* As noted above, very limited customer identification requirements apply to the trade in unpolished diamonds and unwrought precious metals (see the above description of Recommendation 5 as applied to dealers in precious metals and stones). The limited information that is collected on Notes and registers must be kept for five years. Registers must be submitted annually to the South African Diamond and Precious Metals Regulator (ss.56-57 Diamonds Act; s.15 Precious Metals Act; s.33 Precious Metals Regulations).

745. *Estate agents:* All transactions relating to the purchase and sale of real estate must be recorded on the property deed which is registered electronically in one of South Africa's nine deeds offices. The property registry is maintained by the Department of Land Affairs.

Applying R.11 (Unusual transactions)

746. The scope issue described above (see the application of Recommendation 5 to the DNFBP sector) also applies to the requirement to pay special attention to unusual transactions.

4.1.2 Recommendations and Comments

747. South African authorities should most importantly expand the scope of the FIC Act to more broadly cover the requirements in R.5, 6, and 8-11 for DNFBPs as well as financial institutions. Authorities should also the broaden the scope of obligations for the various DNFBP sectors to enhance CDD obligations as follows:

- Casinos should not be exempt from collecting and verifying the residential address and income tax registration number of natural persons (Exemption 14), unless this can be justified on the basis of demonstrated low risk.

- Accountants should also be specifically covered when: buying and selling real estate or business entities; managing bank, savings or securities accounts; organising contributions for the creation, operation or management of companies; and creating, operating or managing legal persons or arrangements.

- Attorneys should be required to apply AML/CFT obligations in relation to company services when dealing with a South African company.

- Dealers in precious metals and stones should be made to be accountable institutions.

- Company service providers (other than lawyers or accountants) should be required to apply appropriate AML/CFT measures.

748. South African authorities should also consider the best ways to deal with the particular risks in the real estate sector relating to the non-face to face transactions, the use of cash, and obligations to identify the buyer of real property.

4.1.3 Compliance with Recommendation 12

	Rating	Summary of factors relevant to s.4.1 underlying overall rating
R.12	NC	• The deficiencies identified in R.5, 6, and 8-11 that apply in the financial sector also apply to all DNFBPs. • Scope issues further reduce the application of the requirements of R.5 and R.8-11 in that: accountants are not covered when conducting all of the activities prescribed in R.12 and the applicability of the requirements when providing investment advice is not clear to the industry; attorneys are not covered when performing company services in relation to legal persons and arrangements within South Africa; the majority of dealers in precious metals and stones sector are not covered and the others are only subject to limited CDD and record keeping requirements; and trust and company service providers (other than lawyers or accountants providing investment advice) are not covered in the situations specified in R.12. • Applying R.5: Casinos are permitted to apply reduced CDD in all cases, and this was not based on demonstrated low risk. In particular, casinos are fully exempt from collecting and verifying the residential address and income tax registration number of natural persons (Exemption 14). Exemption 10 for attorneys does not comply with the FATF Recommendations in that it fully exempts attorneys from all CDD requirements (as well as some or all record keeping requirements) even where there is a suspicion of ML/FT. • Applying R.9: The characteristics of the real estate market (often cash-based) make it troubling that the full range of preventative measures required by Recommendation 9 do not apply to non-face-to-face transactions in the real estate sector. • Applying R.10: (Dealers): Only very limited information on limited transactions is recorded. • Effectiveness: The results of the EAAB inspection process show that, overall, implementation of AML/CFT measures, including CDD requirements, is low among estate agents.

4.2 Suspicious transaction reporting (R.16)

(applying R.13 to 15 & 21)

4.2.1 Description and Analysis

Applying R.13 and SR.IV (STR Reporting)

749. All "businesses" and, therefore, all DNFBP are subject to the suspicious and usual transaction reporting obligations of the FIC Act. See Section 3.7 of this report (R.9 and SR IV) for a detailed discussion of these requirements and related deficiencies. No scope issues arise in relation to Recommendations13 and Special Recommendation IV as all businesses (not just accountable institutions) are covered. The following chart shows a breakdown of STR reporting in the DNFBP sector.

Type of DNFBP	Number of persons/entities reporting	2005/06	2006/07	2007/08	Total	Percent of reports received by the Centre
Casinos	25	75	173	809	1 057	2%
Estate agents	27	15	16	17	48	0.07%
Car dealers	61	767	2 363	1 129	4 259	6%
Legal entities	58	49	50	116	215	0.3%
Other	5	71	76	99	246	0.4%
TOTALS	**176**	**977**	**2 678**	**2 170**	**5 825**	**8.1%**

750. Also, one TPR was filed by a casino in 2007/08 and seven were filed by car dealers in 2006/07 (representing 2% and 13% of all TPRs received by the Centre respectively).

751. Additionally, the following sector-specific legal requirements and implementation issues should be noted in relation to the reporting obligations.

Casinos (applying R.13 and SR.IV)

752. The ability of casinos to detect suspicious activity is facilitated by the sophisticated surveillance and monitoring systems that are implemented in casinos, including on-line monitoring of transactions and physical surveillance of customer behaviour. Given the large amount of surveillance normally undertaken in a casino, it is not uncommon for the same suspicious incident to trigger several reports (so-called "founding reports") from different casino employees (*e.g.* the dealer, the pit supervisor, the pit inspector, the electronic surveillance room staff). In such cases, the casino's compliance officer consolidates the founding reports and files a single STR with the Centre. Some casinos have had problems with their electronic reporting systems, so fax is the preferred method of filing STRs.

753. The number of STRs being filed by casinos increased significantly in 2007/08. The industry attributes this to a re-evaluation of their reporting systems, following feedback that there was under-reporting. As a result, detections of counterfeit and dye-stained notes (which were previously only reported to the SAPS or relevant Provincial Licensing Authority) are now being reported as STRs. Vast numbers of STRs relate to such incidents and most casinos have implemented electronic note acceptors to detect fake or stained notes. Detection of even a single such note will trigger an STR and further surveillance on the customer. Other types of suspicion that are triggering STRs in the casino industry are: the customer asking questions about internal controls; large buy-ins; cashing in an overly short time after buying chips; and, in a few cases, persons coming in with bags of cash. Better training has also improved implementation of the reporting obligation in this sector.

Accountants (applying R.13 and SR.IV)

754. Accountants who are auditors registered with the IRBA are under a general obligation to report STRs directly to the Centre as required by Section 29 of the FIC Act.

Attorneys (applying R.13 and SR.IV)

755. The industry is still debating how to interpret legal privilege in the context of meeting the reporting obligations pursuant to the FIC Act. The LSSA and PLA regularly receive inquiries from attorneys on this issue (about 15 to 20 calls per month). The LSSA would welcome further clarity from the Centre on this issue. In practice, attorneys seem to be interpreting the obligation to report very widely and, when in doubt, are generally erring on the side of caution and reporting the transaction. Although the LSSA and PLA do not receive copies of STRs, their sense is that most of the STRs being filed by the industry relate to property transactions being effected in cash. The risk of such transactions is widely understood.

Dealers in precious metals and stones (applying R.13 and SR.IV)

756. To date, only two STRs have been filed by dealers in precious metals and stones. The reporting requirements apply to all transactions performed through dealers ("businesses" pursuant to the FIC Act). This goes further than Recommendation 16 which, for this sector, only requires the reporting of suspicious cash transactions equal to or exceeding EUR 15 000. The industry view is that cash transactions above this threshold are uncommon and only likely to occur in the context of retail sales and manufacture to the public. A six-month industry survey of 200 retail stores (one large national chain store, some mid-size

stores and very small stores) showed about 120,000 cash transactions over six months, only two of which exceeded ZAR 50 000 (EUR 4 200). Both transactions were below ZAR 100 000 (EUR 8 400) and occurred in high-end jewellery stores. For most retailers, 90% of transactions are conducted by credit card. Only about 20-25% of retailers' revenue comes from cash transactions, most of which are small.

Estate agents (applying R.13 and SR.IV)

757. Although property transactions in some areas are often effected in cash, until recently, it was not widely recognised that this is suspicious activity that should be reported. The EAAB has been working to raise more awareness on this issue, including warning estate agents about the risk of receiving cash in their trust accounts without reason. Another frequent impediment to effective implementation is concerns by estate agents that they could face reprisals from the customer if they file an STR. The EAAB has been working to reassure estate agents that the process is confidential and other parties involved in the same transaction (*e.g.* the lawyers and banks involved) are subject to the same obligation to report.

758. To date, estate agents have filed 48 STRs. However, the EAAB has detected some unreported activity, especially in the Western Cape Province, which is suspected of relating to ML. The EAAB is working with the Centre on this issue, and has asked for statistics concerning the number of STRs being filed by the industry and the provincial spread, so that it can focus its inspections on the provinces where there is the most risk. The EAAB is not aware of any suspected terrorist financing through the real estate sector.

Applying R.14 (Tipping off)

759. The legal protections and tipping off provisions of the FIC Act are fully compliant with Recommendation 14 (see Section 3.7 of this report for details). Additionally, the following sector-specific implementation issue should be noted.

760. *Casinos:* Filing an STR without tipping off the customer can be challenging in the casino environment, particularly if it is a dealer who becomes suspicious during the course of play. However, this risk is mitigated in practice by implementing irregular patterns of shift changes of dealers. This allows a dealer to be relieved for the purpose of filling out a founding statement, without arousing suspicion.

Applying R.15 (Internal controls)

761. DNFBPs that are accountable institutions are required to implement internal controls pursuant to Sections 42 and 43 of the FIC Act and MLTFC Regulations 26 and 27. See Section 3.8 of this report for a detailed discussion of these requirements and their related deficiencies.

762. The scope issue described above (see the application of Recommendation 5 to the DNFBP sector) also applies to the requirement to implement internal controls. Additionally, the following sector-specific legal requirements and implementation issues should be noted.

Casinos (applying R.15)

763. When the FIC Act was first introduced, the industry association (the Casino Association) developed a set of generic internal control rules for casinos. These were problematic because they did not take into account specific risks associated with each casino's location, customer base (ratio of walk-in customers to loyalty club members) and types of gaming services offered. As the industry has moved towards a risk-based approach, internal rules have become more customised to address the specific risks associated with a particular casino. A committee of the voluntary Casino Association endorses each casino's internal control which must also be submitted to the NGB and the Centre for approval. The NGB

requires casinos to submit, on an annual basis, updated internal control rules and training manuals, a list of trained staff, and reconsideration of the lead time during which staff may be exposed to customers before being trained in AML/CFT.

764. About 12 months prior to the on-site visit, the NGB detected problems with casino staff being exposed to customers before having undergone AML/CFT training. Since then, implementation has significantly improved, with many casinos giving training priority to staff who have gaming interaction with the customer (as opposed to the food, beverage or hotel staff).

765. All casinos in South Africa have designated compliance officers who are independent of the line function of the casino. The larger casinos have dedicated compliance officers. In the smaller casinos, the compliance officer is the casino surveillance officer, *i.e.* the manager of the "eye" (surveillance room).

766. All provincial gaming legislation imposes screening requirements on key and other employees, including dealers and other gaming staff. These include background, criminal record and solvency checks (s.49(1) National Gambling Act).

Applying R.21 (Internal controls)

767. There are no specific requirements for DNFBP to give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations. See Section 3.6 of this report for more details.

Additional elements

768. Auditors (as businesses) are required to report suspicious or unusual transactions where they have received or are about to receive proceeds or terrorist-related funds, are party to a transaction likely to facilitate ML/FT, or are about to be used for ML/FT. However, when conducting an audit, the auditor is not involved with or a party to the transaction, or otherwise being used for ML/FT purposes. So the reporting obligation would not apply in those circumstances.

769. DNFBP are required to report to the Centre when they suspect or have reasonable grounds to suspect that funds are the proceeds of any criminal act that would constitute a predicate offence for money laundering domestically.

4.2.2 Recommendations and Comments

770. The obligations to report activity suspected of being related to money laundering or terrorist financing, protection for reporting and the prohibition on tipping off apply to all DNFBPs. In general, compliance in reporting has been improving; however, South African authorities should work with the dealers in precious metals and stones sector and real estate sectors to determine whether they are adequately identifying and reporting suspicious activity. The Centre should also work with the legal profession to further clarify the issue of how legal privilege applies in the context of reporting. Authorities should also strengthen the requirements relating to R.15 and R.21 in relation to all DNFBPs.

4.2.3 Compliance with Recommendation 16

	Rating	Summary of factors relevant to s.4.2 underlying overall rating
R.16	PC	• Applying R.13 and SR.IV: • Effectiveness: Implementation of the reporting obligation is negatively affected as follows: 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; for dealers, there has been very low rates of reporting in contrast to the relative importance of the sector in the South African context; and for estate agents, until recently it was not widely recognised that property transactions effected in cash are suspicious. Additionally, the EAAB has detected some activity in the estate agent sector which should have been reported (but was not) and which is suspected of relating to ML. • Applying R.15 and R.21: The deficiencies identified in R.15 that apply in the financial sector also apply to all DNFBPs.

4.3 Regulation, supervision and monitoring (R.24-25)

4.3.1 Description and Analysis

Recommendation 24

771. The Centre is responsible for monitoring and giving guidance to accountable institutions (including DNFBP), supervisory bodies and other persons regarding the performance by them of the duties and compliance with the provisions of the FIC Act (s.4). It does not, however, have official supervisory functions or powers.

772. The following supervisory bodies are designated as being responsible for supervising DNFBP which are accountable institutions for compliance with the FIC Act:

- the Estate Agency Affairs Board (EAAB);
- the Public Accountants and Auditors Board (PAAB) (now the Independent Regulatory Board for Auditors (IRBA));
- the National Gambling Board (NGB); and
- the Law Society of South Africa (LSSA) (s.45 and Schedule 2 FIC Act) (collectively referred to as Designated Supervisors).

773. As the Centre has no inspection powers of its own, Designated Supervisors who wish to have Centre participation must use their general powers to appoint employees of the Centre to the inspection team. In this way, the Centre has been able to participate jointly with the NGB in 25 inspections of casinos (October 2007 to April 2008) and with the EAAB in 21 inspections of estate agents (November 2006 to June 2007).

774. As noted above, the FIC Act currently only provides for enforcement of its provisions through criminal sanctions. Administrative sanctions will not be available under the FIC Act until the Amendment Bill comes into force. See Section 3.10 of this report for more details.

775. In some cases, these designations exacerbate the overarching scope issue that only DNFBP which are accountable institutions are subject to monitoring and supervision for compliance with AML/CFT

requirements, and appropriate sanctions. For more details about the overarching scope issue, see above on the application of Recommendation 5 to the DNFBP sector. In particular, the designations of the NGB, IRBA and LSSA are problematic.

776. *National Gambling Board (NGB):* Although the NGB is the designated AML/CFT supervisor for casinos, it has no specific inspection authority or enforcement power to do so. Instead, inspection and enforcement powers, including specifically for the purpose of ensuring compliance with the FIC Act, lies with the nine provincial licensing authorities (PLA) (s.31(1)(b) and (e) National Gambling Act (NG Act)). Nevertheless, the NGB has been conducting AML/CFT inspections of casinos, in co-ordination with the Centre and the PLAs. As the basis for its authority to do so, the NGB points to: (a) its designation under the FIC Act; (b) its power under s.33 of the NG Act to monitor and supervise the PLAs to ensure that they act in accordance with standards established by the NGA, including when issuing gambling licences; and (c) the joint national/provincial competence over gambling in the Constitution. Although the NGB's power to conduct such inspections has never been challenged, on its face, the NGB's inspection authority is focused on monitoring, supervision and evaluation of the PLAs, not the casinos themselves.

777. *Public Accountants and Auditors Board (PAAB):* The Independent Regulatory Board for Auditors (IRBA) (formerly the PAAB) is the designated AML/CFT supervisor for auditors. The problem is that the IRBA only has jurisdiction to supervise auditors. Of the approximately 25 000 chartered accountants in South Africa, only 4 500 are auditors and a further 1 500 are attest accountants. Therefore, even if the IRBA had clear authority to supervise auditors for compliance with the FIC Act, its supervision would only extend to a relatively small number of accountants. This gap may be somewhat ameliorated by the fact that anyone who provides investment advice or investment brokering services also falls under the supervisory jurisdiction of the FSB (another designated supervisor under the FIC Act). However, the FSB would have no supervisory jurisdiction over the other activities of accountants which should also be covered pursuant to the FATF Recommendations.

778. *Law Society of South Africa (LSSA):* Although the LSSA is the designated AML/CFT supervisor for attorneys, it has no specific inspection authority or enforcement power to do so. Instead, it is the four regional law societies (RLS) which have statutory powers to supervise the conduct of attorneys (s.56 Attorneys Act). This situation has stalled implementation of AML/CFT requirements in the legal profession. The Centre has embarked on a process to amend Schedule 2 to the FIC Act and to replace the reference to the LSSA with references to the four RLS. However, it should also be noted that the FIC Act designates both non-practising and practising attorneys as accountable institutions; however, the RLS only regulates independent lawyers (not in-house counsel who are classified as non-practising).

779. Additionally, the following sector-specific legal requirements and implementation issues should be noted in relation to the supervisory framework for DNFBP.

Casinos

780. The National Gambling Board (NGB) was established in terms of the National Gambling Act, 1996, which was repealed and replaced by the National Gambling Act, 2004 (NG Act). The NG Act is national legislation that promotes uniform norms and standards, and provides for the co-ordination of concurrent national and provincial legislative competence in relation to the oversight of gambling activities throughout South Africa. Each province has adopted its own gambling legislation to give effect to the broad guidelines of the national legislation in the province. There are nine provincial licensing authorities (PLA), one in each of the nine provinces, which are responsible for issuing gambling licenses and supervising the casinos within their respective jurisdictions.

781. Casinos are subject to rigorous licensing requirements. Fit and proper tests are conducted on all owners and key employees. This process includes checking backgrounds, criminal records, solvency and regulatory histories, and seeking relevant information from foreign counterparts where appropriate. An adverse licensing decision may be made on the basis of another jurisdiction's report. The PLA are also specifically authorised to make use of reports submitted by other regulatory authorities, the Centre, the National Director of Public Prosecutions and the SAPS.

782. Compliance with the FIC Act is a condition of every national (but not provincial) gambling licence (s.37 NG Act). Failure to do so may result in suspension or revocation of the licence (s.43 NG Act). Licenses (even 10-year or perpetual licences) must be renewed annually. Renewal is not automatic; the licence will not be renewed if gross violations of the licensing conditions are detected. Changes to the ownership of a casino during the course of a license trigger an investigation which could extend to the entire structure of the casino.

783. NGB and the Centre jointly conducted 33 thematic AML inspections in 2006/2007 and 23 in 2007/2008. In the medium term, the Centre intends to continue participating in the joint inspection process with a view to building capacity, although the NGB has conducted some inspections alone when the Centre has been unable to participate. The PLA are also invited to join these inspections and it has become more common for them to participate. Inspection teams are usually comprised of one NGB inspector, one or two Centre inspectors, and one or two PLA inspectors (if they join). In general, the industry views the AML inspection process and the Centre's participation favourably, but welcome the forthcoming amendments to the FIC Act which will designate the PLA as the relevant supervisory body. If the PLA are designated, consideration needs to be given as to whether they have sufficient resources to meet their new supervisory and enforcement obligations.

784. Each casino undergoes an annual AML/CFT inspection which last about four to five hours. The inspection focuses on assessing compliance with the CDD, recordkeeping, STR reporting and internal control requirements of the FIC Act, POCDATARA and S/RES/1267(1267). The inspectors are provided access to the casino's CDD, transaction records, updated training schedules of the FIC Act training conducted and an updated set of risk-based approach internal rules, and will conduct random testing and file reviews to confirm whether CDD procedures were followed. Interviews and integrity testing of management and front-line staff are conducted. To facilitate the process, the NGB has developed an AML-specific spreadsheet checklist that can be transposed into the final inspection report. Final reports are routinely forwarded to the relevant PLA even if the PLA had not joined the inspection team.

785. NGB's authority to monitor and sanction casinos is contained in Section 37 of the National Gambling Act, which makes it a condition of every national licence that the licensee must comply with every applicable provision of the National Gambling Act, the FIC Act, and applicable provincial law. Sections 82(2) and (3) of the Act also provide for criminal penalties for violations of the Act.

786. The results of the inspection process show a high level of compliance with AML/CFT measures in the casino sector. Although some differences of interpretation remain, the industry has a better understanding overall of the requirements than it did a few years ago. The PLAs are also authorised to apply criminal sanctions for violations of the NG Act (fines up to ZAR 10 million or 10 years in jail) and administrative sanctions for violations of licensing conditions (fines not exceeding 10% of the annual turnover of the casino's licence) (s.83 NG Act). The NGB has issued twenty-five correction letters issued. All casinos provided with such a letter are taking corrective steps, and no further action has been taken.

787. The NGB is also taking steps, in co-ordination with the NPA and Commercial Crime Unit, to prevent internet gambling which currently exists illegally in South Africa. Through its investigations, the NGB has determined that some illegal internet gambling operators are South African. The NGB has sent

written complaints to jurisdictions that are facilitating this practice, although this effort has not generated results.

Accountants

788. The Independent Regulatory Board for Auditors (IRBA) is the statutory regulator for the auditing profession and is responsible for accrediting auditing firms. IRBA members are required to pass the IRBA exams to become an auditor. Auditors are required to follow the IRBA Code of Ethics.

789. The IRBA has circulated a questionnaire to all of its members with a view to determining which firms are accountable institutions pursuant to the FIC Act. On the basis of the questionnaire, the IRBA began conducting AML inspections of the largest firms, as a component of its normal practice reviews which, among other things, check for compliance with auditing standards. The IRBA has jurisdiction to inspect anyone employed by an auditing firm, including accountants who give investment advice, but do no auditing work (so-called "non-attest" accountants). The IRBA's AML inspections cover a firm's internal controls, and systems for STR reporting and record keeping. The IRBA has not yet begun reviewing for compliance with Special Recommendation III. An inspection by the Centre lasts about five days, depending on how involved the firm is in giving investment advice. Inspections are conducted by teams of two IRBA inspectors. The IRBA has not conducted any joint inspections with the Centre. The IRBA, in co-operation with the Centre, is developing inspection criteria and procedures specific to AML/CFT inspections. A database containing information about members' FIC Act compliance history has also been established. Following an inspection, the firm is provided with a formal report. No follow-up visits have yet occurred; they are scheduled to commence in 2009. It should also be noted that auditors providing investment advice, also fall under the supervisory jurisdiction of the FSB. As there is no co-ordination between FSB and IRBA inspections, there is the possibility of overlap in this regard.

790. The results of the inspection process show that firms generally have AML/CFT policies and processes in place, but lack sufficient training to implement them effectively. Employee training, which commenced in the industry in 2003, has not been renewed annually. Other problems detected include compliance officers appointed at an overly junior level.

791. The IRBA indicates that it is able to sanction violations of the FIC Act (*e.g.* persistent patterns of CDD or STR reporting violations) in the same way as it can sanction non-compliance with auditing standards and any other applicable laws or regulations. However, it is not clear what the legal basis is for doing so and, to date, no specific action for AML/CFT breaches has been taken. The forthcoming amendments to the FIC Act will clarify the supervisory of the IRBA and provide it with related supervisory and enforcement powers. At that time, consideration will needed to whether the IRBA has sufficient resources to meet its new supervisory and enforcement obligations.

Attorneys

792. The LSSA is the umbrella organisation for attorneys which fulfils mainly an education role for the profession. As it has no supervisory powers, the LSSA has not conducted any inspections for compliance with AML/CFT requirements. The four Regional Law Societies (RLS), which do have supervisory powers over the profession, have taken the view that attorneys, as custodians of the law, should comply with the FIC Act and, on that basis, may be disciplined for failing to do.

793. The High Court admits persons to the practice of law on the basis of an application by a suitably qualified person who meets the criteria for admission (s.15 Attorneys Act). The person must: complete law school and a two-year articling period; pass board, ethics and accounting exams; undergo an interview by a senior member of the bar; undergo criminal conviction and solvency checks; and satisfy the applicable

RLS that he/she is a "fit and proper" person to be admitted and enrolled (s.16 Attorneys Act). The RLS issue attorneys with a certificate of good standing on an annual basis. Once admitted to the bar, attorneys are required to submit an independent auditor's report annually for the purpose of ensuring that the accounting rules are being complied with.

794. The RLS have monitoring units that proactively try to identify irregularities in an attorney's practice, with a view to ensuring whether the attorney is compliant with the relevant code of conduct. If an irregularity is detected or otherwise comes to the attention of an RLS, or if an annual auditor's statement is qualified, the RLS may inspect the attorney's practice. Where it is alleged that an attorney acted unprofessionally or engaged in dishonourable or unworthy conduct, the RLS can institute an inquiry (s.71 Attorneys Act). During an inquiry, the RLS may inspect the attorney's records and premises, compel production of relevant documents and summon persons to appear (s.70 Attorneys Act).

795. Currently, the RLS are not routinely checking for compliance with the FIC Act. For instance, although the RLS have an expectation that attorneys will check their clients against the UN terrorist lists, most inspections are focused on an attorney's trust accounting obligations, and do not focus AML/CFT. Nevertheless, some instances of non-compliance with the FIC Act have been detected, although this was in the context of finding irregularities related to trust accounting requirements. These inspection results are shared generically with the LSSA.

796. The RLS do not have specific powers to impose sanctions in accordance with the FIC Act. Consequently, in cases where breaches of the FIC Act have been detected, the corresponding sanctions were based on the relevant trust accounting provisions. The RLS are specifically empowered to impose sanctions against attorneys for breaches of the applicable code of conduct. These sanctions range from a fine to making an application to the High Court to have the attorney barred from practice. An attorney who committed a criminal offence, may be disbarred and/or the matter referred to the SAPS or NPA for investigation and prosecution. Overall, there is consistency in how the RLS approach disciplinary action.

797. The Centre has expressed willingness to join RLS inspections; however, if the RLS become designated supervisors pursuant to the FIC Act amendments, they will need to substantially increase their resources to meet their new supervisory and enforcement obligations.

Dealers in precious metals and stones

798. The South African Diamond and Precious Metals Regulator (DPM Regulator) is responsible for issuing licenses ensuring compliance with the Kimberley Process Certification Scheme (ss.3 and 4 Diamonds Act), the Diamonds Act and the Precious Metals Act (PM Act). Additionally, a number of industry associations are active in promoting the implementation of the Kimberley Process and AML/CFT measures in the sector, developing codes of conduct and best practices for their members. However, the industry as a whole is not covered as membership in these organisations is voluntary. The Diamond and Jewellery Federation of South Africa (DJFSA) is an umbrella organisation under which the following bodies fall: the Jewellery Council of South Africa (JCSA) comprised of mining houses, manufacturers, wholesalers, retailers (small, medium and large); and the Diamond Council of South Africa (DCSA) comprised of buyers and sellers of rough diamonds (60% of the total industry), and cutters and polishers of diamonds (56% of the total industry). It is a major vulnerability is that there is no industry-wide supervisory body to ensure compliance with the relevant provisions of the FIC Act. The industry associations would welcome the establishment of such a body.

799. The diamond trade in South Africa is highly regulated, controlled and supervised from the point of production until the point where the diamond is polished. Producers and dealers may only sell unpolished diamonds on approved premises. No licensee shall receive or purchase any unpolished diamond

from any person not lawfully in possession of it (s.55 Diamonds Act). To lawfully possess an unpolished diamond, a person must be: an authorised producer (s.1 Mineral and Petroleum Resources Development Act); a licensee or permit holder pursuant to the Diamonds Act; implementing a written agreement with an authorised producer, licensee or permit holder; or otherwise be in lawful possession of the diamond (s.18 Diamonds Act). The DPM Regulator enforces strict licensing requirements, which include fit and proper tests, for dealers (buyers, sellers, importers or exporters), beneficiators (diamond polishers), temporary diamond buyers (who are not otherwise licensed to buy unpolished diamonds from a diamond exchange and export centre) and diamond trading houses (facilitators of the buying and selling of unpolished diamonds). Certificates and permits must also be obtained to possess, sell, export or import unpolished diamonds (s.26 Diamonds Act). A licence can be revoked if the licensee is rendered no longer "suitable" (*e.g.* following a criminal conviction).

800. Likewise, the precious metals trade (including gold and platinum) is also highly regulated, controlled and supervised from the point of production until the point where the metal is finished precious metal products. The DPM Regulator enforces similar licensing requirements and fit and proper tests on refiners, beneficiators and jewellers (which deal semi-fabricated precious metals, including changing their form and adding value to them) (ss.7-9 Precious Metals Act; ss.3, 7, 11, 21 and 22 Precious Metals Regulations).

801. The DPM has extensive powers to compel the production of documents and conduct inspections of any premises or vessel in which activity concerning unpolished diamonds takes place or where there are reasonable grounds to suspect that an offence has taken place (s.81 Diamonds Act). The DPM has more limited powers pursuant to the Precious Metals Act; although the DPM or SAPS can compel the production of a register upon request, only the SAPS has powers of inspection, search and seizure (ss.15 and 16 Precious Metals Act). In the case of both the unpolished diamonds and precious metals trade, the DPM regularly conducts spot checks to ensure that transaction registers are being kept up to date.

802. For unpolished diamonds, failure to keep proper Notes or registers is an offence under the Diamonds Act punishable a fine not exceeding ZAR 25 000 and/or up to 12 months imprisonment. Unlawful possession of an unpolished diamond is punishable by a fine not exceeding ZAR 250 000 and/or up to ten years imprisonment (s.87 Diamonds Act). For unwrought precious metals, failure to keep a proper register is an offence pursuant to the Precious Metal Act is punishable by a fine not exceeding ZAR 500 000 and/or imprisonment for up to 10 years.

803. There is no comparable supervisory framework for dealers in polished diamonds, wrought (refined) precious metals and other precious stones. No licensing requirements apply to dealers (wholesale or retail) in polished diamonds, other precious stones or jewellery. It is a particularly significant gap that there is no supervision or monitoring of wholesale or retail dealers in polished stones or jewellery (of which there are an estimated 3 000 to 4 000) for AML/CFT purposes. Feedback from awareness raising campaigns conducted by the industry associations illustrates that awareness of AML/CFT issues varies among small retailers (not well informed), wholesalers (reasonably well informed) and larger retail chains (quite well informed).

804. The polished diamond dealers who are members of the Diamond Dealers Club of South Africa have been exposed to training and guidelines on the AML/CFT issues. Complementary detailed communication on the FATF guidelines and recommendations for dealers has been communicated to members. The vulnerability remains with those dealers who are not members, and one effective way to mitigate the vulnerability is through having an industry supervisory body that would monitor compliance and enforce codes of conduct and ethics for the industry members.

805. It should be noted that the jewellery manufacturing industry in South Africa is very small, and a negligible quantity of cash transactions take place above the amount of ZAR 50 000, reducing the risk environment for money laundering and terrorist financing.

Estate agents

806. The Estate Agency Affairs Board (EAAB) is the statutory regulator for all estate agents in South Africa. The EAAB was established as a juristic person by the Estate Agency Affairs Act (EAA Act) to regulate and control certain activities of the estate agents in the public interest and for incidental matters. According to the registration office of the EAAB, there are 96 504 registered estate agents.

807. Estate agents are required to be licensed (certified) by the EAAB in terms of the EAA Act and be issued with a valid fidelity fund certificate (ss.16 and 26). To qualify as an estate agent, applicants must undergo training, pass a board exam and an articling period, and establish that they have not be convicted of an honesty crime, are not insolvent and are able to pay the registration fees (s.27). These latter requirements must be re-established annually every time the full estate agent status is renewed. The EAAB has agreements with SAPS concerning access to information concerning convictions and, if appropriate, the EAAB can block a person from the system to prevent their becoming an estate agent. Where information is received (either from the SAPS or another person) about a licensed agent being convicted of a crime or being otherwise inappropriate, the licence can be withdrawn immediately.

808. About ten percent of lawyers in South Africa are also real estate conveyancers, and are almost exclusively responsible for the registration of mortgage bonds. To qualify for practice as a conveyancer, the person must be an attorney or notary, undertake special training and pass relevant examinations.

809. Except in the case of attorneys, the EAAB board inspectors have extensive powers to enter premises, inspect documents and generally make such enquiries as are necessary to determine whether the provisions of the EAA Act are being complied with (s.32A EAA Act). Failure to co-operate with an inspector in the performance of his/her lawful duties is an offence. Since 2006, the EAAB and the Centre have jointly inspected 23 estate agents for compliance with the FIC Act. Each team consisted of two members of the EAAB legal department who focused on compliance with the EAA Act and two members of the Centre who focused on compliance with the FIC Act. From now on, there will be no joint inspections. The EAAB will be establishing its own inspectorate division. However, the EAAB considers that the joint inspection process was useful in that it educated the EAAB on how to inspect for compliance with the FIC Act and facilitated the development of a related inspection methodology which contemplates routine sample CDD and transaction testing.

810. In its first AML inspection cycle, the EAAB focused on the 17 biggest firms in all provinces. Each inspection lasted one to two days, depending on the size of the firm. The results of that inspection cycle showed an overall low level of compliance. After a period of time to allow for corrective action to be taken, these firms were re-inspected. The results of the second inspection cycle showed significant improvement. Overall, however, compliance in the real estate sector is very low, irrespective of the location or size or the firm (although those firms that were subject to follow-up inspections showed significant improvement). In its next round of inspections (which began just after the on-site visit), the EAAB will focus on medium or smaller firms which have not yet been inspected for AML/CFT compliance. The inspection schedule is being developed using a risk based approach. Firms are selected for inspection on the basis of: public opinion that the firm is not being run properly; excessive numbers of complaints concerning the firm; pending charges; and tips from other firms concerning improper management. By the end of the second round, about 19 000 firms will have been inspected.

811. Although the EAAB has the authority to sanction for violations of the EAA Act (s.34), it does not have power to sanction for violations of the FIC Act. Consequently, although the EAAB has detected breaches (some of them serious), it has only been able to take specific action in relation to breaches of the real estate requirements. In this way, the EAAB was able to close a firm in Pretoria which had many breaches of the real estate and AML requirements. The EAAB welcomes the forthcoming amendments to the FIC Act which will give it comprehensive powers to sanction for violations of the FIC Act. Resources have already been allocated to support the new inspectorate division.

Trust and company service providers

812. For company service providers, the supervisory framework described above in relation to attorneys applies only when they are providing services for companies outside of South Africa. Although accountants may be involved in the creation or management of companies, they are not subject to the provisions of the FIC Act or any related supervision when conducting such business. Other persons providing company services do not have to meet any particular qualifications or requirements and, are not subject to any AML/CFT supervision.

813. For trust services, the providers are generally attorneys and banks. However, the supervisory framework described above in relation to attorneys applies only when they are providing services for trusts outside of South Africa. For banks, the supervisory framework described in Section 3.10 of this report applies.

Recommendation 25 (Guidance for DNFBPs other than guidance on STRs)

814. Guidance Notes 1 and 4 issued by the Centre, on CDD and STR reporting respectively, apply DNFBP that are accountable institutions (see Sections 3.2 and 3.7 of this report for more details).

815. *Casinos:* The NGB and the Centre are in the process of developing sector-specific guidance for casinos, in consultation with the private sector. It is expected that this guidance will be published in the fall of 2009. The industry welcomes this initiative, particularly if it helps to resolve outstanding interpretation issues.

816. *Accountants:* The PAAB issued a guide on Money Laundering Control for Auditors in June 2003 (before the IRBA was established). The guide provides general guidance to registered auditors on the requirements of the FIC Act. Workshops and seminars were presented throughout the country just after June 2003, when most of the provisions of the FIC Act became effective.

817. *Attorneys:* The LSSA issued a manual for the attorneys which may be used as a basis for developing internal control rules and policies for compliance with the obligations of the FIC Act. Additionally, the Centre has assisted the LSSA in providing extensive AML/CFT education to the profession (the LEAD initiative).

818. *Dealers in precious metals and stones:* The industry associations have conducted extensive awareness raising throughout the sector. Such initiatives include: issuing circulars and awareness campaign flyers; road shows; seminars and regional meetings in key areas of the country. However, formal guidance has not been issued.

819. *Estate agents:* The EAAB and the Centre have conducted joint training sessions for estate agents on their AML/CFT obligations. The EAAB has also published an AML manual, holds free seminars on AML and, from 15 July 2008, imposed new educational requirements relating to AML for which attendance is mandatory. Additionally, the EAAB is in the process of developing sector-specific guidance on AML.

4.3.2 Recommendations and Comments

820. South Africa should bring into effect as soon as possible provisions that will provide adequate authority for the DNFBP supervisors/monitoring bodies to inspect for and apply a range of sanctions that is effective, proportionate, and dissuasive for non-compliance with the FIC Act. A comprehensive AML/CFT monitoring regime needs to be developed for dealers in precious metals and dealers in precious stones. South Africa should also address the scope issues identified under R.12 to ensure that the full range of DNFBPs have comprehensive AML/CFT obligations and supervision or monitoring.

821. If the Provincial Licensing Authorities are designated as AML/CFT supervisors for casinos, consideration needs to be given as to whether they have sufficient resources to meet their new supervisory and enforcement obligations. If the regional law societies become designated supervisors of attorneys, they will need to substantially increase their resources to meet their new supervisory and enforcement obligations.

822. Comprehensive AML/CFT guidance should also be issued for casinos and dealers in precious metals and dealers in precious stones.

4.3.3 Compliance with Recommendations 24 & 25 (criteria 25.1, DNFBP)

	Rating	Summary of factors relevant to s.4.3 underlying overall rating
R.24	PC	• The FIC Act currently only provides for enforcement of its provisions through criminal sanctions, none of which have yet been applied. Administrative sanctions will not be available under the FIC Act until the Amendment Bill comes into force. • The designations of the NGB, IRBA and LSSA as supervisory bodies are problematic. • The FIC Act-designated supervisory authorities for casinos (National Gambling Board), attorneys (Law Society of South Africa), and estate agents (Estate Agency Affairs Board) do not have specific authority to inspect for compliance or apply sanctions in respect to the FIC Act. • ***Dealers in precious metals and stones***: It is a major vulnerability is that there is no industry-wide supervisory body to ensure compliance with the FIC Act. • ***Company service providers:*** Only company service providers that are lawyers or accountants have a designated AML/CFT supervisor and the existing framework in relation to attorneys applies only when they are providing services for companies outside of South Africa. • ***Casinos:*** None of the provincial licensing authorities (PLAs) has yet been required or requested to exercise its authority to apply sanctions for violations of the FIC Act requirements. • ***Attorneys:*** Currently, the regional law societies (RLS) are not routinely checking for compliance with the FIC Act, and they do not have specific powers to impose sanctions in accordance with the FIC Act. • ***Accountants:*** The IRBA does not have clear authority to supervise auditors beyond ensuring their compliance with the AP Act, and its supervision would only extend to a relatively small number of accountants. • Auditors providing investment advice, also fall under the supervisory jurisdiction of the FSB. As there is no co-ordination between FSB and IRBA inspections, there is the possibility of overlap in this regard. • ***Trust service providers:*** The providers are generally attorneys and banks. However, the supervisory framework described above in relation to attorneys applies only when they are providing services for trusts outside of South Africa. For banks, the supervisory framework and identified deficiencies described in Section 3.10 of this report apply.

	Rating	Summary of factors relevant to s.4.3 underlying overall rating
R.25	PC	• AML/CFT guidance, although developed by the Centre in consultation with the NGB and casino industry, has not been issued for casinos (or dealers in precious metals and stones, or trust and company service providers that are not attorneys or accountants, although these sectors are not subject to national AML/CFT requirements).

4.4 Other non-financial businesses and professions

Modern secure transaction techniques (R.20)

4.4.1 Description and Analysis

823. The FIC Act requirements on CDD, record keeping and internal controls apply a number of non-financial businesses and professions that have not been designated by the FATF as DNFBPs, including limited payout machine route operators, bingo operators, book makers and totalisators (pari-mutuel) operators. Additionally, the STR reporting obligation extends to all businesses (regardless of type), their managers and employees. AML/CFT inspections have are already being undertaken in relation to totalisators and book makers. A review process is currently underway with a view to expanding the list of accountable institutions in an effort to broaden the scope of the FIC Act.

824. South Africa has adopted an expressed policy to increase access by the general population to financial services. This entails, among others, formal undertakings on a collective basis by financial institutions such as the banking sector and insurance sector to extend the provision of their products and services to potential clients who have not traditionally had access to financial institutions. As a result certain innovations were developed in relation to basic banking products. One example of this is the Mzansi account. This is a basic bank account offered by a number of banks in South Africa at a minimum cost. These accounts offer limited debit card services.

825. South Africa does not issue large denomination bank notes; the largest is ZAR 200 (approximately EUR 17).

4.4.2 Recommendations and Comments

826. This Recommendation is fully observed.

4.4.3 Compliance with Recommendation 20

	Rating	Summary of factors underlying rating
R.20	C	This Recommendation is fully observed.

5. LEGAL PERSONS AND ARRANGEMENTS & NON-PROFIT ORGANISATIONS

5.1 Legal Persons – Access to beneficial ownership and control information (R.33)

5.1.1 Description and Analysis

827. In preventing the use of legal persons for illicit purposes, South Africa relies primarily on an investigatory approach, supplemented by a company registry and corporate record keeping requirements.

Company registry (CIPRO)

828. All companies doing business in South Africa, including foreign companies, must be registered in the national company registry, CIPRO. Most registrations are performed electronically. The vast majority of registrations are received from large specialised private companies that do company registration as a business. The largest of these company service providers send about 200 to 300 registration requests to CIPRO per day. The category of "company service provider" is not caught by the FIC Act. Any person can act as a company service provider, and certain specialised firms include lawyers and accountants (but are not required to) and also employ other professionals. Attorneys (whether they are part of a law firm or a specialised company service provider) are subject to CDD (and other FIC Act) requirements to the extent that the legal person involved is outside of South Africa. Accountants are only subject to CDD requirements when they provide investment advice or brokering services, but there is currently an industry debate as to whether company management services would be considered to amount to investment advisory services.

829. The registration requirements for companies (public or private), close corporations and co-operatives are similar.

830. When registering a company, the applicant must file the requested business name, address, power of attorney, articles of association (for a company without share capital) or memorandum of association (for a company with share capital), and details of the directors. The particulars of the directors and officers to be supplied and updated include: surname, full forenames, former surname and forenames, identity number or, if not available, date of birth, date of appointment, designation, name and registration number of every other company of which the person is a director, residential address, business address, postal address, nationality (if not South African), occupation, and whether resident in South Africa or not. Companies are required to notify CIPRO within 15 days of changes to certain particulars (occupation, residential and business address) and within 28 days of changes to directors or officers. Failure to file the particulars or changes to particulars is an offence, but one that is punishable only by a token fine (ZAR 150 / EUR 13) (ss.211 and 216 Companies Act). Directors and other persons directly or indirectly involved in the management of the company must be natural persons. However, nominee directorship is allowed, and there is no requirement to file with CIPRO information concerning on the underlying party. Nominee shareholders are also allowed, and the Registry does not contain information on shareholders, meaning that, the Registry cannot be relied upon for information on either legal or beneficial ownership.

831. The 426 public companies that are listed have additional disclosure and reporting obligations. They must comply with the JSE listings requirements on an on-going basis. These deal mainly with the disclosure and timing of financial information (3.15 to 3.25 and 3.86 and 8.64 of the JSE Rules). There is the general obligation to issue announcements where there is information which cannot be kept confidential and the knowledge thereof may lead to movements in the company's share price *i.e.* trading statements and cautionary announcements (3.4 to 3.10). They must announce the dealings of directors and certain other parties when trading in the listed company's securities. There are also times during which

trading by these person is prohibited (3.63 to 3.74). Changes to the board and their functions need to be announced and all new appointments must complete a Schedule 21 declarations for submission to the JSE (3.59 to 3.62). While these obligations are comprehensive, it should be noted that they apply to only 426 of the 3 521 public companies, and do not apply to the 450 966 private companies or 1 735 111 close corporations.

832. When registering a close corporation, the applicant must supply a "founding statement" that includes the close corporation's name, the principle business to be carried on, postal address, the full name of each member, identity number (or date of birth if he/she does not have an ID number), and residential address, and the size, expressed as a percentage, of each member's interest in the corporation, and particulars of contribution and fair monetary value thereof (if applicable) (s.12 Close Corporations Act). Although members generally must be natural persons, there is an exception for trustees (provided that the trustee does not benefit from the trust). There is no requirement for a member trustee who is a legal person to register with CIPRO information concerning the underlying natural person(s). Close corporations are required to notify the CIPRO of any changes in the particulars referred to above within 28 days (s.15 Close Corporations Act). CIPRO can remind CCs of this obligation and write a written notice to comply, for which there is a penalty of 5 ZAR per day upon which the reminder was sent and not complied with.

833. When registering a cooperative, the applicant must submit the list of founding members and directors, and the constitution of the cooperative (including the name, objectives, description, location of registered office and general meetings, etc.) (ss.6 and 14 Cooperatives Act.). The Cooperatives Act does not specify what information on directors must be supplied or updated, and they are not limited to being natural persons. Where a director is a legal person, there is no obligation to register with CIPRO information about the beneficial owner(s) of that director.

834. For legal persons generally, CIPRO is a good depository of information concerning legal control and, in the case of close corporations and cooperatives, legal ownership. However, the Registry does not collect information on beneficial ownership and control, as those terms are defined by the FATF. Another overarching problem in relation to all of the information contained in the Registry is that none of it is verified, so it cannot be said to be accurate.

Corporate record keeping requirements

Register of Directors:

835. South African companies must keep registers of the directors and officers (s.215 Companies Act). Similar requirements apply to foreign companies, including in relation to the types of particulars on directors must be recorded and supplied (s.322 Companies Act). Foreign companies must appoint a local South African representative and maintain in South Africa a register of directors, managers and secretaries; the provisions in ss. 211, 215 and 216 cited above also apply the local agent (ss.327). Changes must be recorded in the register by the end of the financial year, and reported to CIPRO within 14 days of their entry in the register. Similarly, cooperatives must maintain registers of the directors, including name, address, identification number, the date and which such director became a director (s.21).

Register of shareholders

836. Companies must keep a register of members (shareholders) which includes a statement of the shares issued to each member, distinguishing each share by its number, if any, and by its class or kind and the date on which each name was entered in the register as a member and the date that he ceased to be a member. Each member is entitled to a share certificate which reflects the shares registered in his or her name. Where a company has converted any of its shares into stock (whether in certificated or uncertificated

form), the register must show the amount of stock held by each member instead of the number of shares and the particulars relating to the shares. Foreign companies must keep a register of shares at a registered office in South Africa. The register of members must be open to inspection by any member and any other person upon a nominal fee (s.113 Companies Act).

837. Shareholders may be natural or legal persons. Nominees shareholders are allowed, and shares can be held on behalf of another person. Where shares are held on behalf of another person, the registered shareholder is under a duty to disclose to the company the identity of the person on whose behalf the share is being held, and the number and class of securities so held. This duty of disclosure is triggered at the end of every three-month period. A company may also, by notice, require the registered shareholder to disclose this information if it is suspected that shares are being held on behalf of someone else. All companies are required to maintain a register of such disclosures and shall publish in their annual financial statements a list of persons who hold beneficial interest equal to or in excess of 5% of the total number of securities of that class issued by the issuer together with the extent of those beneficial interests (s.140A, Companies Act). However, the duty to disclose the identity of the person on whose behalf the share is being held, that person could be a natural or legal person, and the duty to disclose would not extend any further. This does not capture the FATF's concept of beneficial ownership/control – *i.e.* the natural person that exercises ultimate ownership/control.

Share warrants to the bearer

838. Public companies (and only public companies) can issue "share warrants to the bearer". The bearer of a share warrant is entitled to the shares specified in the warrant itself. Such shares may be transferred by the delivery of the share warrant to the issuing company (s.101). Upon surrendering a share warrant for cancellation, the bearer is entitled to have his/her name entered in the register of shareholders (s.105(3)(c) Companies Act). If authorised by the company's articles, the bearer of a share warrant may be deemed to be a member of the company (s.103(4) Companies Act).

839. Although they are titled "share warrants", this situation effectively allows for the use of bearer shares for public companies in South Africa, who can own stock and exercise control. To the knowledge of the CIPRO representatives with whom the evaluation team met, such bearer shares were never used. It is believed that they might have been used more in the past, but that other requirements in the company law and FIC Act have inhibited their use. Nor did banking representatives report having seen them when asked.

840. No specific measures are in place to ensure that the share warrants to bearer are not misused for money laundering. However, the Exchange Control Regulations may limit the use of bearer shares and share warrants as it says that "no person shall dispose of, acquire or otherwise deal in any bearer security" (s.15). "Security" is broadly defined and means "shares, stock, bonds, dentures, debenture stock, unit certificates and includes any letter or other document conferring or containing any evidence of rights in respect of any security." It is unclear whether the measures to prevent share warrants to the bearer to be misused for money laundering are sufficient.

Access to information on beneficial ownership and control

841. There are no impediments to accessing the information available. The Company Register is publically available. Any person who pays a nominal fee may obtain the information contained in CIPRO's register. Company registers of directors and shareholders, and close corporation registers of members are also open to public inspection by any person (s.113 Companies Act). These provisions provide easy and timely access to investigative and supervisory authorities for any purpose.

842. The problem is that the information which is available pursuant to the collection mechanisms described above does not capture accurate and current information on the beneficial ownership and control of legal persons. In particular, the information in CIPRO is not verified, and the provisions relating to nominee shareholders may obscure beneficial ownership in the company's share registry. Share warrants to the bearer may also obscure beneficial ownership and control.

5.1.2 Recommendations and Comments

843. There are limited measures in place to ensure that there is adequate, accurate, and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. South Africa operates should broaden the requirements on beneficial ownership so that information on ownership/control is readily available in a timely manner. This could include, for example, restricting the use of nominee shareholders, adopting additional measures to deal with share warrants to the bearer, or requiring legal persons to record full information on beneficial ownership and control in its register which would be available to law enforcement and regulatory/supervisory agencies.

5.1.3 Compliance with Recommendations 33

	Rating	Summary of factors underlying rating
R.33	NC	• There are limited measures in place to ensure that there is adequate, accurate, and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. • Shareholders can be legal persons, and nominees, which may obscure beneficial ownership information. • Information in the company registers pertains only to some legal ownership and control; it does not necessarily contain information concerning beneficial ownership and control; the information is not verified and is not necessarily reliable. • For cooperatives, it is not specified what information on directors must be supplied or updated, and they may also be legal persons. • It is unclear whether the measures to prevent share warrants to bearer to be misused for money laundering are sufficient.

5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34)

5.2.1 Description and Analysis

844. In preventing the use of legal arrangements for illicit purposes, South Africa relies primarily on an investigatory approach, supplemented by a national trust registration system whereby a national registry records details on trusts, including information on the settlers (founders), trustees and beneficiaries. The registry system is supplemented by record keeping requirements related to trust accounting.

845. The administration of trusts is regulated by the Trust Property Control Act, 1988 (TPC Act). There are basically two types of trust in South Africa: *(a)* an inter-vivos trust created between living persons; and *(b)* a testamentary trust which derives from a valid will of a deceased person.

Trust registry system

846. All inter-vivos trusts involving property that is located in South Africa must be registered, regardless of where the settler, trustee or beneficiaries are located. Trusts are usually registered in the jurisdiction where the trust assets are located.

847. Of the 14 Masters of the High Court, only six of them handle trust registrations. A trust must be in the jurisdiction where the trust assets are located (s.3 TPC Act). The majority of trusts (70%) are registered in Johannesburg and Pretoria. Usually, the person physically registering the trust is an auditor or accountant (for tax planning purposes), lawyers (for estate planning purposes) or persons in the trusts services industry (*e.g.* the banks which have separate trust company businesses).

848. There are about 150 000 trusts registered in South Africa. Most of these were created since 1987 when the TCP Act came into force. The most common purpose of these trusts is for tax planning. In last three to four years, about 15 000 to 20 000 trusts have been registered annually.

849. Historically, the trust register was a paper-based system. Each Master's office had a Register of trusts that contained the name of the trust as well as the year in which the trust was registered. A file is opened when a trust is registered and all documents relating to the trust is kept in the file, including the completed forms.

850. However, at the time of the on-site visit, the Master of the High Court was in the process of implementing an electronic version of the trust register. The system was fully operational within two weeks following the on-site visit, and allows full searchability in relation to the names of founders, trustees, beneficiaries and trust name. This system also allows electronic access to the full trust instrument and any amending documents, and all related documentation (including the trustee application form). The database is fully searchable. The database also has the capability to link into the court system for the purpose of cross-checking names; however, this function has not yet been implemented.

851. Run on a central database, the register prevents the same matter from being entered twice. It also generates a time/date stamp for each action, so that the trust actions cannot be backdated and an electronic history of transaction is preserved. The Registry still keeps hard copies as an additional precaution.

852. Work is still ongoing to fully populate the electronic database with information relating to trusts that were created before the electronic Registry was developed. However, in some jurisdictions, this work is substantially completed. There will only be about 2 000 trusts (out of the 150 000 in existence) for which it will not be possible to enter into the new database, as these trusts pre-date the TPC Act and its related data collection requirements. As trusts are entered on the electronic Registry, they are being checked against NPA and SARS lists of red flag names (suspected criminals). This is not the 1267 list; the SARS list, for instance is focused on persons using trusts to evade tax. To date, no matches have been detected.

Information collected

853. No CDD is conducted on the founder of a trust. A settlor (founder) can be a natural or legal person. If the founder is a legal person, it must be represented by an authorised representative. When registering the trust, or dealing with any changes in the trustee, the founder is not required to attend personally to the Master (although the founder's signature is required) (Trust Property Control Regulation (TPC Regulation) 15(f)(1)). The minimum corpus of the trust is ZAR 100. The founder may also be a beneficiary of the trust.

854. CDD is conducted on trustees (TPC Regulation 15(d)(1)). A trustee may be any natural major person or legal person. If a legal person is acting as trustee, a natural person must be appointed who will be representing the legal person. Usually this is a director or someone designated through a special resolution of the legal person. Before someone can be appointed as a trustee, a person must submit a completed application and disclosure form which collects information on the trustee's name, ID number, address, occupation, the location of the trust assets, whether the trustee has been convicted of a dishonesty offence and details of the trustee's solvency. Conviction for a dishonesty offence disqualifies someone from acting

as a trustee and is grounds for removal as a trustee (s.20 TPC Act). The trustee must attend personally and present ID documents. Some Masters' offices place copies of the trustee's ID documents on file; however, this procedure has not been implemented everywhere.

855. Before a trustee assumes control of the trust property, he/she must lodge with the Master the trust instrument in terms of which the trust property is to be administered (s.4 TPC Act). Other supporting documentation must also be filed, including the original trust deed (or notarial certified copy), an undertaking by an auditor (if applicable), a completed "Acceptance of Trustee" form for every trustee and a completed form JM21. The Acceptance of Trusteeship form contains the details of each of the trustees, including name, ID number, residential address and, in the case of an inter-vivos trust, the location of the trust assets. The form JM 21 requires the trustee to furnish information including:

- the names and ages of the beneficiaries under the trust;
- the relationship of the trustee to the beneficiaries;
- the full names and copies of the identity documents of the trustees, including their profession or business occupation, and what previous practical experience each trustee has in trust administration (mentioning any specific cases);
- the written views of beneficiaries under the trust, as to the possibility of exempting the trustee(s) from furnishing security under the TPC Act;
- whether the trust will be subject to annual audit and, if so, the details of the auditor to be appointed to act in the trust; and
- the name of the bank and branch thereof at which the trust banking account will be kept.

856. On receipt of all the required documents, the Master may issue the nominated trustees with Letters of Authority, to administer the trust. No trustee may act as such without the written authority of the Master. The exception is someone who became a trustee prior to the TPC Act coming into force; however, if there is a change of trustee, the new trustee must attend at the Master's to obtain Letters of Authority.

857. Trustees are required to notify the Master within 14 days of any change of address and must also lodge with the Master any amendments to the trust instrument (s.4-5 TPC Act).

858. The Registry does not regulate trusts; it is an office of record. Where a trust is required to file an auditor's statement, for instance, it is not reviewed for suspicious or anomalous activity. The statement is simply received and certified.

859. When a complaint is made about a trust (*e.g.* by an auditor) or there is a suspicion that a negligent misstatement has been made, the Master will usually first call on the trustees to explain. The Master can also conduct an investigation of the trust either through the Master's office, in the case of simple matters, by retaining an auditor to determine whether the conditions of the trust are being complied with or if there has been any strange influx of capital to the trust. The Master does not, however, have any legal basis to impose sanctions in the event that a problem is found, other than applying to a court to have the person removed as a trustee (*e.g.* in cases of significant unlawful conduct).

860. To date, the Masters have never had a suspicion of criminal activity. However, if they became aware of ML, they would immediately go the NPA (without notifying the trustees). The Masters have a very close relationship with the NPA. The Centre does not consider the Master to be a regulator (only a

government agency). As the Master is not a "business", it is not permitted to report suspicious transactions to the Centre under the FIC Act.

Access to information on beneficial ownership and control

861. The contents of the trust deed and the appointment of the trustees are a matter of public record. In addition, in terms of Section 18 of the TPC Act, the Master must on written request and payment of the prescribed fee furnish a certified copy of any document under the Master's control relating to trust property to a trustee, his surety or his representative or any other person who in the opinion of the Master has "sufficient interest" in the document. This is a very low threshold, and is easily met in the context of an investigation or when a creditor is about to lend money to the trust. Additionally, the Registry is establishing relationships with NPA and SARS to further facilitate access to the Registry. SARS also has access to the Registry. It will soon be possible for the banks to have access to the Register to verify the registration of a trust to facilitate their own CDD processes.

862. The Master's office will allow a member of the public access to the file containing the documents relating to a particular trust property, but will allow that person to only make a copy of the trust deed and the Letter of Authority. However, the person may peruse the contents of the entire file under supervision and make notes on the contents of the file. It would appear that this facility is mainly used by attorneys and the trustees themselves.

863. Law enforcement officers (including those from foreign jurisdictions) have access to the contents of the files held at the Masters office and may make a copy of any document in the file. This includes the names of the founders (settlor), trustees, and beneficiaries of trusts. However, where a legal person is a founder, trustee or beneficiary, there is no obligation to obtain information on the beneficial owner as defined by FATF – *i.e.* the natural person that exercises ultimate effective control over the legal arrangement.

864. This access can be exercised in a timely manner. Although exact figures could not be ascertained on the frequency that law enforcement officers request information contained in the files at the Master's office, it would appear that this does not happen very often. The Cape Town Master's office indicated that they recently received a request from a UK law enforcement agency relating to the contents of a file of a particular trust property.

865. Another concern is that accountants who are in the business of providing trusteeship services are not required to perform CDD while providing such services. As indicated in the discussion of accountants under Recommendation 12, the FIC Act requirements apply to accountants when they are rendering investment advice or investment broking services (Schedule 1, s.12 FIC Act). Lawyers are also exempted funder Exemption 10(1) from performing CDD when creating or managing a legal person or arrangement.

5.2.2 Recommendations and Comments

866. The Trust Registry is a valuable source of current information on trusts, including the founder, trustee and beneficiary. However, steps should be taken to ensure that the information held in the Registry is accurate (*e.g.* verification), and that the remaining paper files are uploaded into the register. In addition, the South African authorities should consider providing the Masters of the High Court the authority to report suspected ML/FT directly to the Centre.

5.2.3 Compliance with Recommendations 34

	Rating	Summary of factors underlying rating
R.34	PC	• Where a legal person is a founder, trustee or beneficiary, there is no obligation to obtain information on the beneficial owner of the legal person. • Identification information on the founder and beneficiary is not verified by the trust register. • No records exist of the 2 000 trusts that were created prior to 1987 when the TPC Act came into effect.

5.3 Non-profit organisations (SR.VIII)

5.3.1 Description and Analysis

Special Recommendation VIII

General Legal Provisions

867. The Non-Profit Organisations (NPO) sector in South Africa is well established and is comprised of various voluntary associations, charitable trusts and corporations in relation to education, health, faith, environment, arts and culture, sports and recreation.

868. In recognising the vital role of NPOs in the social and economic environment, South Africa has established a legal framework that supports the formation of NPOs based on common law, the country's Constitution and other statute laws. The Non-Profit Organisations Act (NPO Act), which came into operation on 1 September 1998, is the principal legislation that regulates NPOs in South Africa. The Act is administered by the NPO Directorate (the Directorate) established within the Department of Social Development (DSD) pursuant to Section 4 of the NPO Act. The Directorate is headed by a director (the Director) who is appointed by the Minister of Social Development. The Directorate has a staff complement of 32.

869. An NPO is defined in terms of Section 1(x) of the NPO Act as "a trust, company or other association of persons; a) established for a public purpose; and b) the income and property of which are not distributable to its members or office bearers except as reasonable compensation for service rendered".

870. Under the NPO Act, there are therefore three legal structure options for NPOs, namely: trusts; not for profit companies registered under Section 21 of the companies' legislation and voluntary associations. As at 31 May 2008, there were 20 359 not for profit active companies registered with the CIPRO. Trusts and non-profit companies are registered with the Master's Office and CIPRO respectively and must comply with the legislation under which they are registered. In some cases, an NPO may be required to comply with dual registration processes and ongoing registration obligations. For example, a not for profit company which is registered with both the CIPRO and the Directorate must comply with the requirements of the NPO Act and of the Companies Act 61 of 1973. Voluntary Associations are governed by the common law, which requires that the voluntary association's objectives must be lawful and not primarily for gain or profit for its members.

Composition and size of the NPO Sector in South Africa

871. The South African NPO sector is characterized by a wide spectrum of organisations of different sizes and shapes across the social, political and economic landscape. Within the register of NPOs held with

the Directorate, organisations are classified according to the International NPO classification system. The table below shows the number of registered organisations in each category.

Total number of registered NPOs as at 21 July 2008

Classification Category		Percentage	Total
1	Social services	27.67	14 305
2	Development and Housing	20.79	10 751
3	Education and research	13.25	6 852
4	Health	11.43	5 908
5	Religion	10.56	5 461
6	Culture and recreation	4.88	2 521
7	Law, advocacy and politics	2.23	1 152
8	Environment	1.22	629
9	Philanthropic intermediaries and voluntarism promotion	1.05	541
10	Business and professional associations, unions	0.33	173
11	International	0.07	36
12	Others	6.52	3 373
Total		100	51 702

872. The total income of the non-profit sector in South Africa was estimated to be ZAR 9.3 billion in 1998 (1,2% of 1998 gross domestic product) of which government provided ZAR 5.8 billion (42%), ZAR 500 million of which derived from overseas development assistance, channelled largely but not exclusively through the South African government. Self-generated income derived from fees, sales, and membership dues accounted for 29%, private sector donations (mostly local) accounted for 25% and investment income accounted for the remaining 5%. The fields benefiting the most from this source were social services (36% of the total government contribution), health (29%), and development and housing (20%), with education and environment receiving little amounts (of the total government contribution, 86% went to the delivery sectors).[23] It is further estimated that only 4% of organisations have revenues that exceed ZAR 1 million, 8% had revenues between ZAR 250 000 and ZAR 1 million, 77% had revenue of less than ZAR 250 000 and 11% have no financial resources.[24]

873. The South African economy experienced a significant growth for the last five years or so and the estimated expenditure of the sector has subsequently also increased to ZAR 12.5 billion of which government contributed about ZAR 10 billion.[25]

[23] Swelling M. and Russell B. (2002) *The Size and Scope of Non-profit Sector in South Africa*. Graduate School of Public Development Management (P&DM), University of the Witwatersrand & The Centre of Civil Society (CSS) University of Natal.

[24] Department of Social Development (2005). An impact Assessment of the NPO Act, No 71 of 1997.

[25] Bonochis, R. article *on BoE gives advice NGOs can bank on*. Business Day, Monday, 5 March 2007.

Reviews of the domestic non-profit sector

874. The South African government has completed a study on the Impact Assessment of the NPO Act in 2005 as part of the regular review of its legislative framework on the non-profit sector. This exercise was aimed at finding out whether the current provisions of the Act are still relevant to the NPO sector since its enactment and implementation in September 1998. This study recommended that a process should be initiated to amend the NPO Act. As a result, draft regulations have already been issued to the NPOs for comment on the process and appointment of a technical committee to take this recommendation forward.

875. Despite the above exercise, no assessment of the potential risks of terrorist financing posed within the NPO sector in South Africa has been undertaken yet.

Protecting the NPO sector from terrorist financing through outreach and effective oversight

876. One of the stated objects of the NPO Act is to encourage NPOs to maintain adequate standards of governance, transparency and accountability and to improve those standards. Further, under Section 5(b)(ii) of the Act, the Directorate is responsible for ensuring that the standard of governance within non-profit organisations is maintained and improved. To this end, the Directorate has, pursuant to its powers under Section 6(b) of the Act, issued a Code of Good Practice for South African NPOs. The Code of Practice provides guidelines for NPOs on improving their governance and resource mobilisation including the roles and responsibilities of donors and sponsors as efforts to promote self-regulation within the sector.

877. To compliment the Code of Good Practice, the Directorate undertakes outreach programs by conducting information sharing workshops with networking organisations within the NPO sector on good governance practices and compliance with the legal framework as part of the efforts to promote public confidence in the administration and management of NPOs.

878. No outreach programme has however been undertaken or encouraged to raise awareness in the NPO sector about the vulnerabilities of NPOs to terrorist abuse and terrorist financing risks, and the measures that NPOs can take to protect themselves against such abuse.

879. Registration of NPOs under the NPO Act is not mandatory. The concept of voluntary registration adopted under the Act finds its roots in the South African Constitution which guarantees everyone the right to freedom of association and expression.

880. It is projected that out of the 100 000 non-profit organisations existing in South Africa 52 000 are registered with the Directorate.

881. The Directorate must in terms of the Act keep a register of all registered NPOs. All members of the public have the statutory right to access and to inspect the register.

882. The monitoring and supervision of all registered NPOs falls under the responsibility of the Directorate. The Directorate has a desk compliance programme which is largely based on information from the annual narrative reports of the activities of NPOs, financial statements and complaints and tips from the public.

883. Section 18(4) of the NPO Act also imposes a whistle blowing obligation on the accounting officer of a registered NPO where he becomes aware of any instance in which the organisation has failed to comply with the financial provisions under the NPO Act or its constitution. Any instance of non-compliance must be notified to the Director. In practice, this provision has seldom been used.

884. Applicants use a standard form for registration purposes under the NPO Act. As part of the registration process an NPO must submit the following particulars to the NPO Directorate in respect of each office bearer:

- name;
- surname;
- business and residential addresses;
- ID Number;
- contact details; and
- capacity in organisation.

885. In addition, the constitution of a non-profit organisation that intends to register must contain information on its main and ancillary objectives, and specify the organisational structures and mechanisms for its governance. Pursuant to Section 19 of the NPO Act, the Directorate must be notified of any change to the constitution or name of a registered NPO.

886. Furthermore, in terms of Section 18(b) of the NPO Act, a registered NPO must, within one month after any appointment or election of its office-bearers even if their appointment or election did not result in any changes to its office-bearers, provide the Directorate the names and physical, business and residential addresses of its office-bearers.

887. The Directorate is maintaining a complete database of all registered organisations as required in terms of Section 24 of the NPO Act. This database has all of the documentation that organisations have submitted to the Directorate to meet registration requirements in terms of Sections 12 and 13 and to maintain the registration status in terms of Sections 17 and 18. These documents include a narrative report outlining the activities to achieve the said purpose and objectives of the organisation and its financial statements together with the accounting officer's report.

888. The Directorate must, in terms of Section 25 of the NPO Act, make all records of registered organisations publicly available. To this end, the Directorate had initiated a process to review and upgrade the existing database system of registered organisations with the intention of providing easier and timely access to records of organisations on a World Wide Web public information platform. As part of this initiative, the Directorate has already digitised more than 1.8 million pages of 52 000 organisations records.

889. The database of registered NPOs held by the NPO Directorate in the DSD as well as all information and documents submitted by NPOs are publicly available for inspection.

890. The Director has limited powers to sanction violations of oversight measures. Where a registered NPO fails to comply with a material provision of its constitution or its obligations in terms of Sections 17 (keeping of accounting records), 18 (duty to provide reports and information) and 19 (changing constitution or name of registered NPO) or any other provision of the NPO Act, the Director must in accordance with Section 20 of the Act send a compliance notice to the registered NPO. The NPO has one month to comply with the requirements of the notice. Failure to comply with a compliance notice entails the cancellation of the registration of the NPO.

891. The Directorate uses the compliance notice to ensure that registered NPOs comply with the requirement to submit the annual narrative report of their activities and financial statements under Sections 17 and 18 of the NPO Act. A reminder in the form of a compliance notice is sent annually to all registered NPOs 3 months before these financial statements are due. In the course of last year, the Directorate had sent 31 000 compliance notices out of which 23 279 responses were received while 1 453 NPOs were deregistered for failure to comply with the compliance notice.

892. The Director has neither the power to sanction office bearers nor the power to impose fines or to freeze accounts of NPOs for violations of oversight measures.

893. The NPO Act also provides for certain criminal offences, *e.g.* making of material false representations in financial reports or any document submitted to the director, etc. Pursuant to the provisions of Section 29(2) of the Act, these offences apply to persons, bodies or organisations.

894. In cases where the Director is satisfied that any non-compliance may constitute an offence he must refer the registered NPO to the SAPS for criminal investigation. During the last three years the Directorate has referred about 10 cases to SAPS for investigation. The cases were mostly related to fraud and corruption within the NPO. There has been no conviction for offences under the NPO Act yet.

895. Registered NPOs in South Africa must comply with financial disclosure requirements as provided under the Act. Accounting records must be kept and financial statements together with a report from an accounting officer certifying compliance with the organisation's constitution, its accounting policies and the NPO Act must be filed with the NPO Directorate annually.

896. Pursuant to the provisions of Section 17(3) of the NPO Act a registered NPO must preserve each of its books of account, supporting vouchers, records of subscriptions or levies paid by its members, income and expenditure statements, balance sheets and accounting officer's reports for the prescribed period. However, no period has been prescribed yet.

897. Other than the requirements set out under Section 18 of the NPO Act (see above) there is no specific requirement under the NPO Act, for NPOs to maintain for a period of five years information on the identity of person(s) who own, control or direct their activities, including senior officers, board members and trustees.

898. In terms of Section 25 of the NPO Act, the Directorate has a duty to preserve all reports and documents submitted to the Director under the Act. All members of the public have the right of access to and to inspect these documents.

Targeting and attacking terrorist abuse of NPOs through effective information gathering, investigation

899. The SAPS is responsible for the investigation of all criminal activities including terrorist financing offences through the abuse of the NPO sector.

900. The South African authorities have set up a special unit within the SAPS Detective Service under the organised crime component to deal with and investigate all crimes against the State, terrorism and terrorist financing offences including NPOs of potential terrorist financing concern. Information may be gathered by the SAPS through formal powers under statute and informal powers pursuant to existing working arrangements with other government agencies.

901. The Crime Intelligence Division within the SAPS and the National Intelligence Agency are capable of gathering intelligence information on NPOs irrespective of whether they registered or not.

902. A number of mechanisms have been put into place to deal with terrorism and terrorist financing offences. An Inter-Departmental Counter-Terrorism Working Group was formed under the auspices of the Department of Foreign Affairs comprising of the SAPS, NPA, Defence Force, National Intelligence Agency, South African Secret Service, National Intelligence Co-ordinating Committee, Department of Home Affairs, Department of Transport, National Treasury and the Centre.

903. Further, the Priority Crimes Litigation Unit in the NPA has an arrangement with the Divisional Commissioner: Detective Service, South African Police Service relating to the referral of investigations in respect of offences under the POCDATARA.

904. Save for the referral of suspected cases of offences under the Act to SAPS, the Directorate has no formal gateway for the exchange of non-public information regarding registered NPOs. However, the Directorate has indicated that it has developed a good working relationship with the Centre over the last two years and this should facilitate the exchange of information to some extent.

905. The constitution of a registered NPO and the information relating to a registered NPO submitted to the NPO Directorate as well as the register kept by the NPO Directorate are all publically available and may therefore be accessed in the course of an investigation.

906. Moreover, information may also be obtained by the SAPS through a search warrant or through the use of other statutory investigative powers to gather information.

907. South Africa has developed and implemented mechanisms for prompt sharing of information among all relevant authorities with regard to terrorism and terrorist financing offences as well as mechanisms to take preventive or investigative action when there is a suspicion or reasonable grounds to suspect that a particular NPO is being exploited for terrorist financing purposes or is a front organisation for terrorist financing. The POCDATARA imposes an obligation on all persons in South Africa to report to a police official any suspicion of a terrorist financing offence.

908. Officers of the SAPS have been exposed to significant investigative training including AML/CFT training and have the necessary investigative skills and capability to examine those NPOs of potential terrorist financing concern.

Responding to international requests for information about an NPO of concern

909. The Department of Justice is the primary contact point for international cooperation issues including requests for information regarding particular NPOs that are suspected of terrorist financing or other forms of terrorist support. This Department is designated in terms of the provisions of the International Cooperation in Criminal Matters Act, No. 75 of 1996. The Act facilitates the provision of evidence and the execution of sentences in criminal cases and the confiscation and transfer of the proceeds of crime between South Africa and foreign states.

910. In respect of mutual legal assistance and extradition, the SAPS has its own international cooperation regime in addition to that of extradition and mutual legal assistance. The SAPS cooperates with other police agencies via Interpol and in terms of a number of police-to-police cooperation agreements that have been concluded with a number of states since 1995.

5.3.2 Recommendations and Comments

911. The voluntary requirement for the registration of NPOs under the NPO Act undermines the transparency and accountability in the way that NPOs collect and transmit funds in South Africa and creates a loophole that increases the risk of abuse of unregistered NPOs by terrorist financiers. South

Africa must make an assessment of the potential risks of terrorist financing posed within its NPO sector and the level of oversight measures must be reviewed to ensure that these are effective and proportional to the risk of abuse.

912. The legislation governing the NPO sector in South Africa should further be reviewed to require the mandatory registration of NPOs in South Africa.

913. In addition, the enforcement powers under the NPO Act should be reviewed to provide additional sanctions including, the power to sanction office bearers, impose fines and freeze accounts of NPOs for violation of oversight measures.

914. Regulations must be passed under the NPO Act to specify the retention period that applies to the record keeping requirement of NPOs under Section 17(3) of the Act.

915. The NPO laws should be amended to provide for the requirement for NPOs to maintain for a period of at least five years information on the identity of person(s) who own, control or direct their activities, including senior officers, board members and trustees.

916. Further the governing legislation should also provide for formal gateways for the exchange of non-public information by the Directorate.

917. Outreach programmes must be undertaken with the specific aim to protect the NPO sector from terrorist financing abuse.

5.3.3 Compliance with Special Recommendation VIII

	Rating	Summary of factors underlying rating
SR.VIII	PC	• No assessment of the potential risks of terrorist financing posed within the NPO sector in South Africa has been undertaken yet. • No outreach programme has been undertaken with the specific aim to protect the sector from terrorist financing abuse. • There is no registration requirement under the NPO Act in as much as registration of NPOs is only voluntary. • The Director has neither the power to sanction office bearers of defaulting NPOs nor the power to impose fines or to freeze accounts of NPOs for violation of oversight measures. • There is no prescribed retention period that applies to the record keeping requirement of NPOs. • There is no specific requirement under the NPO Act, for NPOs to maintain for a period of five years information on the identity of person(s) who own, control or direct their activities, including senior officers, board members and trustees. • There are no formal gateways for the Directorate to exchange non-public information.

6. NATIONAL AND INTERNATIONAL CO-OPERATION

6.1 National co-operation and coordination (R.31)

6.1.1 Description and Analysis

Policy cooperation

918. The anti-money laundering (AML)/combating the financing of terrorism (CFT) systems in South Africa are relatively young. However, South Africa has demonstrated a strong commitment to implementing the country's AML/CFT systems which has involved close cooperation and coordination between a variety of government departments and agencies.

919. The FIC Act in 2002 established a Money Laundering Advisory Council (MLAC) to advise the Minister of Finance of polices and practices to combat money laundering activities and act as a forum in which the Centre, associations representing categories of accountable institutions, and government agencies (such as National Treasury, SAPS, SARS, NPA, NIA, SARB, and FSB) can consult one another. The Centre provides administrative and secretarial support for the MLAC. The MLAC is one of the parties that must be consulted before the Minister may make, repeal, or amend regulations under the FIC Act, amend the lists of accountable institutions, supervisory bodies or reporting institutions.

920. The MLAC was inaugurated on 18 October 2002 by the Minister of Finance. In practice, however, the MLAC does not hold regular meetings, and ML policy development is led by the Centre in ongoing but separate meetings with the various agencies. There is evidence that policy coordination in the past has not been fully effective, for example the FIC Act did not designate the correct SROs for the legal profession. Nevertheless, there currently appears to be much more and active involvement in AML/CFT coordination by all relevant stakeholders.

921. At Cabinet level, the National Security Council and the Justice, Crime Prevention and Security Cluster are amongst the fora for co-ordination among ministries and heads of departments in the Criminal Justice System. The Cluster comprises of the Departments of Home Affairs, Defence, Finance, Foreign Affairs, Intelligence Services, Safety and Security, Correctional Services, Justice and Constitutional Development, Social Development and the National Prosecuting Authority.

922. In respect of terrorism and terror financing an Inter-Departmental Counter-Terrorism Working Group was formed under the auspices of the Department of Foreign Affairs to facilitate the implementation of UNSC Resolutions 1267(1999) and 1373(2001) as well as international conventions relating terrorism. In addition to the Department of Foreign Affairs, the Working Group consists of the SAPS, NPA, Defence Force, National Intelligence Agency, South African Secret Service, National Intelligence Co-ordinating Committee, Department of Home Affairs, Department of Transport, Department of Justice and Constitutional Development, Department of Social Development, South African Revenue Service, the Border Control Co-Ordination Committee, National Treasury and the Centre. Meetings are generally held monthly. In addition a Project Team on International Terrorism under the National Intelligence Co-ordination Committee (NICOC) has been established in 2005 by the Minister of Intelligence – as a result of the risk of international terrorism identified in the National Intelligence Estimate. Concerns of ML and TF are also addressed in this forum, as well as strategy responses to international trends and UN listings of terror suspects.

923. Additionally, there has been Cabinet level involvement throughout every stage of the FATF mutual evaluation process.

Operational cooperation

924. A number of mechanisms exist to promote effective operational cooperation amongst the bodies combating ML and FT.

925. A National Priority Committee on Commercial Crime under the Chairmanship of the South African Police Service with representatives from the Department of Justice and Constitutional Development, the SAPS and the South African Banking Risk Information Centre[26] meet on a monthly basis to identify threats, coordinate efforts to address and combat commercial crime.

926. The Priority Crimes Litigation Unit in the NPA has an arrangement with the Divisional Head of SAPS: Detective Services relating to the referral of investigations in respect of offences under POCDATARA.

927. A framework document exists between the National Prosecuting Service, the SAPS and the AFU to deal with organised crime, which includes money laundering. This document defines the level of co-ordination and co-operation between these structures. This operational co-operation exists at both a provincial and national level. A similar memorandum of understanding exists between the Specialised Commercial Crimes Unit, the SAPS and the AFU to deal with money laundering cases which are received from the SAPS Commercial Branch.

928. The BSD and the ExCon Department regularly participate in meetings with the Centre where issues relating to money laundering and terror financing are discussed. An MOU is due to be entered into between the SARB and the Centre in order to formalise and facilitate an enhanced relationship between the various departments of the SARB and the Centre.

929. The Centre also plays a leading role in coordinating cooperation in relation to the FIC Act. Regular meetings and contact at various levels happen between the Centre and the various supervisors *e.g.* the SARB, the FSB, JSE, EAAB, NGB, IRBA, CIPRO, and LSSA. The FSB has entered into a MOU with the Centre to cooperate *inter alia* on matters relating to money laundering. The FSB is a member of the South African Regulators Forum where all regulators irrespective of the sector they regulate meet and discuss issues of mutual concern which include money laundering and terrorist financing. The FSB has ongoing interaction with *inter alia* the BSD in the SARB, the SARS, the Competition Commission, the Asset Forfeiture Unit, the Specialised Commercial Crimes Unit, the Centre and the Department of Trade and Industry.

930. The SAPS also indicated that it has an excellent working relationship with the Centre. The SAPS and the Centre hold frequent consultations with the Centre providing intelligence for police investigations, and as a result the SAPS does more investigations on information received from the Centre. The assessors were informed that the intelligence information from the Centre has good value enabling the police to follow up. Often such information has resulted with the police being able to seize substantial amounts of assets.

931. The NIA works in cooperation with other departments and coordinates on intelligence sharing relating to terrorism and terrorist financing. The NIA and the Centre have designed personnel to liaise in

[26] The South African Banking Risk Information Centre (SABRIC) is a not-for-gain company established to combat crime in the banking industry. Its key stakeholders are the major banks and its principle business is to detect, prevent and reduce organised crime in the banking industry through effective public private partnerships. The company also provides crime risk information and consequence management to the banking industry and cash in transit companies.

regard to STRs that relate to potential terrorist or terrorist financing activity. The NIA also makes other departments aware of intelligence concerns.

932. The JSE indicated that it has very close cooperation with the Centre, and regular meetings between the two are held. The Centre attended all of the JSE's reviews of its members for FIC Act compliance. LSSA also meets regularly with the Centre, who has assist LSSA with FIC Act education.

933. The Centre has also signed an MOU with the EAAB, which is aimed at enhancing the relations between the two organisations in the fight against money laundering and terror financing. There are standing quarterly meetings between the Centre and the EAAB which seek to discuss and address the latest development on compliance and AML/CFT issues pertaining to estate agents.

Additional elements

934. The FSB holds regular meetings with industry bodies such as the Life Offices' Association, the Association of Collective Investments, South African Insurance Association, Financial Intermediary Association, Banking Association of South Africa, Investment Management Association of South Africa, Link Investment Services Providers Association, Alternative Investment Management Association of South Africa, Compliance Institute of South Africa, South African Institute of Charted Accountants, Funeral Assistance Business Association, Black Brokers Association as well as the Reserve Bank. The FSB is a member of and participates in the activities of the Anti Money Laundering Advisory Council.

935. The legislation governing accountable institutions in the spheres of Collective Investment Schemes (Section 8 of CISC Act), Long-term Insurance (Section 6 of the LTI Act) and Financial Services Providers (Section 5 of the FAIS Act) established Advisory Committees on which industry representatives serve. These Committees meet regularly with the Registrar or Minister of Finance in order to investigate, report or advice on matters relevant to the industry which include AML/CFT requirements.

Recommendation 32

936. South Africa has not reviewed the effectiveness of its systems for combating money laundering and terrorist financing on a regular basis.

Resources (policy makers)

937. The MLAC is a forum in which the Centre, associations representing categories of accountable institutions, and government agencies (such as National Treasury, SAPS, SARS, NPA, NIA, SARB, and FSB). See Sections 2.5, 2.6, 3.10, and 6.3 of the report for resources information on these entities.

6.1.2 Recommendations and Comments

938. South African authorities have established effective mechanisms to cooperate on operational matters to combat ML and FT. The Centre has in place mechanisms to exchange information and coordinate effectively with the various stakeholders, and regulators and law enforcement agencies, and to cooperate effectively amongst themselves. Authorities should ensure that effective policy coordination continues.

6.1.3 Compliance with Recommendation 31

	Rating	Summary of factors underlying rating
R.31	C	• This Recommendation is fully observed.

6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)

6.2.1 Description and Analysis

Recommendation 35 and Special Recommendation I

United Nations Conventions

939. South Africa ratified the Palermo Convention on 20 February 2004, and the Terrorist Financing Convention on 1 May 2003, and acceded to the Vienna Convention on 14 December 1998. The vast majority of the Conventions' provisions have been implemented. However, as noted in Section 2 of this report, Section 6 POCA (acquisition, use and possession) does not apply to the person who committed the predicate offence as required by the Palermo Convention 6(1)(b)(i) and 6(2)(e). Also, South Africa does not fully comply with Article 18(1), which requires countries to implement sufficient measures to identify customers in whose interest accounts are opened (see Section 3.2 of this report).

Implementation of S/RES/1267(1999) and its successor resolutions and S/RES/1373(2001)

940. South Africa has implemented components of S/RES/1267(1999) and its successor resolutions and S/RES/1373(2001).

Additional elements

941. South Africa has signed and ratified the OECD Convention for Bribery of Foreign Officials. The accession was in April 2007 and the official handing over of the accession documents took place on 19 June 2007.

942. South Africa also became party to the Tokyo Convention on 26 May 1972, the Hague Convention for the Suppression of Unlawful Seizure of Aircraft on 30 May 1972, the Montreal Convention relating to the Safety of Civil Aviation on 30 May 1972, the UN Convention on Crimes Against Protected Persons on 23 September 2003, the UN Convention on Hostages on 23 September 2003, the Montreal Protocol on 21 September 1998, the Montreal Convention on Plastics Explosives on 1 December 1999, the UN Convention on the Suppression of Terrorist Bombings on 1 May 2003, the UN Convention on the Suppression of the Financing of Terrorism on 1 May 2003, the Rome Convention on the Safety of Maritime Navigation on 10 March 1998, the Rome Protocol for the Suppression of Unlawful Acts on Fixed Platforms on 10 March 1988, the Vienna Convention for the Physical Protection of Nuclear Material on 18 May 1981 and the AU Algiers Convention on the Prevention of Terrorism on 14 July 1999.

6.2.2 Recommendations and Comments

943. South Africa should amend its money laundering offence to be fully consistent with the Palermo Convention and enact stronger customer identification measures. South Africa should also enact measures to be able to more effectively freeze funds without delay in the context of S/RES/1267(1999) and S/RES/1373(2001).

6.2.3 Compliance with Recommendation 35 and Special Recommendation I

	Rating	Summary of factors underlying rating
R.35	LC	• *Palermo:* Section 6 POCA (acquisition, use and possession) does not apply to the person who committed the predicate offence as required by the Palermo Convention 6(1)(b)(i) and 6(2)(e).

	Rating	Summary of factors underlying rating
		• *FT Convention*: South Africa does not fully comply with Article 18(1), which requires countries to implement sufficient measures to identify customers in whose interest accounts are opened (see Section 3.2 of this report).
SR.I	LC	• *FT Convention*: South Africa does not fully comply with Article 18(1), which requires countries to implement sufficient measures to identify customers in whose interest accounts are opened (see Section 3.2 of this report).

6.3 Mutual Legal Assistance (R.36-38, SR.V)

6.3.1 Description and Analysis

Range of assistance

944. The measures and provisions discussed below apply to international co-operation relating to money laundering as well as terrorist financing.

945. The ICCMA specifically provides that the following forms of assistance may be rendered by South Africa:

- request for assistance in obtaining evidence (including production orders) – (s.8);
- request for assistance in compelling attendance of witness in certain foreign states [27]– (s.11);
- request for execution of a foreign sentence (fines only) – (s.15); and
- request Enforcement of foreign restraint and confiscation order – (ss.20 and 24).

946. Apart from the forms of assistance specifically mentioned in the ICCMA, the assessment team was also advised that South Africa is able to render assistance for those matters ***not*** mentioned in the ICCMA. These can be rendered pursuant to domestic legislation and other established practices, and they include:

- locating or identifying persons;
- service of documents, including seeking the attendance of persons;
- locating or providing documents, records and articles, including lending of exhibits;
- taking of statements or testimony of persons;
- making detained persons available to give evidence or assist in investigations;
- facilitating the appearance of witnesses or the assistance of persons in investigations;
- search and seizure; and
- any other forms of assistance not prohibited by South African domestic law.

[27] Lesotho, Swaziland Botswana, Malawi, Namibia, and Zimbabwe: see Schedule 1 ICCMA.

947. While it may be that South Africa is able to render a wide range of assistance, there are nevertheless minor issues concerning some of these mechanisms for assistance.

948. First, in respect of the request to enforce a foreign restraint order pursuant to Section 24(1) of the ICCMA, it is noted that such requests can only be enforced if the foreign restraint order in question is not subject to any review or appeal. Given that restraint orders are often in themselves interim measures meant to prevent the dissipation of property, the requirement of finality in the foreign restraint order clearly creates a potential loophole which a defendant facing such an order may exploit.

949. Secondly, where the request is for the obtaining of evidence from a person, there is a difference between the procedure provided under Section 8 of the ICCMA, which governs such requests, and Section 205 of the CPA, which governs the obtaining of evidence pursuant to a local investigation. Under both Section 8(1) of the ICCMA and Section 205 CPA, such a person is compelled by a subpoena to attend before a magistrate or court to testify on oath and to produce the documents.

950. However, Section 205 of the CPA also contains a proviso that if such person furnishes that information to the satisfaction of the Director of Public Prosecutions concerned, prior to the date on which he is required to appear and testify before a judge, regional court magistrate or magistrate, he shall be under no further obligation to appear before such judge, regional court magistrate or magistrate. This proviso is absent in Section 8(1) of the ICCMA and consequently, the person subpoenaed under s 8(1) of the ICCMA must appear before the court in any event even if he was able and willing to furnish the information before the hearing date.

951. Given that production orders for bank and other financial records are commonly sought in money laundering investigations, the procedure as provided under Section 8 of the ICCMA may not be the most efficient way of rendering assistance for a request to produce the evidence when compared to the simplified procedure in Section 205 of the CPA, which allows for dispensation of attendance of the witness where the witness is able to provide the evidence before the date set down for hearing. This may result in delays in executing a request.

952. The ICCMA also does not have a Section dealing with the certification of documentation for foreign processes. However, South Africa is a signatory to the Hague Convention and the method of authentication specified in the Convention applies to the Act. Depending on the circumstances surrounding specific documents, original documents could be supplied.

Processing and execution of requests

953. The Director-General: Department of Justice and Constitutional Development is the Central Authority for all matters pertaining to MLA and Extradition within South Africa. Requests for mutual legal assistance must therefore be directed to the Office of the Director-General: Department of Justice and Constitutional Development as the Central Authority for South Africa for processing according to the relevant provisions in the ICCMA.

954. With the exception of a request to enforce a foreign restraint order where the prior approval of the Minister is not needed (s 24) the Director-General then submits the request to the Minister of Justice for approval. Upon the Minister's approval, the relevant agencies will make the necessary arrangements for the request to be executed. As noted, search and seizure is not a form of assistance expressly provided in the ICCMA, and an issue of how such requests are to be processed arose in the past in. This was dealt with in *Beheermaatscappij Helling I N.V. and others v The Magistrate, Cape Town, and others [Case No: 5635/2004, CPD]*, where the High Court held that such requests would, by logical extension and necessary implication having regard to the objectives of the ICCMA, be processed according to Section 7 of the

ICCMA, (which lays down the procedure for processing a request to obtain evidence). Since then, there have not been any challenges to this judgement and it seems to be the accepted view on this issue.

955. At the on-site meeting, the assessment team was informed that the turn-around time for a request depended on the nature and complexity of the request. It may range from a few days to six months. Priority will be accorded to urgent requests where time is of the essence. In general, the officers dealing with requests aim to attend to the request no later than five days on receipt of the request, and to submit a memorandum for approval by the Minister not later than five days on receipt of all relevant information, and to act on the approval by the Minister not more than five days on receiving such approval, with follow-up every four weeks with the agencies executing the request.

956. In addition to the ICCMA, South Africa is also able to render assistance on the basis of bi-lateral or multi-lateral treaties as well as the principle of international comity. To date, South Africa has signed mutual assistance treaties with twelve countries: Algeria, Argentina, Canada (in force 2001), Egypt (in force 2003), France (in force 2004), India, Indonesia (in force 2003), Iran, Lesotho, Nigeria, Peoples' Republic of China (in force 2004) and the United States of America (in force 2001). South Africa has also signed the Southern Africa Development Council (SADC) Protocol on Mutual Legal Assistance in Criminal Matters which it ratified in 2003. South Africa is also a member of the Harare Scheme relating to mutual legal assistance in criminal matters among Commonwealth states.

Conditions and restrictions

957. The ICCMA does not regulate the discretionary power of the Minister in considering whether or not he should approve a request, nor does the ICCMA provide any grounds of refusal on which a request can be rejected. However, for a request by a foreign country for execution of a foreign sentence of fine pursuant to Section 15(1) of the ICCMA, the Minister may refuse assistance if he is 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.

958. Dual criminality is also not a pre-requisite for the rendering of mutual legal assistance in terms of the ICCMA.

959. Assistance is generally provided on the basis of an assurance of reciprocity, but this principle is not interpreted in an overly strict manner.

960. Neither the ICCMA nor the treaties impose restrictions against requests relating to fiscal matters. South Africa is therefore able to accede to requests for mutual legal assistance on fiscal matters.

961. Banking secrecy or confidentiality is not a ground for refusal in rendering mutual legal assistance. The ICCMA only permits a witness to claim a privilege which the person is entitled to raise under South African law or where he would be entitled to raise according to the law of the Requesting State (Section 9). Financial institutions in South Africa are not legally entitled to claim a privilege on the basis of client confidentiality.

Availability of police powers and avoiding conflicts of jurisdiction

962. The Interpol component of the South African Police Service is responsible for the execution of approved requests for mutual legal assistance. Interpol is entitled, not only to exercise the powers in terms of the Act or Treaties, but also to exercise its ordinary police powers. Where a request involves court proceedings, the Presiding Judicial Officer may issue directives for the subpoenaing of witnesses and the

production of documents. As a result, the SAPS would be entitled to exercise its powers and investigative techniques in the execution of a request.

963. The assessment team was informed that South Africa would consult with other countries to avoid conflicts of jurisdiction. This, however, would have to be addressed on a case-by-case basis. No examples of cases where such consultation took place were provided to the assessment team.

Additional elements

964. All requests for formal mutual legal assistance must be submitted to the Central Authority, the Director-General: Department of Justice and Constitutional Development for processing and for onward transmission to the relevant authority for assistance.

Recommendation 37 and Special Recommendation V

965. Dual criminality is not a pre-requisite for the rendering of mutual legal assistance under the ICCMA.

Recommendation 38 and Special Recommendation V

966. Chapter 4 of the ICCMA provides for the confiscation and transfer of proceeds of crime or property of corresponding value through the execution of "foreign confiscation orders". South Africa also has an asset forfeiture regime under the POCA which provides for both criminal and civil forfeiture. The mechanisms of the POCA are used to give effect to a request relating to the freezing and confiscation of the proceeds and instrumentalities of crime. In terms of these provisions the foreign order is registered with the registrar of the appropriate court, whereupon the foreign order acquires the status of a South African order which can then be executed in terms of the POCA.

967. In addition, the CPA provides for the search and seizure of articles which are concerned in the commission or suspected commission of an offence, whether within the Republic or elsewhere or which may afford evidence of the commission or suspected commission of an offence, whether within the Republic or elsewhere (s.20, CPA). Such articles may be disposed of by an order of a magistrate that the articles be delivered to a member of a police force established in another country who may then remove it from South Africa (s.36, CPA).

968. South African authorities indicate that these CPA provisions would be used to cover the search and seizure of instrumentalities intended for use in ML, predicate offences, and FT.

969. South Africa can also co-ordinate seizure and confiscation actions with other countries on the basis of bilateral agreements or on a case-by-case basis.

970. The POCA provides for the setting up of a Criminal Assets Recovery Account in the National Revenue Fund into which the net proceeds of confiscated property are deposited. Funds must be used for law enforcement purposes or to assist organisations that assist the victims of crime.

971. South Africa is able in terms of the ICCMA to share confiscated assets with countries involved in co-ordinated law enforcement actions. The general rule in terms of the ICCMA is that the amount recovered in terms of a foreign confiscation order, less all expenses incurred in connection with the execution the order is paid over to the requesting state (s.21, ICCMA). The Director-General: Justice and Constitutional Development may enter into an arrangement to the contrary with the requesting state. This is done on an *ad hoc* basis. The sharing of assets can also be achieved in terms of mutual legal assistance treaties entered into with other countries.

Additional element

972. The definition of a "foreign confiscation order" in Section 1 of the ICCMA, where a foreign confiscation order means "any order issued by a court or tribunal in a foreign aimed at recovering the proceeds of any crime or the value of such proceeds" is wide enough to include civil forfeiture orders. Hence, the authorities advised that a foreign non-criminal confiscation order can be registered and enforced in South Africa. South Africa has assisted various countries by bringing civil forfeiture applications and repatriating the assets to the foreign jurisdiction.

Resources (Central authority for sending/receiving mutual legal assistance/ extradition requests)

973. The Central Authority, is in the Office of the Director-General: Department of Justice and Constitutional Development.

974. In order to address the mutual legal assistance and extradition requirements, an official within the office of the NDPP has been designated to deal with all matters relating to MLA and Extradition (including such requests which relate to ML and FT). This official is tasked with liaison between the Central Authority (*i.e.* the DG: DoJ & CD) and the prosecution component. The functions in relation hereto are cascaded down to the various Business Units within the NPA and to Regional Level, e.g. nodal points have been established in all the offices of the DPP's country wide.

975. At the on-site meeting, the assessment team was informed that the current strength of the unit or department dealing with mutual legal assistance and extradition matters comprises 13 officers and two support staff. There are plans to recruit 4 more officers.

976. Staff of the Central Authority are required to maintain high professional standards.

977. The Justice College provides regular training on a variety of topics relevant to mutual legal assistance and extradition which training also includes training on money laundering.

978. The assessment team was advised at the on-site meeting that the Chief Directorate: International Legal Relations of the Department of Justice and Constitutional does not keep comprehensive statistics of mutual legal assistance and extradition matters. The statistics provided relate to organized crime, money laundering, financing of terrorism and are estimates.

Number of Mutual Legal Requests received broken down by nature of the request

Organized Crime (Fraud)	1
Money Laundering	14
Financing of Terrorism	0
Illegal military material and nuclear weapons	3
Illicit trafficking in drugs	12
Trafficking in persons	1
Exchange control	1
Number of requests granted	32
Number of requests refused	0

6.3.2 Recommendations and Comments

979. South Africa adopts a flexible approach in dealing with MLA requests, and it is able to render a wide range of mutual legal assistance. Under the ICCMA, South Africa is able to render assistance without the need for a treaty or agreement, and there is also no requirement for dual criminality or, where the request is to obtain evidence, there is no requirement that judicial proceedings should have already been instituted before assistance can be rendered. ICCMA does not mandate any grounds of refusal which can be invoked by the Minister, nor does it regulate how the Minister should exercise his discretion whether or not to approve or accede to the request.

980. Of the current heads of assistance mentioned in the ICCMA, some gaps or efficiency issues have also been identified. These relate to the process of obtaining evidence and documents under s 8(1) of the ICCMA which when compared to similar provisions in Section 205 of the CPA may not be the most efficient way of rendering assistance for a request to produce the evidence. Unlike Section 205 CPA, there is no provision to dispense with the presence of witnesses subpoenaed under s 8(1) of the ICCMA even if such witnesses are willing and able to produce the documents in question way before hand. The South African authorities should consider having a similar provision along the lines of Section 205 of the CPA in Section 8(1) of the ICCMA so as to make it simpler for routine production orders.

981. In the case of foreign restraint orders, it is noted that South Africa can render assistance only if such orders have been made final – *i.e.* that the order is not subject to appeal or review. Given that the purpose of a restraint order is to prevent dissipation of proceeds, the requirement that such orders must have been finalised potentially creates a loophole that a defendant faced with such an order may exploit with regard to his proceeds in South Africa. Measures should therefore be taken to address this issue.

6.3.3 Compliance with Recommendations 36 to 38 and Special Recommendation V

	Rating	Summary of factors relevant to s.6.3 underlying overall rating
R.36	LC	• Enforcement of foreign restraint order may be made only where such orders are not subject to any review or appeal. • Effectiveness: Section 8 (on obtaining of evidence) does not dispense with the presence of a witness subpoenaed to appear before a court to give evidence where such witness is able to provide the evidence before the date set down for the hearing.
R.37	C	• This Recommendation is fully observed.
R.38	LC	• Enforcement of foreign restraint order may be made only where such orders are not subject to any review or appeal.
SR.V	LC	• The deficiencies highlighted in relation to R. 36 also impact SR. V. • The deficiencies highlighted in relation to R. 38 also impact SR. V.

6.4 Extradition (R.37, 39, SR.V)

6.4.1 Description and Analysis

Recommendation 39

982. The South African Extradition Act provides for extradition in respect of "extraditable offences" namely offences which in terms of South African law and the law of the foreign State, are punishable with a sentence of imprisonment for a period of six months or more. This would include the money laundering offences under the POCA.

983. South Africa has signed extradition agreements with the following countries: Algeria, Argentina, Australia, Botswana Canada, Egypt (in force 2003), India (in force 2005), Iran, Israel, Lesotho (in force 2003), Malawi, Nigeria, Peoples' Republic of China (in force 2004), Swaziland, and the United States of America. It should be noted that extradition is not dependent on a treaty. Under Section 3(2) of the Extradition Act, the President may in writing consent to the surrender of a fugitive. Under Section 3(3), fugitives may also be surrendered to countries to countries which have been designated pursuant to that Section. Currently, South Africa has designated Ireland, Zimbabwe, Namibia and the United Kingdom.

984. South Africa does not impose a bar on the extradition of its nationals.

985. The ICCMA and Extradition Act do not preclude cooperation between South Africa and a foreign country in procedural and evidentiary matters in order to ensure the efficiency of prosecutions. The South African authorities indicated that any arrangement would have to be made on a case-by-case basis in terms of treaties that may have been entered into with particular countries.

986. The Extradition Act does not contain an expedited process for extradition in terms of which a person may waive his/her right to an extradition hearing. The Extradition Act, however, contains a provision for the waiver of the right of appeal against a magistrate's finding in an extradition hearing.

987. The Extradition Act does not deal with consent to extradition and a waiver of the requirements of the Act. The South African authorities have indicated however, that in terms of the general principles of South African law, there would be no legal obstacle to a person freely and voluntary wanting to surrender himself to a foreign state for prosecution.

988. The Extradition Act provides for a simplified (no-evidence) extradition hearing whereby the magistrate conducting the hearing may accept a statement by a competent authority in the requesting state stating that it has sufficient evidence at its disposal to warrant the prosecution of the person concerned (s.10(2)).

989. Further, and in relation to an extradition request from an "associated State" – *i.e.* a state in Africa which has a reciprocal agreement with South Africa for the execution of a warrant of arrest, a simplified procedure may be adopted whereby the magistrate, if satisfied with the evidence produced before him, can order the surrender of the fugitive who can then be received by the associated State concerned: Section 12(1). This is contrasted with the normal situation of a fugitive from a non-associated State where the magistrate shall only issue an order committing the fugitive to await the Minister's decision with regard to his surrender. In both situations, the fugitive has 15 days to appeal against the order of the magistrate.

Special Recommendation V

990. Terrorist financing is a substantive offence in South African law which means that it falls within the description of an "extraditable offence". In addition, POCDATARA amended the Extradition Act to provide that an extradition request for a terrorist financing offence may not be refused on the sole ground that it concerns a political offence, or an offence connected with a political offence or an offence inspired by political motives, or that it is a fiscal offence.

Additional elements

991. The simplified procedures for extradition hearings apply to all extradition proceedings including proceedings relating to terrorist acts and terrorist financing.

Recommendation 37

992. Section 1 of the Extradition Act reflects the principle of dual criminality in that it requires an offence in terms of South African law and the law of the foreign State, which is punishable with a sentence of imprisonment or other form of deprivation of liberty for a period of 6 months or more. The test for dual criminality is whether the offence in the foreign State is, in essence, the same as a domestic offence. Technical differences between the laws in the requesting and requested states, such as differences in the manner in which each country categorises or denominates the offence do not pose an impediment to the provision of mutual legal assistance.

Statistics

993. The assessment team was advised at the on-site meeting that the Chief Directorate: International Legal Relations of the Department of Justice and Constitutional does not keep comprehensive statistics of mutual legal assistance and extradition matters. The statistics provided relate to organized crime, money laundering and terrorist financing, and are estimates.

Number of Extradition Requests received relating to domestic nationals	0
Number of Extradition Requests received relating to foreign nationals (Money laundering)	1
Number of requests granted relating to domestic nationals	0
Number of requests granted relating to foreign nationals	1
Number of requests refused relating to domestic nationals	0
Number of requests refused relating to foreign nationals	0
Time required to finalise the request	unknown

Extraditions: all offences

	2007	**2008**
All offences	12+	23+

6.4.2 Recommendations and Comments

994. South African extradition law is flexible to the extent that there is no requirement that there must be a treaty between itself and the requesting state before an extradition request can be considered. South Africa can also extradite its own nationals. South Africa should, however, maintain proper statistics for extradition requests, as it is currently not possible to assess the effectiveness of the measures in place.

6.4.3 Compliance with Recommendations 37 & 39, and Special Recommendation V

	Rating	**Summary of factors relevant to s.6.4 underlying overall rating**
R.39	LC	• Effectiveness cannot be assessed.
R.37	C	• This Recommendation is fully observed.
SR.V	LC	• The deficiency highlighted in R. 39 also impacts on SR.V.

6.5 Other Forms of International Co-operation (R.40 & SR.V)

6.5.1 Description and Analysis

Recommendation 40 and Special Recommendation V

995. The Centre, police, and supervisors are able to provide a wide range of international co-operation to foreign counterparts, and generally do so in a rapid, constructive, and effective manner. South Africa does not refuse cooperation on the ground that offences also involve fiscal matters.

996. The provisions and practices for the exchange of information described below apply to all criminal conduct including money laundering and terrorist financing.

FIU to FIU exchange of information

997. The Centre supports wide co-operation and exchange of information amongst Egmont members. This is done on the basis of reciprocity or mutual agreement and following the rules established in the Principles of Information Exchange. To effect the above, the Centre promotes: free exchange of information for purposes of analysis at FIU level; no dissemination or use of the information for any other purpose without prior consent of the providing FIU; and protection of the confidentiality of the information.

998. There are clear and effective gateways to facilitate information exchange with other FIUs. Communication between the Centre and other Egmont FIUs takes place directly via the Egmont Secure Web (ESW). Such exchanges are not made subject to disproportionate or unduly restrictive conditions. The Centre can exchange information upon request or spontaneously, and in relation to ML/FT, and predicate offences.

999. Although the Centre does not require a memorandum of understanding (MOU) to share public information such as company records or addresses, an MOU is required to share STR information. The Centre has MOUs in place with the following Egmont members: Australia, Brazil, Cyprus, Colombia, Israel, Indonesia, Peru, Panama, Russia, and the United Kingdom. The Centre is currently negotiating an MOU with the United States and plans to make more information sharing agreements as more FIUs are established in the region. The Centre has also entered into an information sharing agreement with Zimbabwe, which is not an Egmont member.

1000. The Centre is able to access information from its own databases as well as other databases in the course of executing international requests.

1001. All international requests are submitted in compliance with the Principles for Information Exchange that have been set out by the Egmont Group, considering provisions of information sharing arrangements as set out in agreements amongst the Centre and other FIUs. Requests from counterpart FIUs are dealt with in the same manner as a domestic disclosure, but as a matter of higher priority.

Statistics of requests from foreign FIUs

Received		Disseminated	
Financial year	**Total**	**Financial year**	**Total**
2005/06	75	2005/06	50
2006/07	57	2006/07	49
2007/08	79	2007/08	47

1002. The Centre could not provide statistics on the average time required to respond to requests from foreign FIUs. However, no requests have been refused – *i.e.* in no cases where the Centre had information relevant to a request at its disposal did the Centre refuse to provide such information to a requesting FIU. The Centre made 39 requests in the financial year 2007/2008 and made three spontaneous disclosures to the value of about ZAR 3.6 million (EUR 304 000) to FIUs in other jurisdictions in the financial year 2007/2008. The statistics in the above table were drawn at the end of each respective financial year. The number of requests that were not answered in each of those years (25, 8 and 32) represents requests received in one financial year and responded to in the next.

Police to police exchange of information

1003. The cooperation between the SAPS and foreign police agencies is regulated by police–to-police cooperation agreements which do not fall within the scope of the ICCMA. (The ICCMA provides explicitly that it does not prevent or abrogate or derogate from any arrangement or practice for the provision or obtaining of international co-operation in criminal matters in a manner not provided for by the Act). The police cooperation agreements provide for "informal" cooperation between law enforcement agencies, such as the exchange of information, expertise, training, etc. The agreements cannot be used for purposes of extradition or for the formal facilitating / provision of evidence.

1004. The SAPS has agreements with: Mozambique; Swaziland; Brazil; Russian Federation; France; Argentina; Chile; Hungary; People's Republic of China; Egypt; Nigeria; Portugal; Rwanda; Austria; Iran; Turkey; Bulgaria; Uganda; United Arab Emirates; Malta; the Netherlands; and the so-called SARPCCO (SADC) Countries, namely: Angola, Mozambique, Zambia, Zimbabwe, Tanzania, Malawi, Lesotho, Swaziland, Botswana, Namibia, and Mauritius.

1005. The SAPS send and receive police-to-police cooperation requests via the Interpol Bureau in South Africa. Interpol South Africa is authorised to conduct police-to-police enquiries, and SAPS can respond to requests or provide information spontaneously. There is also continued cooperation between South Africa and the SADC countries in respect of the SARPCCO Agreement relating to police-to-police cooperation. The cooperation also enables the SAPS to hold joint investigations in any other police force's jurisdiction in the SADC region. The cooperation includes investigations that focuses on a wide range of criminality *e.g.* vehicle crime, trafficking etcetera. A further example is the cooperation between China and South Africa and France and South Africa, on a wide range of crimes.

1006. The South African Revenue Service is mandated in terms of domestic legislation to conduct inquiries on investigations of tax evasion cases where it is required for the providing of information on request from foreign tax administrations.

Supervisor to supervisor exchange of information

SARB

1007. The SARB may furnish information to a foreign counterparty (s.89(b), Banks Act) and enter into MOUs with foreign counterparts (s.4(3)). There are not unduly restricted; there are no restrictions on grounds of secrecy and confidentiality, provided that the Registrar is satisfied that the recipient of the information is willing and able to keep the information confidential within the confines of the laws applicable to the recipient. These MOUs allow for (a) the sharing of information upon request or such other times as the parties may agree; and (b) sharing of information on financial crime (which includes by definition AML/CFT). This includes the conducting allowing for conducting inquiries on behalf of foreign counterparts. SARB (BSD) is also part of the SADC Banking Supervisors MOU. SARB has entered into MOUs with the following:

- Argentina (Central Bank of Argentina);
- Australia (Australian Prudential Regulatory Authority);
- Germany (Federal Financial Supervisory Authority);
- Hong Kong (Monetary Authority of Hong Kong);
- Ireland (Irish Financial Services Regulatory Authority);
- Isle of Man (Financial Supervision Commission of the Isle of Man);
- Mauritius (Bank of Mauritius);
- Namibia (Bank of Namibia);
- Nigeria (Central Bank of Nigeria);
- South Africa (Financial Services Board);
- South Africa (Share Transactions Totally Electronic Limited);
- United Kingdom (Financial Services Authority); and
- Dubai (Dubai Financial Services Authority).

1008. BSD is in the process of negotiating MOUs with the following:

- China (Peoples Bank of China);
- France (French Banking Commission);
- India (Reserve Bank of India);
- Lesotho (Central Bank);
- Netherlands (Nederlandsche Bank);

- Swaziland (Central Bank);
- Chinese Taipei (Financial Supervisory Commission);
- United States of America (Federal Reserve Bank of New York); and
- Venezuela (Superintendence of Banks).

1009. Employees of the SARB are not to disclose any information obtained during the course of their duties (s.33, SARB Act), except under circumstances set out under s.89 of the Banks Act.

1010. BSD maintains records and minutes of meetings held with other supervisors pursuant to the MOUs. BSD indicated that it had only been approached once by a foreign supervisor with respect to ML.

FSB

1011. The FSB can conduct inquiries on behalf of foreign counterparts. Section 3A of the Inspection of Financial Institutions Act, 1998 provides that the Executive Officer of the FSB may at any time instruct an inspection pursuant to and for the purposes of implementation of any agreement, communiqué or memorandum of understanding contemplated in Section 22(2)(b) of the FSB Act of the affairs of any person referred to in or identified by the requesting authority and who is present or resident in the Republic of South Africa.

1012. Section 22(2)(b) of the Financial Services Board Act provides that the Executive Officer may disclose to any foreign financial or investment services regulatory or supervisory authority information relating to a particular financial or other institution or financial or other service or a particular individual who is or was involved in a particular financial institution or financial service, if he is of the opinion that such information will be of importance to the relevant regulatory or supervisory authority.

1013. Although the FSB does not need an MOU to exchange information, the FSB has concluded MOUs with:

AUTHORITY	DATE
1. United States Securities and Exchange Commission – Communiqué	March 1995
2. United Kingdom Securities and Investment Board (now the Financial Services Authority)*	October 1995
3. Securities and Exchange Commission of the Republic of China (Chinese Taipei)**	March 1996
4. United States Commodity Futures Trading Commission – Communiqué	May 1997
5. Securities Commission of Malaysia	October 1997
6. Superintendencia De Valores Y Seguros of Chile	May 1998
7. Securities and Futures Commission of Hong Kong	September 1998
8. Registrar of Banks, South African Reserve Bank	December 1998
9. Comisión Nacional De Valores of Argentina	May 1999
10. Australian Securities and Investments Commission	May 1999
11. Financial Supervision Commission of the Isle of Man	October 1999
12. Comissão do Mercado De Valores Mobiliários of Portugal	October 1999
13. Bank of Mozambique	November 1999

AUTHORITY	DATE
14. Securities and Exchange Commission of the Republic of Zambia	November 1999
15. Central Bank of Swaziland	November 1999
16. Guernsey Financial Services Commission	May 2000
17. Jersey Financial Services Commission	May 2000
18. The Insurance Supervisory Department of the United Republic of Tanzania	June 2000
19. Central Bank of Lesotho	June 2000
20. Commission De Surveillance Du Secteur Financier (Grand-Duchy of Luxembourg)	September 2000
21. Reserve Bank of Malawi	September 2000
22. Commission Des Operations De Bourse of France	October 2000
23. The Office of the Securities Exchange Commission of Thailand	November 2000
24. The Ministry of Finance and Development Planning of Botswana	April 2001
25. The Namibia Financial Institutions Supervisory Authority	April 2001
26. The Capital Markets and Securities Authority of Tanzania	April 2001
27. The Ministry of Finance of Zimbabwe	April 2001
28. The Monetary Authority of Singapore	June 2001
29. Comissão de Valores Mobiliários of Brazil	June 2001
30. The National Bank of Angola	October 2001
31. The Ministry of Finance of Mozambique (The Insurance General Inspection)	October 2001
32. Bundesaufsichtsamt Für Den Wertpapierhandel (Germany)	October 2001
33. Ministry of Finance of Swaziland	October 2001
34. Securities and Exchange Commission of Nigeria	March 2002
35. Commissione Nazionale Per Le Societa E La Borse of Italy	May 2002
36. Hellenic Capital Market Commission, Greece	October 2002
37. China Securities Regulatory Commission	October 2002
38. Office of the Registrar of Pension, Insurance of Zambia	October 2003
39. The Financial Services Commission of Mauritius	October 2003
40. The Financial Services Authority, United Kingdom*	January 2004
41. Capital Markets Authority of the Republic of Uganda	April 2004
42. The Ministry of Finance and Development Planning of Botswana	October 2004
43. Bermuda Monetary Authority	August 2005
44. Israeli Securities Authority	October 2005
45. Securities and Exchange Commission of Ghana	June 2006
46. Financial Supervisory Commission of Chinese Taipei	September 2006
47. Emirate Securities and Commodities Authority	April 2007
48. Dubai Financial Services Authority	May 2008

1014. The FSB abides by the provisions of applicable MOUs and bilateral agreements. International cooperation is co-ordinated through the Executive Committee of the FSB on which the four deputy executive officers abides by the provisions of applicable MOU's and bilateral agreements.

1015. The FSB can provide information upon request or spontaneously, and in relation to ML/FT, and predicate offences.

1016. The FSB, where it receives requests for assistance in conducting inquiries/investigations or to provide information from foreign counterparts will undertake the necessary actions of inquiry or inspection in so far as the subject entities or persons operate as financial institutions or render financial services within the geographical territory of the Republic of South Africa.

1017. The FSB is also a signatory to the International Organisation of Securities Commissions' (IOSCO) Multilateral Memorandum of Understanding. The FSB can exchange information relating to ML/FT using these bilateral and multilateral MOUs, as these agreements are wide enough to encompass the exchange of any relevant information. Requests for information from JSE would (and has) come through this mechanism.

1018. The National Gambling Board also indicated that it often cooperates and shares information with foreign counterparts. For example, it liaises with a foreign authority if it receives an application from another jurisdiction and is considering granting a local license to a potential non-South African owner. NGB is also a member of the International Association of Gambling Regulators as well as the permanent secretary and founding member of the Gambling Regulators Africa Forum.

Recommendation 32

1019. FSB keeps copies of documentation relating to supervisors' international cooperation, *i.e.* requests made and requests received form foreign regulatory authorities. Furthermore, the FSB is required to provide the Screening Group of IOSCO (for submission to IOSCO's Monitoring Group) with information on foreign requests received, the nature of such requests (according to the types of requests as listed in the IOSCO Multilateral MOU) and the response time per request. This information is summarized per signatory of the IOSCO Multilateral MOU and submitted to IOSCO's Monitoring Group. The purpose of the Monitoring Group is to monitor the operation of the IOSCO Multilateral MOU, *i.e.* to identify those jurisdictions that are not able or not willing to cooperate with their foreign counterparts. No requests were specifically related to ML/FT. However, some of the information requested could be related to ML/FT.

INTERNATIONAL REQUESTS RECEIVED FOR INFORMATION	
Date of request	**Authority**
25 February 2005	United States Securities and Exchange Commission (SEC)
18 March 2005	Financial Supervision Commission Isle of Man
12 April 2005	Financial Services Authority (UK)
9 June 2005	Australian Securities and Investments Commission (ASIC)
31 August 2005	US Commodity Futures Trading Commission (CFTC)
27 October 2005	United States Securities and Exchange Commission (SEC)
30 November 2005	Australian Securities and Investments Commission (ASIC)
Subtotal	**7**
2 January 2006	Commission de Surveillance du Secteur Financier (Luxembourg)

INTERNATIONAL REQUESTS RECEIVED FOR INFORMATION	
Date of request	**Authority**
24 January 2006	Securities and Futures Commission Hong Kong
8 February 2006	US Commodity Futures Trading Commission (CFTC)
12 April 2006	Guernsey Financial Services Commission
26 May 2006	Irish Financial Services Regulatory Authority
13 July 2006	Jersey Financial Services Commission
23 August 2006	US Commodity Futures Trading Commission (CFTC)
05 September 2006	Irish Financial Services Regulatory Authority Irish Financial Services Regulatory Authority
19 September 2006	Dubai Financial Services Authority
25 September 2006	British Columbia Securities Commission
26 October 2006	Irish Financial Services Regulatory Authority Irish Financial Services Regulatory Authority
3 November 2006	Australian Securities and Investments Commission (ASIC)
6 November 2006	Jersey Financial Services Commission
8 November 2006	Jersey Financial Services Commission
8 November 2006	Jersey Financial Services Commission
9 November 2006	Jersey Financial Services Commission
27 November 2006	New Zealand Securities and Exchange Commission
Subtotal	**17**
22 January 2007	Autorite des Marches Financiers (AMF) – French Securities Regulator
23 January 2007	Irish Financial Services Regulatory Authority
1 March 2007	United States Securities and Exchange Commission (SEC)
9 March 2007	Jersey (Financial Services Commission)
14 March 2007	Monetary Authority of Singapore
18 May 2007	Commission de Surveillance du Secteur Financier (Luxembourg)
22 May 2007	Securities Commission New Zealand
8 June 2007	Financial Services Authority (UK)
28 June 2007	Commission de Surveillance du Secteur Financier (Luxembourg)
6 July 2007	Guernsey Financial Services Commission
30 July 2007	Financial Services Authority (UK)
14 August 2007	Financial Regulator Ireland
24 August 2007	Lusaka
27 August 2007	United States Securities and Exchange Commission (SEC)
26 November2007	Financial Supervision Commission Isle of Man
28 December 2007	Irish Financial Services Regulatory Authority
Subtotal	**16**
7 January 2008	Irish Financial Services Regulatory Authority

INTERNATIONAL REQUESTS RECEIVED FOR INFORMATION	
Date of request	**Authority**
9 May 2008	Guernsey Financial Services Commission
30 June 2008	Financial Services Authority (UK)
1 July 2008	Commission de Surveillance du Secteur Financier (Luxembourg)
17 July 2008	Dubai Financial Services Authority
18 July 2008	Commission de Surveillance du Secteur Financier (Luxembourg)
29 July 2008	Australian Securities and Investments Commission (ASIC)
6 August 2008	Guernsey Financial Services Commission
12 August 2008	Bank of Botswana
1 September 2008	Israeli Securities Authority
Subtotal	**10**
GRAND TOTAL	**50**

Additional elements

1020. The information contained in the Centre's own database which could be provided in a response to a request from a foreign counterpart can include information contained in STRs, additional information relating to a reported transaction and public record information.

6.5.2 Recommendations and Comments

1021. This Recommendation is fully observed.

6.5.3 Compliance with Recommendation 40 and Special Recommendation V

	Rating	Summary of factors relevant to s.6.5 underlying overall rating
R.40	C	This Recommendation is fully observed.
SR.V	LC	With regards to these elements, this Recommendation is fully observed.

7. OTHER ISSUES

7.1 Resources and statistics

1022. The text of the description, analysis and recommendations for improvement that relate to Recommendations 30 and 32 is contained in all the relevant Sections of the report i.e. all of Section 2, parts of Sections 3 and 4, and in Section 6. There is a single rating for each of these Recommendations, even though the Recommendations are addressed in several Sections.

	Rating	Summary of factors relevant to Recommendations 30 and 32 and underlying overall rating
R.30	LC	<u>Law enforcement and prosecutors</u> • The NPA experiences challenges with attracting and appointing qualified applicants.
R.32	PC	• South Africa has not reviewed the effectiveness of its systems for combating money laundering and terrorist financing on a regular basis. • The assessment team was not provided with comprehensive data or statistics on details of money laundering investigations. The authorities do not maintain comprehensive statistics on the criminal sanctions applied to person convicted of money laundering cases. • No statistics are maintained concerning the number of cases and the amounts of property frozen, seized, and confiscated in relation to money laundering and terrorist financing. • There are no adequate statistics on cross border transportations of currency and BNI over the thresholds. • South Africa does not keep comprehensive statistics of mutual legal assistance and extradition matters.

TABLES

Table 1: Ratings of Compliance with FATF Recommendations
Table 2: Recommended Action Plan to improve the AML/CFT system
Table 3: Authorities' Response to the Evaluation (if necessary)

Table 1: Ratings of Compliance with FATF Recommendations

The rating of compliance vis-à-vis the FATF Recommendations should be made according to the four levels of compliance mentioned in the 2004 Methodology (Compliant (C), Largely Compliant (LC), Partially Compliant (PC), Non-Compliant (NC)), or could, in exceptional cases, be marked as not applicable (NA).

Forty Recommendations	Rating	Summary of factors underlying rating
Legal systems		
1. ML offence	LC	• Section 6 POCA (acquisition, use and possession) does not extend to the perpetrator of the predicate offence. • Lack of more comprehensive statistics makes it difficult to assess the effectiveness of the anti-money laundering regime.
2. ML offence – mental element and corporate liability	LC	• Lack of more comprehensive statistics makes it difficult to assess the effectiveness of the anti-money laundering regime.
3. Confiscation and provisional measures	C	• This Recommendation is fully observed.
Preventive measures		
4. Secrecy laws consistent with the Recommendations	C	• This Recommendation is fully observed.
5. Customer due diligence	PC	• No specific legal obligation for an accountable institution to undertake CDD when there is a suspicion of money laundering or terrorist financing or when it has doubts about the veracity or adequacy of previously obtained customer identification data. • The FIC Act does not require accountable institutions to verify the identification information relating to directors and senior management by comparison with the CM29 form filed with CIPRO. • No specific requirement in law or regulation that requires accountable institutions to identify beneficial owners (*i.e.* the natural persons who ultimately controls and owns the customer) or to verify their identities. Therefore, there is no obligation to identify the beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. • No specific requirement to understand the ownership and control structure of a customer that is a legal person or arrangement, beyond the requirements described above to identify: the manager and 25% shareholders of a company; the members of a close corporation; the partners in a partnership; and the founders, trustees

Forty Recommendations	Rating	Summary of factors underlying rating
		and beneficiaries of a trust. • No explicit requirement that information on the purpose of a business relationship be obtained. • There is no explicit requirement to conduct on-going due diligence. • There is no specific requirement that accountable institutions apply enhanced due diligence for higher risk categories of customers, business relationships or transactions. • Certain exemptions do not comply with the FATF Recommendations in that they fully exempt certain accountable institutions from all CDD requirements (as well as some or all record keeping requirements). In addition: o For insurance exemptions, the annual and single premium thresholds greatly exceed the examples cited in the FATF methodology of the types of insurance policies that may be considered low risk. o A further concern is that the full exemptions from CDD and related record keeping in Exemptions 7, 15 and 16 would also apply in cases where an accountable institution is considering filing a suspicious transaction report. • Once a business relationship has been established, there is no specific requirement to terminate the business relationship or to consider filing an STR if doubts about the veracity or adequacy of previously obtained customer identification data arise. • Uncovered Financial Institutions are not subject to the CDD obligations of the FIC Act.
6. Politically exposed persons	NC	• No enforceable obligation for financial institutions to identify politically exposed persons (PEPs) or take other such as measures as indicated in Recommendation 6.
7. Correspondent banking	NC	• There is no specific obligation in law or regulation for accountable institutions to conduct enhanced due diligence on cross border correspondent banking and other similar relationships.
8. New technologies & non face-to-face business	PC	• There are no specific legal or regulatory requirements to have policies in place to address the potential abuse of new technological developments for ML/FT. • The general requirements for non face-to-face customers do not extend to when conducting on-going due diligence. Additionally, there is no elaboration of how this general requirement should be applied other than in the context of the banking sector and in relation to cell phone products. • Uncovered Financial Institutions are not subject to the CDD obligations of the FIC Act.
9. Third parties and introducers	NC	• Exemption 5 does not require the institution relying on third-party verification/identification to immediately obtain the relevant CDD information. • Exemption 5 does not require the accountable institution 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.” • For Exemption 5, there is no explicit requirement that the financial institution satisfy itself of the adequacy of applicable AML/CFT measures applicable to the foreign financial institution. • Despite the lack of determinations by relevant supervisory bodies, some accountable institutions are applying Exemption 5 and fully exempting from verification requirements all customers from FATF membership countries. • Uncovered Financial Institutions are not subject to the CDD obligations of the FIC Act.
10. Record keeping	PC	• There is not a specific requirement that the transaction records include the date of the transaction or the address of the customer.

Forty Recommendations	Rating	Summary of factors underlying rating
		• Outside of the banking sector, there is no general obligation to keep transaction records sufficient to permit the reconstruction of account activity. • No requirement to maintain account files or business correspondence as part of the record-keeping obligation. • Effective application of the record keeping obligations is eroded by Exemptions 4, 6, 14, 16 and 17 which exempt accountable institutions from maintaining records of customer identification and verification. • Uncovered Financial Institutions are not subject to the record keeping obligations of the FIC Act. This affects the ratings for Recommendation 10.
11. Unusual transactions	PC	• The FIC Act does not contain a provision which expressly requires financial institutions to pay special attention to transactions based on complexity, size or unusual patterns. • No requirement to make a record that includes customer and transaction information for complex and unusually large transactions or unusual patterns of transactions or to prepare written findings and to maintain them unless it is part of an STR. • Since there is no requirement to prepare any written findings concerning the background and purpose of transactions with no apparent business of lawful purpose, there can be no requirement to keep them available for at least five years. • The obligation to pay attention to transactions with no apparent business or lawful purpose should be extended to Uncovered Financial Institutions.
12. DNFBP – R.13-15 & 21	NC	• The deficiencies identified in R.5, 6, and 8-11 that apply in the financial sector also apply to all DNFBPs. • Scope issues further reduce the application of the requirements of R.5 and R.8-11 in that: accountants are not covered when conducting all of the activities prescribed in R.12 and the applicability of the requirements when providing investment advice is not clear to the industry; attorneys are not covered when performing company services in relation to legal persons and arrangements within South Africa; the majority of dealers in precious metals and stones sector are not covered and the others are only subject to limited CDD and record keeping requirements; and trust and company service providers (other than lawyers or accountants providing investment advice) are not covered in the situations specified in R.12. • Applying R.5: Casinos are permitted to apply reduced CDD in all cases, and this was not based on demonstrated low risk. In particular, casinos are fully exempt from collecting and verifying the residential address and income tax registration number of natural persons (Exemption 14). Exemption 10 for attorneys does not comply with the FATF Recommendations in that it fully exempts attorneys from all CDD requirements (as well as some or all record keeping requirements) even where there is a suspicion of ML/FT. • Applying R.9: The characteristics of the real estate market (often cash-based) make it troubling that the full range of preventative measures required by Recommendation 9 do not apply to non-face-to-face transactions in the real estate sector. • Applying R.10: (Dealers): Only very limited information on limited transactions is recorded. • Effectiveness: The results of the EAAB inspection process show that, overall, implementation of AML/CFT measures, including CDD requirements, is low among estate agents.

Forty Recommendations	Rating	Summary of factors underlying rating
13. Suspicious transaction reporting	LC	• Leasing and financing companies have not yet implemented the reporting obligations.
14. Protection & no tipping-off	C	• This Recommendation is fully observed.
15. Internal controls, compliance & audit	PC	• For financial institutions other than banks, there is not a requirement that the compliance officer be at the management level. • Other than for banks, there is no requirement for accountable institutions to maintain an adequately resourced and independent audit function to test compliance (including sample testing) with AML/CFT procedures, policies and controls. • There is no general requirement for financial institutions to put in place screening procedures to ensure high standards when hiring all employees. • There is no requirement that training be conducted on an ongoing basis. • Uncovered Financial Institutions are not subject to FIC Act requirements relating to internal controls.
16. DNFBP – R.13-15 & 21	PC	• Applying R.13 and SR.IV: o Effectiveness: Implementation of the reporting obligation is negatively affected as follows: 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; for dealers, there has been very low rates of reporting in contrast to the relative importance of the sector in the South African context; and for estate agents, until recently it was not widely recognised that property transactions effected in cash are suspicious. Additionally, the EAAB has detected some activity in the estate agent sector which should have been reported (but was not) and which is suspected of relating to ML. • Applying R.15 and R.21: The deficiencies identified in R.15 that apply in the financial sector also apply to all DNFBPs.
17. Sanctions	PC	• Sanctions are not sufficiently effective and proportionate. Only criminal sanctions can apply for breaches of the FIC Act. • There is no specific authority for SARB, FSB, or JSE, to apply administrative sanctions for breaches of the FIC Act. • Scope issue: The following financial institutions are not subject to AML/CFT supervision: finance companies; leasing companies; collective investment scheme custodians; money lenders other than banks; securities custodians licensed under the FAIS Act, Postbank and members of the Bond Exchange. • Effectiveness: Low level of compliance with AML/CFT requirements in the insurance sector, and among securities market participants. No sanctions have been applied, even though breaches of AML/CFT requirements detected.
18. Shell banks	PC	• There is no direct prohibition on financial institutions from entering into, or continuing, correspondent banking relationships with shell banks. • No requirement that financial institutions satisfy themselves that respondent financial institutions in a foreign country do not permit their accounts to be used by shell banks.
19. Other forms of reporting	C	• This Recommendation is fully observed.
20. Other NFBP & secure transaction techniques	C	• This Recommendation is fully observed.
21. Special attention for higher risk countries	NC	• No specific requirement for financial institutions to give special attention to business relationships and transactions with persons

Forty Recommendations	Rating	Summary of factors underlying rating
		from or in countries which do not or insufficiently apply the FATF Recommendations. • Efforts to inform the financial sector about the risks of certain jurisdictions were directed only to banks. • No explicit requirement for a person to examine such transactions and prepare written findings (other than an STR) that can be made available to competent authorities and auditors. • No requirements to apply counter-measures in situations where countries do not sufficiently apply the FATF Recommendations. • The obligation to pay attention to transactions with no apparent business or lawful purpose should be extended to Uncovered Financial Institutions.
22. Foreign branches & subsidiaries	NC	• There is no direct requirement for South African financial institutions to ensure that their 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 is there a requirement to apply the higher of the requirements if South African and host country requirements differ. • There are serious deficiencies in South Africa's framework for preventative measures for financial institutions, so applying the South Africa standards would not be consistent with the FATF Recommendations. • There is no specific requirement to inform the South African authorities if a foreign branch or subsidiary is unable to observe appropriate AML/CFT measures. • Uncovered Financial Institutions are not subject to FIC Act requirements relating to foreign branches and subsidiaries.
Institutional and other measures		
23. Regulation, supervision and monitoring	PC	• For financial service providers, insurers and CIS, fit and proper tests do not apply to all directors. • There is no legal requirement to submit directors and senior management of long-term insurers to fit and proper tests. • Market entry (banks, securities market participants): adequate measures not taken to determine beneficial ownership or (for JSE) go beyond the 10% if the shareholder is a legal person. • The JSE Rules do not currently specify that persons holding a management function meeting the fit and proper criteria, and they do not currently include "expertise" as a criteria. • No registration/licensing requirements apply to natural or legal persons conducting money/value transfer within South Africa, financial leasing and finance companies. • There is no designated AML/CFT supervisor for Postbank or the Bond Exchange. • Certain types of remittances through informal systems not covered. • Scope issue: The following financial institutions are not subject to AML/CFT supervision: finance companies; leasing companies; collective investment scheme custodians; money lenders other than banks; securities custodians licensed under the FAIS Act, Postbank and members of the Bond Exchange. • Effectiveness: Low level of compliance with AML/CFT requirements in the insurance sector, and among securities market participants. No sanctions have been applied, even though breaches of AML/CFT requirements detected. The largest provider of money remittance services in South Africa has not yet been visited for an AML/CFT review, despite having reported the vast majority of total STRs. Insufficient resources for SARB (BSD and

Forty Recommendations	Rating	Summary of factors underlying rating
		ExCon) and FSB, given the number of entities that they supervise.
24. DNFBP - regulation, supervision and monitoring	PC	• The FIC Act currently only provides for enforcement of its provisions through criminal sanctions, none of which have yet been applied. Administrative sanctions will not be available under the FIC Act until the Amendment Bill comes into force. • The designations of the NGB, IRBA and LSSA as supervisory bodies are problematic. • The FIC Act-designated supervisory authorities for casinos (National Gambling Board), attorneys (Law Society of South Africa), and estate agents (Estate Agency Affairs Board) do not have specific authority to inspect for compliance or apply sanctions in respect to the FIC Act. • ***Dealers in precious metals and stones:*** It is a major vulnerability is that there is no industry-wide supervisory body to ensure compliance with the FIC Act. • ***Company service providers:*** Only company service providers that are lawyers or accountants have a designated AML/CFT supervisor; and the existing framework in relation to attorneys applies only when they are providing services for companies outside of South Africa. • ***Casinos:*** None of the provincial licensing authorities (PLAs) has yet been required or requested to exercise its authority to apply sanctions for violations of the FIC Act requirements. • ***Attorneys:*** Currently, the regional law societies (RLS) are not routinely checking for compliance with the FIC Act, and they do not have specific powers to impose sanctions in accordance with the FIC Act. • ***Accountants:*** The IRBA does not have clear authority to supervise auditors beyond ensuring their compliance with the AP Act, and its supervision would only extend to a relatively small number of accountants. • Auditors providing investment advice, also fall under the supervisory jurisdiction of the FSB. As there is no co-ordination between FSB and IRBA inspections, there is the possibility of overlap in this regard. • ***Trust service providers:*** The providers are generally attorneys and banks. However, the supervisory framework described above in relation to attorneys applies only when they are providing services for trusts outside of South Africa. For banks, the supervisory framework and identified deficiencies described in Section 3.10 of this report apply.
25. Guidelines & Feedback	PC	• The current STR reporting guidelines are not sector specific, and the reporting requirements and reporting forms are mainly designed for banks. • The Centre has not provided general feedback on the methods and trends of money laundering, or sanitised ML cases. • Guidance Note 3 only applies to banks and comprehensive guidance on FIC Act requirements to other financial sectors has not been issued. • The guidance does not contain a description of ML/FT techniques and methods. • Guidance Note 3 only applies to banks and comprehensive guidance on FIC Act requirements to other financial sectors has not been issued. • The guidance does not contain a description of ML/FT techniques and methods. • AML/CFT guidance, although developed by the Centre in consultation with the NGB and casino industry, has not been issued for casinos (or dealers in precious metals and stones, or trust and company service providers that are not attorneys or

Forty Recommendations	Rating	Summary of factors underlying rating
		accountants**,** although these sectors are not subject to national AML/CFT requirements).
Institutional and other measures		
26. The FIU	LC	• No annual reports concerning AML/CFT cases, typologies and trends analysis have yet been issued or published.
27. Law enforcement authorities	LC	• Effectiveness: Lack of more comprehensive statistics makes it impossible to assess the effectiveness of the money laundering regime; the information provided shows a low number of money laundering investigations.
28. Powers of competent authorities	C	• This Recommendation is fully observed.
29. Supervisors	PC	• There is not clear authority for the FSB to inspect for compliance, conduct on-site visits, and obtain information to determine compliance with the FIC Act. • For insurers and FSPs, the FSB does not have general authority to conduct visits in relation to AML compliance, and does not use the broad powers under the IFI Act to conduct inspections. There is no specific authority for SARB, FSB, or JSE, to apply administrative sanctions for breaches of the FIC Act. • Scope issue: The following financial institutions are not subject to AML/CFT supervision: finance companies; leasing companies; collective investment scheme custodians; money lenders other than banks; securities custodians licensed under the FAIS Act, Postbank and members of the Bond Exchange.
30. Resources, integrity and training	LC	<u>Law enforcement and prosecutors:</u> • The NPA experiences challenges with attracting and appointing qualified applicants.
31. National co-operation	C	• This Recommendation is fully observed.
32. Statistics	PC	• South Africa has not reviewed the effectiveness of its systems for combating money laundering and terrorist financing on a regular basis. • The assessment team was not provided with comprehensive data or statistics on details of money laundering investigations. The authorities do not maintain comprehensive statistics on the criminal sanctions applied to person convicted of money laundering cases. • No statistics are maintained concerning the number of cases and the amounts of property frozen, seized, and confiscated in relation to money laundering and terrorist financing. • There are no adequate statistics on cross border transportations of currency and BNI over the thresholds. • South Africa does not keep comprehensive statistics of mutual legal assistance and extradition matters.
33. Legal persons – beneficial owners	NC	• There are limited measures in place to ensure that there is adequate, accurate, and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. • Shareholders can be legal persons, and nominees, which may obscure beneficial ownership information. • Information in the company registers pertains only to some legal ownership and control; it does not necessarily contain information concerning beneficial ownership and control; the information is not verified and is not necessarily reliable. • For cooperatives, it is not specified what information on directors

Forty Recommendations	Rating	Summary of factors underlying rating
		must be supplied or updated, and they may also be legal persons. • It is unclear whether the measures to prevent share warrants to bearer to be misused for money laundering are sufficient.
34. Legal arrangements – beneficial owners	PC	• Where a legal person is a founder, trustee or beneficiary, there is no obligation to obtain information on the beneficial owner of a legal person. • Identification information on the founder and beneficiary is not verified by the trust register. • No records exist of the 2 000 trusts that were created prior to 1987 when the TPC Act came into effect.
International Co-operation		
35. Conventions	LC	• Palermo: Section 6 POCA (acquisition, use and possession) does not apply to the person who committed the predicate offence as required by the Palermo Convention 6(1)(b)(i) and 6(2)(e). • FT Convention: South Africa does not fully comply with Article 18(1), which requires countries to implement sufficient measures to identify customers in whose interest accounts are opened (see Section 3.2 of this report).
36. Mutual legal assistance (MLA)	LC	• Enforcement of foreign restraint order may be made only where such orders are not subject to any review or appeal. • Effectiveness: Section 8 (on obtaining of evidence) does not dispense with the presence of a witness subpoenaed to appear before a court to give evidence where such witness is able to provide the evidence before the date set down for the hearing.
37. Dual criminality	C	• This Recommendation is fully observed.
38. MLA on confiscation and freezing	LC	• Enforcement of foreign restraint order may be made only where such orders are not subject to any review or appeal.
39. Extradition	LC	• Effectiveness cannot be assessed.
40. Other forms of co-operation	C	• This Recommendation is fully observed.
Nine Special Recommendations	**Rating**	**Summary of factors underlying rating**
SR.I Implement UN instruments	LC	• *FT Convention*: South Africa does not fully comply with Article 18(1), which requires countries to implement sufficient measures to identify customers in whose interest accounts are opened (see Section 3.2 of this report).
SR.II Criminalise terrorist financing	LC	• The effectiveness cannot be assessed.
SR.III Freeze and confiscate terrorist assets	PC	• No mechanism for effectively communicating freezing actions taken pursuant to S/RES/1373(2001) to those accountable institutions and others who do not qualify as “interested parties” at the time the freezing order is obtained. • No guidance has been issued. • There is not adequate monitoring for compliance by all financial institutions. • Effectiveness concerns: Although the system remains untested, effectiveness concerns remain in the absence of clear communication mechanisms and guidance to accountable institutions, particularly in relation to freezing actions pursuant to S/RES/1373(2001). • For S/RES/1267(1999), No mechanism for bringing delisting

Forty Recommendations	Rating	Summary of factors underlying rating
		requests to the attention of the UNSC for consideration, or 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).
SR.IV Suspicious transaction reporting	LC	• Leasing and financing companies have not yet implemented the reporting obligations.
SR.V International co-operation	LC	• The deficiencies highlighted in relation to R. 36 also impact SR. V. • The deficiencies highlighted in relation to R. 38 also impact SR. V. • The deficiency highlighted in R. 39 also impacts on SR.V.
SR VI AML requirements for money/value transfer services	PC	• There is no requirement for an MVT service operator that conducts operations within South Africa to be licensed or registered. • MVT service operators are not subject to the full range of the applicable FATF Recommendations. • The systems in place to monitor and ensure compliance for banks are not adequate and there is no designated AML/CFT supervisor for Postbank. • There are not effective, proportionate, and dissuasive sanctions that can be applied to MVT service operators that fail adequately comply with provisions of the FIC Act. • No substantial action has been taken to address the informal (underground) sector.
SR VII Wire transfer rules	PC	• There is no general legal requirement for all wire transfers to be accompanied by full originator information. • For domestic transfers, there is no general requirement that, where full originator information does not accompany the wire transfer, such information can be made available to the appropriate authorities within three business days of receiving the request. • No general requirement on intermediary financial institutions to ensure that all originator information that accompanies a wire transfer is transmitted with the transfer. • No obligation on beneficiary financial institutions to consider restricting or terminating the business relationship with financial institutions that fail to meet the requirements of Special Recommendation VII. • No indication that PASA specifically checks for compliance with Rule 2.16 to ensure that financial institutions are indeed entering the originator's name and address (in Field 50a), and account number (in Field 57a in the case of debit transfers) or a reference number (in Field 20) as required. • No indication that compliance with the requirement on beneficiary financial institutions to file an STR in situations where originator information is missing is tested or that any tests are conducted to ensure that the information entered into the fields is accurate and complete. • No specific sanctions associated with failing to include full, accurate and meaningful originator information in a message conveying payment instructions across borders. • Although MoneyGram's agent banks collect full originator information, in practice, not all the information that is collected is transferred to the receiving MoneyGram agent or office outside of South Africa.

Forty Recommendations	Rating	Summary of factors underlying rating
SR.VIII Non-profit organisations	PC	• No assessment of the potential risks of terrorist financing posed within the NPO sector in South Africa has been undertaken yet. • No outreach programme has been undertaken with the specific aim to protect the sector from terrorist financing abuse. • There is no registration requirement under the NPO Act in as much as registration of NPOs is only voluntary. • The Director has neither the power to sanction office bearers of defaulting NPOs nor the power to impose fines or to freeze accounts of NPOs for violation of oversight measures. • There is no prescribed retention period that applies to the record keeping requirement of NPOs. • There is no specific requirement under the NPO Act, for NPOs to maintain for a period of five years information on the identity of person(s) who own, control or direct their activities, including senior officers, board members and trustees. • There are no formal gateways for the Directorate to exchange non-public information.
SR.IX Cross Border Declaration & Disclosure	PC	• The following aspects of SR IX are not covered in the case of cross-border transportations by persons or by mail: inbound BNI and outgoing BNI payable in foreign currency. • There are no records kept when: (i) there is a false declaration or disclosure and there is no seizure; (ii) there is a suspicion of ML/FT; or (iii) there is a cross-border transportation of BNI through uninsured mail. • There is not yet a requirement to report threshold movements of currency to the Centre or make the information available to the FIU in some other way, and bills of entry for cargo and postal declarations are not available to the Centre. • The sanctions for failing to report a cross-border conveyance of cash are not yet in force. • There are concerns about the effectiveness of measures to monitor the incoming declaration obligation.

Table 2: Recommended Action Plan to Improve the AML/CFT System

AML/CFT System	Recommended Action (listed in order of priority)
1. General	
2. Legal System and Related Institutional Measures	
2.1 Criminalisation of Money Laundering (R.1 & 2)	• It is recommended that South Africa amend Section 6 of POCA in order to extend the ML offence of acquisition, possession and use to a person who committed the predicate offence. • South African authorities should consider amending POCA to regularise and standardise ss. 4-6 with ss.2-9 for avoidance of doubt. • The lack of more comprehensive statistics and data maintained by the relevant authorities is another area which the South African authorities should also address.
2.2 Criminalisation of Terrorist Financing (SR.II)	• The maximum term of imprisonment for an offence under the POCDATARA is 15 years whereas the offence for money laundering under POCA provides for a maximum term of 30 years, while that for racketeering is up to life imprisonment. In view of the serious nature of terrorist financing, the authorities may wish to reconsider this anomaly.
2.3 Confiscation, freezing and seizing of proceeds of crime (R.3)	• While the value of the proceeds confiscated are high, comprehensive statistics and data should be maintained on matters relating specifically to money laundering and terrorist financing
2.4 Freezing of funds used for terrorist financing (SR.III)	• Africa should implement effective mechanisms for communicating freezing actions to accountable institutions and others who do not qualify as “interested parties” at the time the freezing order is obtained. The South African authorities should also issue guidance to the financial sector on how to meet its obligations pursuant to Special Recommendation III. • The authorities should enhance their monitoring of all financial institutions for their compliance with these obligations. • South Africa should also implement a mechanism to bring a delisting request to the attention of the UNSC for consideration, 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).
2.5 The Financial Intelligence Unit and its functions (R.26)	• The Centre’s should publish information concerning AML/CFT cases, typologies and trends analysis. • The Centre should consider tailoring STR forms to meet the needs of the non-bank reporting parties. Additionally, the Centre should issue sector-specific guidance concerning the reporting obligation.
2.6 Law enforcement, prosecution and other competent authorities (R.27 & 28)	• The South African authorities should focus more pro-actively on pursuing specific money laundering offences. • South Africa should consider additional guidance to law enforcement on obtaining production of privileged documents. • It is recommended that the SAPS consider developing its own expertise in forensic analysis (e.g. in accounting and auditing) as expertise in these fields will always be required in analysing ML and FT trends. There is also need to appoint more prosecutors and provide them with a more skills-based through training. • The SAPS should consider maintaining statistics on cases where special investigative techniques are used (e.g. controlled deliveries and undercover operations). This would enable effectiveness of the use of such techniques to be determined.

AML/CFT System	Recommended Action (listed in order of priority)
2.7 Cross Border Declaration & Disclosure	• There is need for South Africa to establish more effective measures to monitor all incoming and outgoing cross-border transportations of currency and BNI, and establish clearer requirements and procedures to declare inbound BNI above the threshold, and outgoing BNI payable in foreign currency. • The proposed amendments to the FIC Act which will enhance that process (including amendments which will make declaration reports available to the Centre and impose sanctions for failing to report cross-border conveyances of currency) should quickly be brought into effect. • There is need for the SAPS to retain readily available records and comprehensive records where there is a false declaration or disclosure and there is no seizure, and when there is a suspicion of ML/FT. • There should also be more detailed statistics of seizures done according to the offence committed, statistics on seizures relating to tax evasion involving ML, and illegal cross-border transportation of cash.
3. Preventive Measures – Financial Institutions	• South African authorities should extend AML/CFT requirements to the currently uncovered financial institutions.
3.1 Risk of money laundering or terrorist financing	• There are no recommendations for this Section.
3.2 Customer due diligence, including enhanced or reduced measures (R.5 to 8)	South African authorities are recommended to take the following measures to enhance the effectiveness of the existing AML/CFT regime: • Apply adequate CDD requirements to financial institutions that are not currently "accountable institutions" under the FIC Act. • Institute a primary obligation to identify beneficial owners. • Review the provisions of the current Exemptions to ensure that current practices of exempting full CDD requirements in situations where the application of simplified or reduced due diligence would be more appropriate are addressed. • Institute explicit requirements to conduct enhanced due diligence when there is a suspicion of ML or FT, if there are doubts about previously obtained CDD data, and with respect to high-risk customers and transactions. • Establish an explicit obligation for accountable institutions to conduct general on-going due diligence on business relationships and reducing the existing reliance on the obligations under the FIC Act to file an STR and the Regulations to update customer identification and verification particulars to serve this purpose. • Introduce a primary obligation for accountable institutions to identify PEPs and to apply enhanced due diligence with respect to these relationships. • Establishing a specific, enforceable requirement for a bank to perform CDD measures on its respondent institutions and gather sufficient information to fully understand the nature of its respondents' business, the respondents' reputation and the quality of AML/CFT supervision being applied to those institutions. • Introduce explicit requirements for accountable institutions to have policies in place or take measure as needed to prevent the misuse of technological developments by money launderers and terrorist financiers.

AML/CFT System	Recommended Action (listed in order of priority)
3.3 Third parties and introduced business (R.9)	• South Africa should adopt specific measures to implement the requirements of Recommendation 9. • There should be a more definitive timeline attached to the "undertaking" to forward the appropriate information in Exemption 5(c) to ensure that the accountable institution relying on the third-party verification obtains the relevant CDD documentation immediately and that the other accountable institution be under an obligation to provide that information within that time frame. • South African authorities should include a specific obligation on accountable institutions relying on customer identification and verification undertaken by third parties indicating that they are ultimately responsible for customer identification and verification even though they may be satisfied by the services provided by the third parties.
3.4 Financial institution secrecy or confidentiality (R.4)	• There are no recommendations for this Section.
3.5 Record keeping and wire transfer rules (R.10 & SR.VII)	• For financial institutions outside the banking sector, there should be a specific obligation to collect sufficient information to reconstruct financial transactions; there should also be a general obligation to keep account files and business correspondence. • South African authorities should establish a general, enforceable obligation to require: all wire transfers to be accompanied by full originator information (or, in the case of domestic transfers, full originator information to be made available to the authorities within three business days of receiving the request), for the intermediary financial institutions to ensure that all originator information that accompanies a wire transfer is transmitted with the transfer, and for beneficiary financial institutions to consider restricting or terminating business relationships with financial institutions that fail to meet the requirements of Special Recommendation VII and/or consider filing an STR. • Effective systems for monitoring compliance with these obligations should be implemented, including the possibility of imposing more effective, proportionate, and dissuasive sanctions where appropriate.
3.6 Monitoring of transactions and relationships (R.11 & 21)	• South Africa should introduce an explicit requirement that all financial institutions pay special attention to all complex, unusual large transactions or unusual patterns of transactions that have no apparent or visible economic purposes. • Authorities should establish requirements to pay special attention to customers and transactions relating to countries that do not, or insufficiently apply, the FATF Recommendations. Authorities should also establish institutionalised mechanisms for routinely advising accountable institutions of concerns about weaknesses in the AML/CFT regimes of other countries. • Authorities should clarify the application of Exemption 5 and Section 29 of Guidance Note 3 with respect to countries with equivalent AML/CFT systems and strengthen the provisions of Section 29 to ensure that accountable institutions are routinely and consistently paying special attention to business relationships and transactions with countries that do not or insufficiently apply the FATF standards.
3.7 Suspicious transaction reports and other reporting (R.13-14, 19, 25 & SR.IV)	• The Centre should consider tailoring reporting forms for non-bank financial institutions and DNFBPs. • The Centre should provide general feedback in respects to the current techniques, methods and trends of money laundering, and sanitised examples of actual money laundering cases either in the its annual reports or typology reports separately.

AML/CFT System	Recommended Action (listed in order of priority)
3.8 Internal controls, compliance, audit and foreign branches (R.15 & 22)	• The FIC Act should be amended to specify that compliance officers should be at the management level and that employee training be on-going. • There should also be more specific requirements for financial institutions to screen all employees and, for non-bank financial institutions, to maintain internal audit procedures to ensure compliance with AML/CFT policies and procedures. • There should be more specific requirements that foreign branches and subsidiaries apply AML/CFT measures consistent with the FATF Recommendations, and apply the higher of either domestic or South African standards, and inform the home supervisor if it is unable to do so.
3.9 Shell banks (R.18)	• South Africa should create a more direct and specific prohibition on financial institutions entering into or continuing correspondent banking relationships with shell banks and requirements for financial institutions to satisfy themselves that respondent financial institutions in a foreign country do not permit their accounts to be used by shell banks.
3.10 The supervisory and oversight system - competent authorities and SROs. Role, functions, duties and powers (including sanctions) (R.23, 29, 17 & 25)	• *R.23:* For financial service providers, fit and proper tests should apply to all directors. • Directors of collective investment schemes or long-term insurers should be submitted to fit and proper tests. • There should also be licensing or registration requirements to natural or legal persons conducting money/value transfer within South Africa. • *R.29:* Clearer authority should be provided for the SARB and the FSB to inspect for compliance for the provisions of the FIC Act (and is expected once amendments to the FIC Act enter into force in 2009). • *R.17:* South Africa should enhance the authority to apply sanctions that are more broadly effective, proportionate, and dissuasive. This is also expected once amendments to the FIC Act enter into force in 2009. • *R.25:* South African authorities should issue comprehensive guidance on CDD and other FIC Act measures to the other financial institutions and also issue guidance containing ML/FT trends and methods. • *R.30:* South African authorities should consider expanding the staff for the BSD's review team and FSB compliance areas. Ongoing AML/CFT training for BSD staff should also be enhanced.
3.11 Money value transfer services (SR.VI)	• South African authorities should subject natural and legal persons conducting remittance only within South Africa subject licensing or registration. • South African authorities should also expand the scope of obligations to comply with the applicable FATF Recommendations
4. Preventive Measures – Non-Financial Businesses and Professions	
4.1 Customer due diligence and record-keeping (R.12)	• South African authorities should most importantly expand the scope of the FIC Act to more broadly cover the requirements in R.5, 6, and 8-11 for DNFBPs as well as financial institutions. Authorities should also the broaden the scope of obligations for the various DNFBP sectors to enhance CDD obligations as follows: o Casinos should not be exempt from collecting and verifying the residential address and income tax registration number of natural persons (Exemption 14), unless this can be justified on the basis of demonstrated low risk. o Accountants should also be specifically covered when: buying and selling real estate or business entities; managing bank, savings or

AML/CFT System	Recommended Action (listed in order of priority)
	securities accounts; organising contributions for the creation, operation or management of companies; and creating, operating or managing legal persons or arrangements. ○ Attorneys should be required to apply AML/CFT obligations in relation to company services when dealing with a South African company. ○ Dealers in precious metals and stones should be made to be accountable institutions. ○ Company service providers (other than lawyers or accountants) should be required to apply appropriate AML/CFT measures. • South African authorities should also consider the best ways to deal with the particular risks in the real estate sector relating to the non-face to face transactions, the use of cash, and obligations to identify the buyer of real property.
4.2 Suspicious transaction reporting (R.16)	• South African authorities should work with the dealers in precious metals and stones sector and real estate sectors to determine whether they are adequately identifying and reporting suspicious activity. • The Centre should work with the legal profession to further clarify the issue of how legal privilege applies in the context of reporting. • Authorities should strengthen the requirements relating to R.15 and R.21 in relation to all DNFBPs.
4.3 Regulation, supervision and monitoring (R.24-25)	• South Africa should bring into effect as soon as possible provisions that will provide adequate authority for the DNFBP supervisors/monitoring bodies to inspect for and apply a range of sanctions that is effective, proportionate, and dissuasive for non-compliance with the FIC Act. • A comprehensive AML/CFT monitoring regime needs to be developed for dealers in precious metals and dealers in precious stones. • South Africa should also address the scope issues identified under R.12 to ensure that the full range of DNFBPs have comprehensive AML/CFT obligations and supervision or monitoring. • If the Provincial Licensing Authorities are designated as AML/CFT supervisors for casinos, consideration needs to be given as to whether they have sufficient resources to meet their new supervisory and enforcement obligations. • Comprehensive AML/CFT guidance should also be issued for casinos and dealers in precious metals and dealers in precious stones.
4.4 Other non-financial businesses and professions (R.20)	There are no recommendations for this Section.
5. Legal Persons and Arrangements & Non-Profit Organisations	
5.1 Legal Persons – Access to beneficial ownership and control information (R.33)	• South Africa should broaden the requirements on beneficial ownership so that information on ownership/control is readily available in a timely manner.
5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34)	• Steps should be taken to ensure that the information held in the Trusts Registry is accurate (e.g. verification), and that the remaining paper files are uploaded into the register. • South African authorities should consider providing the Masters of the High Court the authority to report suspected ML/FT directly to the Centre
5.3 Non-profit organisations (SR.VIII)	• South Africa should assess potential risks of terrorist financing posed within its NPO sector. • The legislation governing the NPO sector in South Africa should further be reviewed to require the mandatory registration of NPOs in South

AML/CFT System	Recommended Action (listed in order of priority)
	Africa. • The enforcement powers under the NPO Act should be reviewed to provide additional sanctions including, the power to sanction office bearers, impose fines and freeze accounts of NPOs for violation of oversight measures. • Regulations should be passed to specify the retention period that applies to the record keeping requirement of NPOs under Section 17(3) of the Act. • The NPO laws should be amended to provide for the requirement for NPOs to maintain for a period of at least five years information on the identity of person(s) who own, control or direct their activities, including senior officers, board members and trustees. • Outreach programme should be undertaken with the specific aim to protect the NPO sector from terrorist financing abuse.
6. National and International Co-operation	
6.1 National co-operation and coordination (R.31)	• Authorities should ensure that effective policy coordination continues.
6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)	• South Africa should amend its money laundering offence to be fully consistent with the Palermo and Convention and enact stronger customer identification measures.
6.3 Mutual Legal Assistance (R.36-38 & SR.V)	• The South African authorities should consider having a similar provision (along the lines of Section 205 of the CPA) in Section 8(1) of the ICCMA so as to make it simpler for routine production orders. • Measures should be taken to address this issue of the requirement that foreign restraining orders must have been finalised.
6.4 Extradition (R.39, 37 & SR.V)	• South Africa should maintain proper statistics for extradition requests, as it is currently not possible to assess the effectiveness of the measures in place.
6.5 Other Forms of Co-operation (R.40 & SR.V)	There are no recommendations for this Section.
7. Other issues	
7.1 Resources and statistics	• South African authorities should consider the best ways to address the challenges with attracting and appointing qualified applicants to the NPA. • South Africa should review the effectiveness of its systems for combating money laundering and terrorist financing on a regular basis. • South Africa should improve its system for collecting and maintaining comprehensive data on money laundering investigations, prosecutions and convictions. • Statistics should be maintained concerning the number of cases and the amounts of property frozen, seized, and confiscated in relation to money laundering and terrorist financing. • There should be more adequate statistics on cross border transportations of currency and BNI over the thresholds. • South Africa should keep comprehensive statistics of mutual legal assistance and extradition matters.

ANNEXES

ANNEX 1: LIST OF ABBREVIATIONS

ADLA	Authorised Dealer with Limited Authority
AFU	Asset Forfeiture Unit of the National Prosecuting Authority
AML	Anti-money laundering
APM	Agricultural Products Market
ATM	Automated teller machine
BASA	Banking Association of South Africa
BCOCC	Border Control Operational Coordinating Committee
BEI	Business Entity Identifier
BNI	Bearer negotiable instruments
BSD	Bank Supervision Department of the South Africa Reserve Bank
CBCU	Customs Border Control Unit
CDD	Customer due diligence
CE Act	Currency and Exchanges Act
CEN	Customs Enforcement Network
Centre	Financial Intelligence Centre
CEO	Chief executive officer
CFT	Counter-terrorist financing
CIPRO	Companies and Intellectual Property Registration Office
CIS	Collective Investment Schemes
CISC Act	Collective Investment Schemes Control Act
CMA	Common Monetary Area
CPA	Criminal Procedure Act
CSD	Central securities depositories
CSDP	Central Securities Depository Participant
CV	Curriculum vitae
DCSA	Diamond Council of South Africa
DFA	Department of Foreign Affairs
DHA	Department of Home Affairs
DJFSA	Diamond and Jewellery Federation of South Africa
DNFBP	Designated non-financial businesses and professions
DoJ & CD	Department of Justice and Constitutional Development
DPCI	Directorate for Priority Crime Investigation
DPM Regulator	South African Diamond and Precious Metals Regulator
DPP	Director of Public Prosecutions
DSD	Department of Social Development
DSO	Directorate of Special Operations (the Scorpions)
EDM	Equity Derivatives Market
EAAB	Estate Agency Affairs Board
EFT	Electronic Funds Transfer
EM	Equities Market
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
EUR	Euro
ExCon	Exchange Control Department of the South Africa Reserve Bank
Exemptions	Exemptions in Terms of the Financial Intelligence Centre Act
FAIS	Financial Advisory and Intermediary Services
FAIS Act	Financial Advisory and Intermediary Services Act

FATF	Financial Action Task Force
FI	Financial institution
FI Act	*Financial Institutions (Protection of Funds) Act*
FIC Act	Financial Intelligence Centre Act
FIC Amendment Act	Financial Intelligence Centre Amendment Act
FIU	Financial intelligence unit
FMC Act	Financial Markets Control Act
FSB	Financial Services Board
FSB Act	Financial Services Board Act
FSC	Financial Sector Charter
FSI	Financial Stability Institute
FSP	Financial services provider
FT	Terrorist Financing
FX Regulations	Exchange Control Regulations
HRD	Human-resource development
ICASA	Independent Communications Authority of South Africa
ID	Identification
IFAC	International Federation of Accountants
IFI Act	Inspection of Financial Institutions Act
ICCMA	International Co-operation in Criminal Matters Act, 1996
IMMS	Immediate settlement
IOSCO	International Organisation of Securities Commission
IRBA	Independent Regulatory Board for Auditors
IT	Information technology
Ithala	Ithala Development Finance Corporation Limited
JCSA	Jewellery Council of South Africa
JIMC	Johannesburg International Mail Chamber
JSE	JSE Limited
KYC	Know your customer
LOA	Life Offices' Association
LSSA	Law Society of South Africa
LTI Act	Long-term Insurance Act
MAA	Mutual Administrative Assistance
ML	Money laundering
MLAC	Money Laundering Advisory Council
MLTFC Regulations	Money Laundering and Terrorist Financing Control Regulations, 2005
MOU	Memorandum of Understanding
MT	Message type
MVT	Money/value transfer
NCOP	National Council of Provinces
NG Act	National Gambling Act
NGB	National Gambling Board
NIA	National Intelligence Agency
NIB	National Immigration Branch
NICOC	National Intelligence Co-ordination Committee
NPA	National Prosecuting Authority
NPA Act	National Prosecuting Authority Act
NPO	Non-profit organisation
NPO Act	Non-profit Organisations Act, 1998
NPS	National Prosecuting Services
NPS	National Payment System
NPS Act	National Payment System Act
OFSI	Office of the Superintendent of Financial Institutions
PAAB	Public Accountants and Auditors Board
Palermo Convention	United Nations Convention Against Transnational Organised Crime, 2000
PASA	Payment Association of South Africa
PCH	Payment Clearing Houses
PEP	Politically exposed person
PF Act	Pension Funds Act
PFM Act	Public Finance Management Act

PLA	Provincial Licensing Authorities
PM Act	Precious Metals Act
POCA	Prevention of Organised Crime Act, 1998
POCDATARA	Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004
Postbank	Post Office Bank
PRECA Act	Prevention and Combating of Corrupt Activities Act
R.	Recommendation
RCMA	Rand Common Monetary Area
RILO	World Customs Organisation Regional Intelligence Liaison Offices
RLS	Regional Law Societies
RTC	Real time credit
s.	Section
SABRIC	South African Banking Risk Information Centre
SADC	Southern African Development Council
SAICA	South African Institute of Chartered Accountants
SAPO	South African Post Office
SAPS	South African Police Service
SARB	South African Reserve Bank
SARS	South African Revenue Service
SASS	South African Secret Service
SCCU	Specialised Commercial Crime Unit of NPA
SEC Act	Stock Exchanges Control Act
SIU	Special Investigating Unit
SR	Special Recommendation
S/RES/1267(1999)	United Nations Security Council Resolution 1267(1999)
S/RES/1373(2001)	United Nations Security Council Resolution 1373(2001)
S/RES/1452(2004)	United Nations Security Council Resolution 1452(2004)
SRO	Self-regulatory organisation
s.	Section
ss.	Sections
SS Act	Securities Services Act
STP	Straight Through Processing
STR	Suspicious transaction report
SWIFT	*Society for Worldwide Interbank Financial Telecommunication*
TCSP	Trust and company service providers
Terrorist Financing Convention	International Convention for the Suppression of the Financing of Terrorism, 1999
TPC Act	Trust Property Control Act, 1988
TPC Regulation	Trust Property Control Regulation
TPR	Terrorist Property Report
TRN	Transaction reference number
UN	United Nations
UNCAC	United Nations Convention Against Corruption
UNSC	United Nations Security Council
USAID	United States Agency for International Development
USD	United States dollars
UTC Act	Unit Trusts Control Act
Vienna Convention	United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988
WCO	World Customs Organisation
ZAPS	South African Payment System
ZAR	South African Rand

ANNEX 2: DETAILS OF ALL BODIES MET ON THE ON-SITE MISSION - MINISTRIES, OTHER GOVERNMENT AUTHORITIES OR BODIES, PRIVATE SECTOR REPRESENTATIVES AND OTHERS.

1. Financial Intelligence Centre
2. Department of Social Development (DSD)
3. Department of Justice and Constitutional Development (DoJ&CD)
4. South African Revenue Service (SARS)
5. National Treasury
6. South African Police Service (SAPS)
7. South African Reserve Bank (SARB)
8. Financial Services Board (FSB)
9. National Gambling Board (NGB)
10. Companies and Intellectual Property Registration Office (CIPRO)
11. Master of the High Court
12. Estate Agents Affairs Board (EAAB)
13. Independent Regulatory Board for Auditors (IRBA)
14. Law Society of South Africa (LSSA)
15. Nedbank Group Limited
16. Banking Association of South Africa (BASA)
17. Montecasino
18. Liberty Group
19. Life Office's Association of South Africa (LOA)
20. JSE Limited (JSE)
21. Barnard Jacobs Mellett Securities (Pty) Ltd
22. Diamond Council of South Africa
23. Jewellery Council of South Africa
24. Bidvest Bank
25. Post Bank
26. Payment Association South Africa (PASA)
27. MoneyGram
28. Association of Collective Investments
29. Stanlib

ANNEX 3: COPIES OF KEY LAWS, REGULATIONS AND OTHER MEASURES

Money laundering offences (POCA, ss.4-6)

4 Money laundering

Any person who knows or ought reasonably to have known that property is or forms part of the proceeds of unlawful activities and-

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

(b) performs any other act in connection with such property, whether it is performed independently or in concert with any other person,

which has or is likely to have the effect-

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

(ii) of enabling or assisting any person who has committed or commits an offence, whether in the Republic or elsewhere-

(aa) to avoid prosecution; or

(bb) to remove or diminish any property acquired directly, or indirectly, as a result of the commission of an offence,

shall be guilty of an offence.

5 Assisting another to benefit from proceeds of unlawful activities

Any person who knows or ought reasonably to have known that another person has obtained the proceeds of unlawful activities, and who enters into any agreement with anyone or engages in any arrangement or transaction whereby-

(a) the retention or the control by or on behalf of the said other person of the proceeds of unlawful activities is facilitated; or

(b) the said proceeds of unlawful activities are used to make funds available to the said other person or to acquire property on his or her behalf or to benefit him or her in any other way,

shall be guilty of an offence.

6 Acquisition, possession or use of proceeds of unlawful activities

Any person who-

(a) acquires;

(b) uses; or

(c) has possession of,

property and who knows or ought reasonably to have known that it is or forms part of the proceeds of unlawful activities of another person, shall be guilty of an offence.

Terrorist financing offences (POCDATARA, s.4)

4 Offences associated or connected with financing of specified offences

(1) Any person who, directly or indirectly, in whole or in part, and by any means or method-

(a) acquires property;

(b) collects property;

(c) uses property;

(d) possesses property;

(e) owns property;

(f) provides or makes available, or invites a person to provide or make available property;

(g) provides or makes available, or invites a person to provide or make available any financial or other service;

(h) provides or makes available, or invites a person to provide or make available economic support; or

(i) facilitates the acquisition, collection, use or provision of property, or the provision of any financial or other service, or the provision of economic support,

intending that the property, financial or other service or economic support, as the case may be, be used, or while such person knows or ought reasonably to have known or suspected that the property, service or support concerned will be used, directly or indirectly, in whole or in part-

(i) to commit or facilitate the commission of a specified offence;

(ii) 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 offence; or

(iii) for the benefit of a specific entity identified in a notice issued by the President under section 25,

is guilty of an offence.

(2) Any person who, directly or indirectly, in whole or in part, and by any means or method-

(a) deals with, enters into or facilitates any transaction or performs 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-

(i) to commit or facilitate the commission of a specified offence;

(ii) 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 offence; or

(iii) for the benefit of a specific entity identified in a notice issued by the President under section 25; or

(b) provides financial or other services in respect of property referred to in paragraph (a),

is guilty of an offence.

(3) Any person who knows or ought reasonably to have known or suspected that property is property referred to in subsection (2) (a) and enters into, or becomes concerned in, an arrangement which in any way has or is likely to have the effect of-

(a) facilitating the retention or control of such property by or on behalf of-

(i) an entity which commits or attempts to commit or facilitates the commission of a specified offence; or

(ii) a specific entity identified in a notice issued by the President under section 25;

(b) converting such property;

(c) concealing or disguising the nature, source, location, disposition or movement of such property, the ownership thereof or any interest anyone may have therein;

(d) removing such property from a jurisdiction; or

(e) transferring such property to a nominee,

is guilty of an offence.

Establishing the FIU (FIC Act, ss.2-5)

2. Establishment

(1) A Financial Intelligence Centre is hereby established as an institution outside the public service but within the public administration as envisaged in section 195 of the Constitution.

(2) The Centre is a juristic person.

3. Objectives

(1) The principal objective of the Centre is to assist in the identification of the proceeds of unlawful activities and the combating of money laundering activities and the financing of terrorist and related activities.

(2) The other objectives of the Centre are-

(a) to make information collected by it available to investigating authorities, the intelligence services and the South African Revenue Service to facilitate the administration and enforcement of the laws of the Republic;

(b) to exchange information with similar bodies in other countries regarding money laundering activities and similar offences.

4. Functions

To achieve its objectives the Centre must-

(a) process, analyse and interpret information disclosed to it, and obtained by it, in terms of this Act;

(b) inform, advise and cooperate with investigating authorities, supervisory bodies, the South African Revenue Service and the intelligence services;

(c) monitor and give guidance to accountable institutions, supervisory bodies and other persons regarding the performance by them of their duties and their compliance with the provisions of this Act;

(d) retain the information referred to in paragraph (a) in the manner and for the period required by this Act.

5. General powers

(1) The Centre may do all that is necessary or expedient to perform its functions effectively, which includes the power to-

(a) determine its own staff establishment and the terms and conditions of employment for its staff within a policy framework determined by the Minister;

(b) appoint employees and seconded personnel to posts on its staff establishment;

(c) obtain the services of any person by agreement, including any state department, functionary or institution, to perform any specific act or function;

(d) acquire or dispose of any right in or to property, but rights in respect of immovable property may be acquired or disposed of only with the consent of the Minister;

(e) open and operate its own bank accounts, subject to the Public Finance Management Act, 1999 (Act No. 1 of 1999);

(f) insure itself against any loss, damage, risk or liability;

(g) perform legal acts or institute or defend any legal action in its own name;

(h) engage in any lawful activity, whether alone or together with any other organisation in the Republic or elsewhere, aimed at promoting its objectives;

(i) do anything that is incidental to the exercise of any of its powers.

AML/CFT obligations (FIC Act, Chapter 3, excerpts)

CHAPTER 3 - CONTROL MEASURES FOR MONEY LAUNDERING CONTROL MEASURES AND FINANCING OF TERRORIST AND RELATED ACTIVITIES

Part 1 - Duty to identify clients

21. Identification of clients and other persons

(1) An accountable institution may not establish a business relationship or conclude a single transaction with a client unless the accountable institution has taken the prescribed steps-

(a) to establish and verify the identity of the client;

(b) if the client is acting on behalf of another person, to establish and verify-

(i) the identity of that other person; and

(ii) the client's authority to establish the business relationship or to conclude the single transaction on behalf of that other person; and

(c) if another person is acting on behalf of the client, to establish and verify-

(i) the identity of that other person; and

(ii) that other person's authority to act on behalf of the client.

(2) If an accountable institution had established a business relationship with a client before this Act took effect, the accountable institution may not conclude a transaction in the course of that business relationship, unless the accountable institution has taken the prescribed steps-

(a) to establish and verify the identity of the client;

(b) if another person acted on behalf of the client in establishing the business relationship, to establish and verify-

(i) the identity of that other person; and

(ii) that other person's authority to act on behalf of the client;

(c) if the client acted on behalf of another person in establishing the business relationship, to establish and verify-

(i) the identity of that other person; and

(ii) the client's authority to act on behalf of that other person; and

(d) to trace all accounts at that accountable institution that are involved in transactions concluded in the course of that business relationship.

Part 2 - Duty to keep record

22. Record to be kept of business relationships and transactions

(1) Whenever an accountable institution establishes a business relationship or concludes a transaction with a client, whether the transaction is a single transaction or concluded in the course of a business relationship which that accountable institution has with the client, the accountable institution must keep record of-

(a) the identity of the client;

(b) if the client is acting on behalf of another person-

(i) the identity of the person on whose behalf the client is acting; and

(ii) the client's authority to act on behalf of that other person;

(c) if another person is acting on behalf of the client-

(i) the identity of that other person; and

(ii) that other person's authority to act on behalf of the client;

(d) the manner in which the identity of the persons referred to in paragraphs (a), (b) and (c) was established;

(e) the nature of that business relationship or transaction;

(f) in the case of a transaction-

(i) the amount involved; and

(ii) the parties to that transaction;

(g) all accounts that are involved in-

(i) transactions concluded by that accountable institution in the course of that business relationship; and

(ii) that single transaction;

(h) the name of the person who obtained the information referred to in paragraphs (a), (b) and (c) on behalf of the accountable institution; and

(i) any document or copy of a document obtained by the accountable institution in order to verify a person's identity in terms of section 21(1) or (2).

(2) Records kept in terms of subsection (1) may be kept in electronic form.

23. Period for which records must be kept

An accountable institution must keep the records referred to in section 22 which relate to-

(a) the establishment of a business relationship, for at least five years from the date on which the business relationship is terminated;

(b) a transaction which is concluded, for at least five years from the date on which that transaction is concluded.

Part 3 - Reporting duties and access to information

28A. Property associated with terrorist and related activities

(1) An accountable institution which has in its possession or under its control property owned or controlled by or on behalf of, or at the direction of -

(a) any entity which has committed, or attempted to commit, or facilitated the commission of a specified offence as defined in the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004; or

(b) a specific entity identified in a notice issued by the President, under section 25 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004, must within the prescribed period report that fact and the prescribed particulars to the Centre.

(2) The Director may direct an accountable institution which has made a report under subsection (1) to report -

(a) at such intervals as may be determined in the direction, that it is still in possession or control of the property in respect of which the report under subsection (1) had been made; and

(b) any change in the circumstances concerning the accountable institution's possession or control of that property.

29. Suspicious and unusual transactions

(1) A person who carries on a business or is in charge of or manages a business or who is employed by a business and who knows or ought reasonably to have known or suspected that -

(a) the business has received or is about to receive the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities;

(b) a transaction or series of transactions to which the business is a party -

(i) facilitated or is likely to facilitate the transfer of the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities;

(ii) has no apparent business or lawful purpose;

(iii) is conducted for the purpose of avoiding giving rise to a reporting duty under this Act;

(iv) may be relevant to the investigation of an evasion or attempted evasion of a duty to pay any tax, duty or levy imposed by legislation administered by the Commissioner for the South African Revenue Service; or

(v) relates to an offence relating to the financing of terrorist and related activities; or

(c) the business has been used or is about to be used in any way for money laundering purposes or to facilitate the com mission of an offence relating to the financing of terrorist and related activities, must, within the prescribed

period after the knowledge was acquired or the suspicion arose, report to the Centre the grounds for the knowledge or suspicion and the prescribed particulars concerning the transaction or series of transactions.

(2) A person who carries on a business or is in charge of or manages a business or who is employed by a business and who knows or suspects that a transaction or a series of transactions about which enquiries are made, may, if that transaction or those transactions had been concluded, have caused any of the consequences referred to in subsection (1)(a), (b) or (c), must, within the prescribed period after the knowledge was acquired or the suspicion arose, report to the Centre the grounds for the knowledge or suspicion and the prescribed particulars concerning the transaction or series of transactions.

(3) No person who made or must make a report in terms of this section may disclose that fact or any information regarding the contents of any such report to any other person, including the person in respect of whom the report is or must be made, otherwise than-

(a) within the scope of the powers and duties of that person in terms of any legislation;

(b) for the purpose of carrying out the provisions of this Act;

(c) for the purpose of legal proceedings, including any proceedings before a judge in chambers; or

(d) in terms of an order of court.

(4) No person who knows or suspects that a report has been or is to be made in terms of this section may disclose that knowledge or suspicion or any information regarding the contents or suspected contents of any such report to any other person, including the person in respect of whom the report is or is to be made, otherwise than-

(a) within the scope of that person's powers and duties in terms of any legislation;

(b) for the purpose of carrying out the provisions of this Act;

(c) for the purpose of legal proceedings, including any proceedings before a judge in chambers; or

(d) in terms of an order of court.

Part 4 - Measures to promote compliance by accountable institutions

42. Formulation and implementation of internal rules

(1) An accountable institution must formulate and implement internal rules concerning-

(a) the establishment and verification of the identity of persons whom the institution must identify in terms of Part 1 of this Chapter;

(b) the information of which record must be kept in terms of Part 2 of this Chapter;

(c) the manner in which and place at which such records must be kept;

(d) the steps to be taken to determine when a transaction is reportable to ensure the institution complies with its duties under this Act; and

(e) such other matters as may be prescribed.

(2) Internal rules must comply with the prescribed requirements.

(3) An accountable institution must make its internal rules available to each of its employees involved in transactions to which this Act applies.

(4) An accountable institution must, on request, make a copy of its internal rules available to-

(a) the Centre;

(b) a supervisory body which performs regulatory or supervisory functions in respect of that accountable institution.

ANNEX 4: LIST OF LAWS, REGULATIONS AND OTHER MATERIAL RECEIVED

Primary legislation:

1. Attorneys' Act
2. Auditing Profession Act
3. Banks Act
4. Civil Aviation Offences Act
5. Close Corporations Act
6. Collective Investment Schemes Control Act (45 of 2002)
7. Companies Act
8. Constitution
9. Co-op Banks Act
10. Counterfeit Goods Act
11. Counterfeiting of Currency Act
12. Criminal Procedure Act
13. Currency and Exchanges Act
14. Customs and Excise Act
15. Defence Act
16. Diamonds Act
17. Domestic Violence Act
18. Drugs and Drug Trafficking Act
19. Environment Conservation Act
20. Estate Agency Affairs Act RO
21. Exchange Control Amnesty and Amendment of Taxation Laws Act
22. Extradition Act
23. FI (Protection of Funds) Act
24. Financial Advisory and Intermediary Services Act (37 of 2002)
25. Financial Intelligence Centre Act
26. Financial Services Board Act
27. Financial Services Ombud Schemes Act (37 of 2004)
28. Firearms Control Act
29. Friendly Societies Act
30. General Law Amendment Act
31. Inspection of Financial Institutions Act
32. International Co-operation in Criminal Matters Act
33. Intelligence Services Act
34. Interception Act
35. Interpretation Act
36. Long-term Insurance Act
37. National Arms Control Act
38. National Gambling Act
39. National Prosecuting Authority Act
40. Non-profit Organisations Act
41. National Payment System Act
42. Nuclear Energy Act
43. Pension Funds Act
44. Prevention of Organised Crime Act
45. Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004

46. Prevention and Combating of Corrupt Activities Act
47. Precious Metals Act
48. Interception and Monitoring Prohibition Act
49. Riotous Assemblies Act
50. South Africa Police Service Act
51. South Africa Reserve Bank Act
52. Securities Services Act 36 of 2004
53. Sexual Offence Act
54. Sexual Offences Amendment Act RO
55. Trust Property Control Act

Regulations and subordinate legislation

1. Banks Act Regulations 2006 (Regulations Relating to Banks)
2. Exchange Control Regulations
3. Orders and Rules under the Exchange Control Regulations
4. FAIS - Board Notice 91 of 2006
5. Exemptions in Terms of the Financial Intelligence Centre Act
6. JSE Rules
7. Money Laundering and Terrorist Financing Control Regulations
8. National Gambling Regulations
9. Collective Investment Schemes Control Act: Conditions
10. Regulations: Collective Investment Schemes
11. Regulations: Financial Advisory and Intermediary Services
12. Regulations: Financial Services Ombud Schemes
13. Regulations: Friendly Societies Act 25 OF 1956
14. Regulations: FSB Act
15. Regulations: Long-term Insurance Act
16. Regulations: Pension Funds
17. Regulations: Prevention of Organised Crime Act

ANNEX 5: SOUTH AFRICAN OFFENCES THAT CORRESPOND TO THE 20 DESIGNATED CATEGORIES OF PREDICATE OFFENCES

Participation in an organised criminal group and racketeering

- Racketeering in terms of section 2 of the POCA
- Gang related offences in terms of section 9 of the POCA
- Conspiracy offences in terms of common law

Terrorism, including terrorist financing

- Terrorism in terms of section 2 of the Protection of Constitutional Democracy Against Terrorist And Related Activities Act, 2004 (POCDATARA)
- Offences associated or connected with terrorist activities in terms of section 3 of POCDATARA
- Offences associated or connected with financing of specified offences in terms of section 4 of POCDATARA

Trafficking in human beings and migrant smuggling

- This is addressed in terms of a number of common law offences such as kidnapping and fraud and statutory offences relating to immigration

Sexual exploitation, including sexual exploitation of children

- Sexual Offences Act, 1957:
  - Keeping a brothel (section 2)
  - Procuration (section 10)
  - Detention for purposes of unlawful carnal intercourse (section 12)
- Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007
  - Rape (section 3)
  - Sexual exploitation of children (section 17)
  - Using children for or benefiting from child pornography (section 20)
- Common law offence of indecent assault

Illicit trafficking in narcotic drugs and psychotropic substances

- Drugs and Drug Trafficking Act, 1992:
  - Manufacture and supply of scheduled substances (section 3)
  - Dealing in drugs (section 5)

Illicit arms trafficking

- Firearms Control Act, 2000:
  - General prohibition in respect of firearms section 9)
  - Prohibition of import, export or carriage in-transit of firearms and ammunition without permit (section 73)
  - Storage and transport of firearms and ammunition (section 83)
- National Conventional Arms Control Act, 2002:
  - Control over conventional arms and provision of service (section 13)

Illicit trafficking in stolen and other goods

- General Law Amendment Act, 1955
  - Possession of stolen property (section 36)
  - Receipt of stolen property (section 37)
- Common law offence of theft

Corruption and bribery

- Prevention and Combating of Corrupt Activities Act, 2004:
  - General offence of corruption (section 3)
  - Offences in respect of corrupt activities relating to specific persons (sections 4-9)
  - Offences of receiving or offering of unauthorised gratification by or to party to an employment relationship (section 10)

Fraud

- Common law offence of fraud

Counterfeiting currency

- Prevention of Counterfeiting of Currency Act, 1965:
  - Offences relating to current coin and bank notes (section 2)

Counterfeiting and piracy of products

- Counterfeit Goods Act, 1997:
  - Dealing in counterfeit goods prohibited and an offence (section 2)

Environmental crime

- Environment Conservation Act, 1989:
  - Prohibition of littering (section 19)
  - Waste Management (section 20)
  - Prohibition on undertaking of identified activities (section 22)

Murder, grievous bodily injury

- Common law crimes of murder and assault with intent to do grievous bodily harm

Kidnapping, illegal restraint and hostage-taking

- Common Law offences of kidnapping, child stealing
- Offences relating to taking a hostage in terms of section 7 of POCDATARA

Robbery or theft

- Common law offences of robbery and theft

Smuggling

- Offences concerning trafficking in prohibited or restricted goods such as those under the Drugs and Drug Trafficking Act and the Firearms Control Act referred to above.

Extortion

- Common law offence of extortion

Forgery

- Common law offences of forgery and uttering

Piracy

- Defence Act, 2002:
  - Piracy (section 24)

Insider trading and market manipulation

- Securities Services Act, 2004:
  - Insider trading (section 73)
  - Prohibited trading practices (section 75)
  - False, misleading or deceptive statements, promises and forecasts (section 76)