MENAFATF
مينافاتف
GAFIMOAN
MIDDLE EAST & NORTH AFRICA
FINANCIAL ACTION TASK FORCE

FATF•GAFI
FINANCIAL ACTION TASK FORCE

Mutual Evaluation Report Executive Summary

Anti-Money Laundering and Combating the Financing of Terrorism

Kingdom of Saudi Arabia

25 June 2010

The Kingdom of Saudi Arabia is a member of the Middle East & North Africa Financial Action Task Force (MENAFATF). It is also a member of the Gulf Co-operation Council, which is a member of the Financial Action Task Force (FATF). This joint MENAFATF-FATF evaluation was adopted as follows:

MENAFATF Plenary 4 May 2010
FATF Plenary 25 June 2010

TABLE OF CONTENTS

PREFACE

INFORMATION AND METHODOLOGY USED FOR THE EVALUATION OF THE KINGDOM OF SAUDI ARABIA

1. The evaluation of the anti-money laundering (AML) and combating the financing of terrorism (CFT) regime of the Kingdom of Saudi Arabia[1] (KSA) 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[2]. The evaluation was based on the laws, regulations and other materials supplied by the KSA, and information obtained by the evaluation team during its on-site visit to the KSA from 1-11 March 2009, and subsequently. During the on-site the evaluation team met with officials and representatives of all relevant KSA government agencies and the private sector. A list of the bodies met is set out in the annexes to the mutual evaluation report.

2. This is a joint mutual evaluation by the Middle East and Northern Africa Financial Action Task Force (MENFATF, مينافاتف) and the Financial Action Task Force (FATF). The evaluation was conducted by an evaluation team which consisted of experts from the MENAFATF and FATF in criminal law, law enforcement and regulatory issues. The team included Mr. Hussam Imam (Mutual Evaluation Officer of the MENAFATF Secretariat) and Mr. Richard Berkhout (Administrator of the FATF Secretariat), and further included the following assessors: Mr. Talal Alsayegh (Deputy Manger, On-Site Supervision Department, Central Bank of Kuwait, Kuwait) who participated as financial expert for the MENAFATF, Ms. Catherine Downard (Assistant Director for Global Affairs, Office of Terrorist Financing and Financial Crimes, Department of the Treasury, United States) who participated as financial expert for the FATF, Mr. Dick van den Ham (Head, Financial Intelligence Unit MOT, Aruba, Kingdom of the Netherlands) who participated as law enforcement expert for the FATF, Mr. Ignacio de Lucas (Prosecutor, Special Prosecution Service for the Prevention and Repression of Illegal Drug Trafficking, Spanish National Court, Spain) who participated as legal expert for the FATF, and Mr. Arz Murr, (Inspector, Compliance Unit, Special Investigation Commission, Lebanon) who participated as financial expert for MENAFATF. 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 and the financing of terrorism through financial institutions and Designated Non-Financial Businesses and Professions, 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 the KSA as at the date of the on-site visit or immediately thereafter. It describes and analyses those measures, sets out the KSA'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] In this report, SA, KSA, the Kingdom and Saudi Arabia all denote the Kingdom of Saudi Arabia.
[2] As updated in October 2008.

EXECUTIVE SUMMARY

1. Background Information

4. Saudi Arabia is a significant regional economic player with a high GDP. It is the biggest oil producer and exporter in the world. In addition, it has embarked during the past decade on a plan to become a regional economic center and to diversify from almost exclusively petroleum based output to other economic sectors and products. The Saudi economy has been opened up in the previous years, including the establishment of the capital market and investment sectors. Saudi Arabia's legal system is a unique one, where the *Holy Qur'an* and *Sunnah* (Prophet Muhammad's teachings and traditions) represent the core of the legal and ruling systems. Islamic Law (or *Shari'ah*) and jurisprudence have a general law standing in many cases, where the statutory laws are silent on some issues.

5. Saudi Arabia's anti-money laundering (AML) and counter terrorist financing (CFT) regime is in creation since 2003. The anti-money laundering statute (AMLS) was issued in 2003, but money laundering (ML) cases were prosecuted and brought to courts already before the law came into effect. The said law and its Implementing Regulations (2005) provide basic requirements that are complemented by rules, instructions and circulars issued by supervisory authorities. In its efforts to combat (ML) and terrorist financing (TF), Saudi Arabia has established a number of permanent national committees to coordinate policy efforts, though such committees' role should be maximized. The CFT framework in Saudi Arabia suffers from shortcomings that need to be addressed and corrected explicitly and adequately, even though terrorism (and therefore TF) is punishable in KSA under *Shari'ah,* which has already led to convictions.

6. On the other hand, the implementation of the different aspects of the AML/CFT system in Saudi Arabia is still gaining momentum, given the novelty of many sectors conducting business, such as the insurance, securities and financing sectors, and the novelty of the AML/CFT instructions for such sectors. This overarching factor has a negative impact on the effectiveness of the whole regime. In addition, some relevant supervisory authorities are young and are in the first stages of acquiring much needed knowledge and experience. The generally below-expectation level of compliance and implementation varies between financial institutions (especially banking financial institutions) and non-financial institutions and among different sectors within each category. The level of awareness of AML/CFT risks and vulnerabilities among the different sectors needs to be raised and better communicated. Investigation and law enforcement authorities, supervisory authorities and the private sectors should pay greater attention to training and awareness-raising.

2. Legal System and Related Institutional Framework

7. Saudi Arabia criminalized ML since 2003 by virtue of the AMLS . This is in addition to *Shari'ah*, which law provided legal authority to prosecute and sanction ML offenders prior to the issuance of the law. The AMLS does not clearly cover self-laundering and does not clearly extend to predicate offences committed abroad. Effectiveness of ML criminalization cannot be fully measured.

8. The definition in the AMLS of ML includes TF, terrorist acts and terrorist organizations. However, no stand alone statutory TF offence with the features and elements as required by the United Nations (UN) TF Convention exists in the Saudi legal system. The criminalization of terrorism in *Shari'ah*,

while producing convictions, does not allow TF as a stand-alone offence from terrorism. TF as a ML offence does not extend to all legal entities or to all funds as required by the UN TF Convention. TF as a ML offence does not cover acts by terrorist organisations of less than 3 persons, nor does it cover attempt. TF as a ML offence requires funds to be linked with a specific terrorist act. TF as a ML offence is not effective (no cases). Effectiveness of TF criminalization cannot be fully measured.

9. As to confiscation, under *Shari'ah*, it is not relevant who owns criminal property (criminal or a third party). The law permits the confiscation of properties related to the offence regardless of whom it is held by. This includes any proceeds of crime, psychotropic substances, and instrumentalities used for the commission of an offence. The AMLS contains specific provisions for confiscation in AML/CFT proceedings. Confiscation is a mandatory sanction in AMLS cases. The confiscation provisions cover proceeds, instrumentalities used and instrumentalities intended to be used for terrorism. On the other hand, the AMLS does not allow law enforcement agencies other than the financial intelligence unit (FIU) to request to the Prosecution Authority for provisional seizure measures, but other competent authorities may request the FIU to make the request for them. In addition, protection of bona fide third parties is insufficient. Overall, the effectiveness of the system cannot be established.

10. As to freezing terrorist related funds and assets, the backbone of the Saudi freezing regime is Royal Order S/2496 of 19 March 2003. It should be noted that the Royal Order targets ministries, not any financial institution, Designated Non-Financial Business and Profession (DNFBP) or other person. However, after the on-site mission a mechanism was set by virtue of a Royal Decree to deal with United Nations Security Council Resolution (UNSCR) 1267 matters, and the authorities were able to provide statistics regarding the implementation of UNSCR 1267 even before the issuing of the Royal Decree. UNSCR 1373 has not been implemented. On the implementation side, there are no clear monitoring and sanctioning procedures to verify implementation of freezing requests. The lack of a regime to deal with UNSCR 1373 presents a major shortcoming.

11. With respect to the Saudi FIU, the Saudi Arabia Financial Investigation Unit (SAFIU) was established on 7 July 2003 as an autonomous authority under the General Security Department of the Ministry of Interior. SAFIU consists of 7 divisions: Reports Division; Information Collection and Analysis Division; Information Exchange and Follow-up Division; Information and Studies Division; Training Division; Financial and Administrative Affairs Division; and IT Division. SAFIU is well resourced. The current total number of staff is 111, with 20 vacancies. The annual budget is Saudi Riyal (SAR) 100 million. However, SAFIU's independence is not fully secured. SAFIU effectively has access to a number of databases. It provides reporting entities with insufficient information on typologies and trends of ML and especially TF. The number of STRs processed by SAFIU is insufficient against the number of staff (effectiveness). STRs disseminated by SAFIU do not seem to match the need of some receiving agencies.

12. Law enforcement powers have been stipulated in the Criminal Procedure Statute. It authorizes the Prosecution Authority with the power to initiate and follow-up criminal action before the competent courts and stipulates that proceedings relating to criminal investigations and other powers (such as information gathering) are to be conducted by members of the Prosecution Authority and certain officials within the police as well as within those entities that have the general power to investigate and arrest. In addition, public security generals, public research officers, passports officers, intelligence officers, civil defense officers, directors and officers of prisons, border guard officers, special security forces officers, national guards generals, and armed forces officers and members of the religious police (each within their own

jurisdiction) also have investigation powers. Captains of Saudi vessels and airplanes and certain natural and legal persons due to special regulations have similar powers.

13. The main investigation and law enforcement bodies concerned with the fight against ML and TF are in the Ministry of Interior. Other bodies, such as the Saudi Arabian Monetary Agency (SAMA) and Saudi Customs, have investigation powers as well.

14. The Kingdom has implemented a declaration system for the detection and prevention of illicit cross-border transportation of cash since June 2007. The system is fairly new and still in a late implementation stage. The law covers cash, bearer negotiable instruments and precious metals valued over SAR 60 000 (or an equivalent amount in foreign currency), to be declared when entering or leaving the Kingdom. Only travelers with cash, bearer negotiable instruments or precious metals exceeding the declaration threshold need to submit a completed form, other travelers do not need to declare. There are no effective, proportionate and dissuasive sanctions. The effectiveness of the system is arguable because of a lack of clear and comprehensive statistics.

3. Preventive Measures – Financial Institutions

15. All financial activities conducted by financial institutions as identified by the FATF standards and definitions are present in Saudi Arabia. Some sectors though are fairly new, such as the insurance, securities, and financing businesses. This is also the case for supervisors of such institutions and businesses. This situation is reflected to some extent on the level of compliance of financial institutions as well as the effectiveness of the supervisory role.

16. Saudi Arabia has a legal and regulatory framework that governs the financial sector obligations vis-à-vis AML/CFT. However, some of the requirements that should be set by a primary or secondary legislation are instead present in instruments that could be categorized as other enforceable means. In addition, with the extensive expansion of the financial sector and the introduction of new domains of financial activities, such as capital market, insurance and financing, many of the regulatory instructions needed for such businesses and activities are new.

17. With regard to customer due diligence (CDD) measures, the current sets of rules, in addition to the AMLS and implementing regulations, detail the requirements to be observed by financial institutions. However, numbered accounts are not addressed by law or regulation. If financial institutions are to be permitted to open them, they should be clearly required to maintain numbered accounts in such a way that full compliance with the FATF Recommendations can be achieved. In addition, the ongoing due diligence requirement should be provided for explicitly by primary or secondary legislation. Insurance companies should be explicitly prohibited from commencing business relations or performing transactions with a client where required CDD measures could not be satisfactorily completed. In such instances, insurance companies, banks and money exchangers should be required to consider making a suspicious transaction report.

18. Insurance companies should be explicitly required to terminate business relationships and consider making a suspicious transaction report in case required CDD measures could not be applied to existing customers and to cases where the institution has doubts about the veracity or adequacy of previously obtained customer identification data. Banks, money exchangers, insurance companies and authorized persons (security sector) should be explicitly required to apply CDD requirements to existing

customers on the basis of materiality and risk and to conduct due diligence on such existing relationships at appropriate times.

19. In addition to the above-mentioned regulatory aspects, the varying levels of implementation of the applicable CDD obligations by financial institutions are/represent also a cause of concern. Many financial institutions heavily rely on automated systems in undertaking their role, sometimes in a way not commensurate with their human resources that need to receive the output of such systems and act accordingly. Furthermore, in many (primarily non-bank) financial institutions, low levels of awareness of AML/CFT risks and requirements as well as of relevant expertise are widespread, mostly due to the novelty of businesses.

20. As to politically exposed persons (PEPs), there exists a general framework to deal with such persons; however, financing companies should be explicitly required, in addition to performing the CDD measures, to put in place appropriate risk management systems to determine whether a potential customer, a customer or the beneficial owner is a PEP. Insurance companies, securities companies and financing companies should be explicitly required to seek senior management approval for continuing the relationship in cases where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a PEP. Banks and money exchangers should be required to determine the source of funds and source of wealth for beneficial owners identified as PEPs. Insurance companies should be required to determine the source of wealth and source of funds for beneficial owners identified as PEPs, as well as the source of wealth for customers identified as PEPs. Financing companies should be required to determine the source of wealth and source of funds for clients or beneficial owners identified as PEPs.

21. The AMLS, regulations, and rules cover to a generally satisfactory degree the issues of correspondent banking and protection against misuse of new technologies and non-face-to-face relationships for ML and TF. Adequate recordkeeping safeguards are also in place. Wire transfer-related provisions cover most of the requirements of the FATF standards. However, the AML/CFT Rules should be addressing diligence to be implemented for batched wire transfers. Beneficiary financial institutions should be required to adopt effective risk-based procedures for identifying and handling wire transfers that are not accompanied by full originator information.

22. As to transaction monitoring, there is a lack of clear understanding among (primarily non-bank) financial institutions regarding the distinction between requirements to monitor transactions and to report transactions that are identified as suspicious. More fundamentally, entities are often unsure of what are the appropriate parameters and considerations to apply to the monitoring of transactions. These issues could be conquered over a reasonable amount of time through a combination of further clarification of the rules and regulations, training, and effective AML/CFT supervision. Such actions would be reflected on the adequacy of suspicious transaction reporting, in terms of both quantity and quality.

23. Moreover, there are insufficient measures in place to ensure that financial institutions are advised of the AML/CFT weaknesses in other countries. The competent authorities should provide better guidance to institutions to assist in the identification of countries that do not sufficiently apply the FATF recommendations. For banks, money exchangers, and insurance companies, where SAMA does distribute by circular FATF statements identifying countries of concern (to date they have done this for banks and money exchange businesses only), it should more explicitly note institutions' obligations with respect to the use of this information. Across all sectors, where it appears in rules and regulations governing the

AML/CFT practices, reference to the non-cooperative countries and territories list (which no longer exists) should be replaced with more comprehensive and up-to-date guidance.

24. With respect to suspicious transaction reporting (STR), an upward trend in STR filings with the SAFIU over the 2004-2008 period is a positive sign. However, the low overall number of STR filings relative to the size of the economy and characteristics of the financial sector point to a lack of effectiveness. Also, the low number of TF-related STR filings by financial institutions suggests significant deficiencies in addressing TF threats. Further improvements can be made in relation to the quantity and quality of STR reporting by more clearly explaining the distinction between the monitoring of transactions for unusual activity and the identification and reporting of suspicious activity. Efforts to increase awareness – through training, provision of typologies and case studies, etc. – of the potential for TF abuse is also recommended.

25. Internal controls and policies are required from financial institutions by virtue of the law, regulations and rules. The same applies to the requirement of setting up internal and independent audit and control systems to ensure that AML/CFT requirements are met, which is provided in the AMLS, regulations and rules. The AMLS sets out the requirement that all covered entities must establish continuing training programs for employees to keep them updated on ML developments and help them fulfill their AML/CFT duties. However, inadequate AML/CFT-related training of staff in some institutions was noted.

26. More can be done to both expand training opportunities across all sectors and broaden the scope of training. The focus of most training is on understanding the rules and regulations in place. More training to enhance the understanding of how various systems, sectors, and individual entities can be exploited for the purposes of ML and TF is required. With observations in the insurance and financing sectors noted, the authorities should work closely and ardently with insurance companies to effectively implement the robust provisions regarding internal controls and policies that are laid out in the recently issued AML/CFT Rules for Insurance Companies.

27. As to supervision and regulation of financial institutions for AML/CFT purposes, supervisory powers are defined in the AMLS. Supervisory authorities (SAMA and the Capital Market Authority, CMA) have adequate powers to conduct inspections of financial institutions, including onsite inspections. In addition, supervisory authorities have the power to impose limited sanctions against financial institutions. However, some supervisory authorities lack adequate staffing, training, and experience in this field. Concerns exist regarding the adequacy of the supervisory role played in general and in the AML/CFT arena in particular.

28. The same also applies to the adequacy of corrective measures taken by SAMA toward institutions subject to its supervision. The relatively limited number of AML/CFT-related sanctions imposed so far is a reason to reach this conclusion. In addition, no complete cycles of AML/CFT inspections have been conducted for many financial sectors, either as result of the newness of the relevant sector, supervisor, or regulations.

29. AML/CFT guidelines are embedded in the current set of rules that were issued by SAMA and CMA. Both provide basic background information in their AML/CFT Rules, which need to be further developed for banks and money exchangers, insurance companies, leasing companies and securities

companies to include a description of ML and FT techniques and methods and additional measures that these institutions could take to ensure that their AML/CFT measures are effective.

4. Preventive Measures – Designated Non-Financial Businesses and Professions

30. Most of the FATF's Designated Non-Financial Businesses and Professions (DNFBPs) exist in KSA: real estate agents, dealers in precious metals, dealers in precious stones, lawyers and legal advisers, and accountants. Trust (*waqfs*) and company services are partly provided by lawyers (forming companies). *Waqfs* are a similar concept to trusts. The remaining two categories of DNFBPs as defined by the FATF do not operate in the Kingdom, as casinos are prohibited, and notaries are civil servants who do not practice or prepare any financial transactions or dealing for clients.

31. The provisions of the AMLS Implementing Regulations, and in particular those dealing with the preventive measures and the monitoring of their implementation, apply equally to financial institutions and to the DNFBPs. The AML/CFT provisions designed for financial institutions, notably on CDD and reporting, are to be applied by DNFBPs to all their clients/ activities/ dealings¸ although these rules for financial institutions may be resource consuming and not useful to deter ML/TF in the DNFBP sector. The Ministry of Commerce and Industry and the Ministry of Justice (MOJ) both issued additional circulars on AML/CFT procedures that request DNFBPs to identify their clients, verify transactions, keep records, and establish internal monitoring and training programs. These regulations mirror the requirements made in the financial sector.

32. The deficiencies identified under the financial section above are the same for the DNFBPs-sector. A general observation in this sector is that the awareness of AML/CFT risks is lacking. As to implementation and effectiveness, it appeared that for real estate agents and dealers in precious metals and dealers in precious stones, there was no adequate compliance with AML/CFT requirements. As for lawyers and legal advisers, accountants and auditors, there was no compliance with AML/CFT requirements.

33. The supervisory authorities of DNFBPs operating in KSA are the Ministry of Commerce and Industry, the Ministry of Justice, and Saudi Organization for Certified Public Accountants. However, no effective system is in place to supervise and examine the compliance of DNFBPs with the AMLS and its Implementing Regulations. Supervisors need to increase their human and technical resources as well as the awareness and expertise necessary to conduct such examination. The said supervisors have not provided adequate guidelines either, nor has SAFIU provided feedback to reporting entities.

5. Legal Persons and Arrangements & Non-Profit Organizations

34. Ownership details have to be submitted and verified against identity documents at the time of registration, and the Company Registration Law requires that any modifications or changes to the information previously recorded have to be updated within 30 days from occurrence.

35. In principle, commercial register information is available to all competent authorities including the public, however accessing such information might require time as the information is only available within the 40 branches of Commercial Register Office. The team encourages the authorities to introduce direct and spontaneous access to the information by the competent authorities.

36. Overall, KSA has created a system for controlling legal arrangements that outperforms systems in other countries. The authorities should, however, require beneficial ownership (in addition to the beneficiary) to be disclosed in the trust deed.

37. With many charities and *waqfs* with multiple transactions, it is essential that the Ministry of Labor and Social Affairs and the Ministry of Islamic Affairs review the NPO system as a whole, with emphasis on the process of reporting and the level of awareness of AML/CFT. This should be done in close cooperation with SAFIU.

6. National and International Cooperation

38. While operational coordination is sound, on the policy level the Kingdom has set up a framework that is not as effective as it should be. The authorities should better coordinate and streamline the mandates and work of the main coordinating bodies. The authorities should also ensure that there is sufficient coordination between those persons that have access to MENAFATF and FATF meetings, and those that are responsible for implementing the FATF Standards domestically.

39. As regards the UN Vienna Convention, the team was able to confirm that its provisions were implemented. However, this is only partially the case for the UN Palermo Convention. The UN TF Convention is not implemented.

40. It is recommended that KSA implements the UN Palermo and TF Conventions, as well as the UNSCRs to correct the deficiencies noted in relation to the implementation of the relevant international conventions and UNSCRs as soon as possible.

41. There is a need to establish clear procedures for the execution of requests for mutual legal assistance which allow, in particular, for the follow-up of the execution and response to the request by the local authorities involved. In this respect, there should be a central body with responsibility for the coordination of the follow-up of such requests. The Permanent Committee for Mutual Legal Assistance would seem to fit this role, regardless of the subject matter of the request, even though it currently does not appear to implement the coordination aspect that such a role requires and is not aware of its functions under articles 23 and 24 of the AMLS.

42. There is a need to implement international agreements at domestic level in order to establish a clear basis that permits the prosecution of those citizens whose extradition has been refused. In addition to this, these provisions should also establish a framework for cooperation with foreign authorities, in particular at the level of the collection and admissibility of evidence, for the effective prosecution of those individuals. Additionally the Kingdom should conclude extradition agreements with more countries and do not narrow the scope of extradition requests in view of the reciprocity principle.

43. International cooperation by the SAFIU is sound on paper, but was not effectively implemented at the time of the on-site visit[3]. Information regarding supervisory entities was scarcely available to the assessment team, but only regarding the general principles for cooperation, not regarding the legal basis for cooperation. SAMA, as a matter of policy, does not conclude Memorandums of Understanding, and no

[3] After the on-site visit, SAFIU was granted membership of the Egmont Group and has sent 60 requests for MOUs to other FIUs. This should have a positive effect on cooperation issues; however if this is the case, this improvement would be achieved outside the time frame of this assessment.

statistics or practical examples of cooperation could be given. Law enforcement cooperation is sound on paper and in practice, thanks to the case flow through INTERPOL Riyadh.

7. Other Issues

44. Saudi Arabia has set up conduits that could well help improve the national AML/CFT system, such as the permanent committees and abundant financial resources. Nonetheless, AML/CFT-related statistics in Saudi Arabia are in many cases inexistent, incomplete or unreliable. There should be a global statistic generation, gathering, analyzing, and utilization mechanism in place in order for the relevant authorities to be able to review the effectiveness of the AML/CFT systems on a regular basis. In addition, while some authorities are well (or over) staffed, some supervisory authorities need to increase their human and technical resources. All supervisors should pay particular attention to training provision and staff experience enriching.

MUTUAL EVALUATION REPORT

1. GENERAL

1.1 General information on Saudi Arabia

45. The Kingdom of Saudi Arabia covers an area of 2 149 690 square kilometers, and shares land borders (4 431 km) with Kuwait, Iraq, Jordan, Yemen, Oman, the United Arab Emirates and Qatar, and sea borders (2 640 km) with Iran, Bahrain (Arabian Gulf), Egypt, Sudan and Eritrea (Red Sea). The Kingdom is divided into 13 provinces or *mintaqat*. The most important cities are Mecca and Medina (holy cities), Riyadh (capital), Dammam and Jeddah (economic centers). Saudi Arabia has a population of 24.5 million (2008) with an average annual increase of 2.3%. Saudis account for 73% of the population. About one third of the population is under 15 years old and the literacy rate is 79%. The literacy rate among younger people is considerably higher. Life expectancy is 76 years and the national language is Arabic.

46. Modern Saudi Arabia was established on 23 September 1932[4] (National Day) by King Abdul Aziz Bin Abdul Rahman Al-Saud who united the country under his rule. The country is devoutly religious, with all aspects of Saudi society adhering to the values of Islam. Saudi Arabia is the birthplace of the Prophet Mohammed (*Peace be upon him*). A pilgrimage to Mecca, or *hajj*, is a sacred journey that all Muslims are required to make once in their lifetime. During the *hajj* up to 2 million pilgrims will enter the country.

Economy

47. From being an underdeveloped country before the unification, the KSA has become one of the wealthier nations in the Middle East due to the country's vast oil resources. The Saudi economy is managed on free market principles, with an important role of the government over major economic activities, but with low levels of taxation and low interest rates.

48. The economy of the Kingdom is dominated by petroleum activities; the Kingdom has 20% of the world's proven oil reserves (262.8 billion barrels) and ranks as the largest exporter of petroleum. The petroleum sector accounts for roughly 75% of budget revenues, 45% of GDP, and 90% of export earnings. Only about 40% of GDP is generated by the private sector (which is partly publicly owned). The Kingdom's dependence on oil revenues has historically made the economy vulnerable to fluctuations in the world price of oil. The government has sought to allocate income from petroleum to develop the wider economy. Since the 1970s, the government is encouraging private sector growth outside the oil sector - especially in power generation, telecommunication, natural gas exploration, and petrochemicals. The development policy also aims to increase employment opportunities for the growing population, including

[4] The dates used in this report are based on the Gregorian calendar. Saudi Arabia uses the Islamic *Hijri* calendar, marking the migration of Prophet Mohammed from Mecca to Medina. The *Hijri* calendar is based on the lunar year which has 354 days, divided into twelve lunar months. The dates used to designate law, royal decrees and other government actions are based on the *Hijri* calendar.

spending almost 7% of GDP on education. This is a timely policy: Despite the 5.5 million foreigners working in the Kingdom, and with one third of the population still younger than 15 years, unemployment is already estimated to reach somewhere between 12% and 25% among Saudi male nationals.

49. The most important export partners are the United States (17.1%), Japan (16.3%), Republic of Korea (9.7%), China (8.1%), Chinese Taipei (4.7%) and Singapore 4%. The Kingdom imports machinery and equipment, foodstuffs, chemicals, motor vehicles, textiles from the United States (12.6%), China (9.4%), Germany (8.8%), Japan (8.1%), Italy (5%), Republic of Korea (4.9%) and the United Kingdom (4.5%) (all data 2007). The currency of the Kingdom is the Saudi Arabia Riyal (SAR), which is pegged to the United States Dollar (USD) at a rate of 1 USD for 3.75 SAR[5]. Real GDP grew by 3.3% in 2007 and 4.4% in 2008. Due to lower commodities prices and the global economic downturn that started in 2008, the economy grew by 0.15% in 2009.

50. Other sectors, besides the petroleum industry, include general industry, desalination plants, gold and jeweler trade (5th place in the world based on demand), agricultural products (number 1 producer in dates). Another source of income for the Kingdom are the millions of pilgrims that visit Mecca and Medina to perform *hajj* (tourism and services industry, transport, banking).

System of government, legal system and hierarchy of laws

Executive and legislative powers

51. Saudi Arabia is an absolute monarchy. The King, currently His Custodian of the Two Holy Mosques King Abdullah bin Abdulaziz Al Saud, is the Head of State (executive powers) and the Prime Minister. The members of the Council of Ministers (legislative powers) are appointed by the King. Legislation is by resolution, ratified by the King (Royal decree).

Consultative powers

52. The legislative branch is known as the Consultative Council, or *Majlis al-Shura (or Shura Council)*. Its 150 members are appointed by the King and have advisory powers. Councils also exist on the local and regional level. Only half the members of the local and regional councils were elected by the people in 2005, and future elections (due for October 2009) have been postponed. There are no political parties allowed or known pressure groups. Citizens have access to high officials (usually at a *majlis*; a public audience) and the right to petition them directly.

Judicial powers

53. Justice is administered according to *Shari'ah* by a system of *Shari'ah* courts whose judges are appointed by the King on the recommendation of the Supreme Judicial Council, composed of twelve senior jurists, themselves appointed by the King. The King acts as the highest court of appeal and has the power to pardon.

[5] On 10 February 2009, SAR 100.00 equalled USD 26.64 or EUR 20.53. EUR 100.00 equalled SAR 487.14. USD 100.00 equalled SAR 375.44

Shari'ah

54. The Basic Law, adopted in 1992, provides the framework for the government and the hierarchy of laws in the Kingdom. It declares that the Holy *Qur'an* and the *Sunnah*[6] is the Constitution of the Kingdom, and that the country is governed by Islamic Law (*Shari'ah*)[7].

55. *Shari'ah* is the body of Islamic religious law. From the outset, it is a form of law like civil law and common law. However, *Shari'ah* is not just the legal framework within which all aspects of life are regulated in the Islamic state, such as the Kingdom, it is also a religious obligation. In addition, since it is a religious obligation, *Shari'ah* binds the rulers of the Islamic state and requires them to implement *Shari'ah*. As a whole, *Shari'ah* is not a static law or legal text, but a body of laws incorporating the *Qur'an* (the religious text of Islam), *hadith* (sayings and doings of Muhammad and his companions), *ijma* (consensus), *qiyas* (reasoning by analogy) and other sources. Nevertheless, while man-made elements within *Shari'ah* are subject to change over time and place, the *Qur'an's* provisions are permanent, irrevocable and unchangeable.

56. If *Shari'ah* is silent on issues, the Islamic rulers may render a judgment and draw out rulings according to the texts of *Shari'ah*. In practice this means that *Shari'ah* takes precedent over statutes issued by the King, the statutes of the King are *Shari'ah*-based and can never contradict *Shari'ah*. *Shari'ah*, as applied in the Kingdom, cannot be changed, however, it can be applied in new ways in new cases based on reasoning by analogy. This means, in practice, that new concepts that were previously unknown or non-existent, can be already covered by *Shari'ah*. This has been done with respect to criminal law, which means that the criminal statute deals with specificities, such as AML provisions, rather than generalities. The Kingdom, however, has extensive civil and commercial statutes. Saudi courts apply the rules of *Shari'ah* and the statutes decreed by the King. An act may be an offence under both *Shari'ah* and statutory law.

Shari'ah and criminal law

57. The general purpose of *Shari'ah* is to protect the five basic values: religion, soul, honor, mind and wealth. A criminal act under such law is thus the commission of a divinely proscribed deed or the omission of a divinely prescribed duty. Crime in Islam is more oriented towards the commission rather than the omission of the act. Under *Shari'ah* law, a criminal act and the punishment associated with it are interlinked. All crimes in *Shari'ah* law are classified according to the type of punishment imposed. Crimes are therefore classified into three groups as follows: *hadd*, *qissas*, and *ta'zir*.

58. *Hadd* crimes**:** Crimes of this type are described in the *Qur'an* and are thus considered to be violations of divine precepts. *Hadd* crimes are classified in the following order: theft (burglary), adultery, drinking of alcohol, slander or defamation, robbery and apostasy. The punishments for each of the crimes are specified in the *Qur'an* and are fixed, that is, there is no possibility for judges to exercise discretion in cases that examine *hadd* crimes, and no one has the right to drop or mitigate stipulated punishment. In

[6] "*Sunnah*" is the saying and doing of the Prophet (peace be upon him).

[7] Basic Law: Article 6: "Citizens shall pledge allegiance to the King on the basis of the Holy *Qur'an* and the *Sunnah* of the Prophet, on the basis of submission and obedience in times of hardships and ease, fortune and adversity." Article 7: "Governance in Saudi Arabia derives its power from the Holy *Qur'an* and the Prophet's *Sunnah*, both of which Governs this Law." Article 8: "Governance in the Kingdom of Saudi Arabia shall be based on the premise of justice, consultation, and equality in accordance with *Shari'ah*"

hadd crimes there is no link between the type of crime committed and the severity of the punishment imposed.

59. *Qissas* crimes ("talion law" crimes): This category includes murder, regardless of the intent, but also covers all types of willful bodily harm inflicted by one person on another. These crimes and their punishments are clearly mentioned in the *Qur'an* and the *Sunnah*. *Qissas* crimes differ from *hadd* crimes however. The punishment for hadd crimes is carried out by the King (the State) alone, while the punishment for *qissas* crimes is decided by the victim himself, if the victim is alive, or by the next of kin in the case of the victim's death.

60. *Ta'zir* crimes: These third category crimes are those which are not specified as *hadd* or *qissas* crimes. Furthermore, they are not included in any statute or any other legal instrument, owing to the fact that such acts were not prevalent in the time of the Prophet, or their occurrence at that time did not constitute a crime. *Ta'zir* crimes are punished because they constitute a threat to the Islamic State and its society and because they may offend standards of public taste, decency, and morality. The King has the right to define what constitutes a wrongful act other than the acts already specified by God and His Prophet. He further has the right to prescribe the type of punishment appropriate for such wrongful acts, regardless of whether such punishment is reformative, retributive, or deterrent. *Ta'zir* punishment is part of the legal policy in Islam.

61. *Ta'zir* crimes are disciplinary violations, and as such, they fall under the category known in Islamic jurisprudence as *syas sharai*, an equivalent to "legal policy" or "jurisprudence" in positive law. This policy is flexible, and there is no restriction on the side of the Islamic State against adding to the list of acts, which constitute crimes. It is important to note however that, for offences to be included under the *ta'zir* category, it is not necessary that there be a specific statute that stipulates the offence and related punishment. Punishments for *ta'zir* crimes differ from those laid down for *hadd* and *qissas* crimes. As indicated above, punishments for *hadd* and *qissas* crimes are fixed, immutable, and mandatory. The punishments for *ta'zir* crimes however are usually legislated and may vary according to the different crimes. Punishment for such crimes may initially be trivial and gradually increase depending on the type of act committed and the circumstances surrounding them. *Ta'zir* crimes involve value judgments in which the King may assess the behavior of individuals and weigh it against the overall interests of society.

ML and TF under Shari'ah

62. Islam generally prevents persons from acquiring and collecting illicitly originated money. This is done on two levels: *i)* by explicitly prohibiting illicit money altogether and, *ii)* by identifying and prohibiting specific avenues for the illicit acquisition of money. The first level is addressed in the *Qur'an*, which prohibits obtaining any person's money illicitly[8]. On the second level, certain specific ways of acquiring money are prohibited. An example includes the prohibition of liquor, which includes the prohibition of its production, usage, carriage, selling, gaining its proceeds, and purchase[9]. The same applies to theft, armed robbery, usury, prostitution, etc. See the annexes for a much more in depth description of ML under *Shari'ah*.

[8] The *Qur'an* reads, "And eat up not one another's property unjustly (in any illegal way *e.g.* stealing, robbing, deceiving, etc.), nor give bribery to the rulers (judges before presenting your cases) that you may knowingly eat up a part of the property of others sinfully" (2:188)

[9] In *Sunnah*, the Prophet explains that "He who prohibited it has prohibited its price."

63. Terrorism is punishable under *Shari'ah* as an offence against society, for which the most severe penalties apply. Under *Shari'ah*, financing of terrorism is considered a way leading to terrorism, inseparable from terrorism[10]. It helps in committing sins and enmity: the terrorist financer is therefore primarily providing support to the perpetrator of the criminal act, whether this act is committed or not, as cooperating with the terrorists means helping them in harming the society. The most severe penalties apply thus to TF as they also do to terrorism.

Transparency, good governance and measures against corruption

64. The Kingdom has signed, but not ratified, the United Nations Convention against Corruption on 9 January 2004.

65. The authorities believe that fighting corruption is an important target for the government. In summary, the Kingdom has a National Strategy for Protecting Ethics and Combating Corruption approved by the Council of Ministers[11], adopted the anti bribery law[12] and set up a law enforcement unit that is tasked to investigate and prosecute those who commit a bribery offence with public funds[13]. The anti bribery law has led to an unknown number of convictions, with penalties ranging from monetary fines to imprisonment (maximum of 10 years). The authorities have observed various forms of corruption in the Kingdom, in the private and public sector. The authorities indicated that transparency, protecting integrity and building confidence in both public and private sectors are considered important policies in Saudi Arabia. The Saudi government has made the objectives of eliminating all forms for corruption in government institutions, safeguarding the integrity and sincerity of its operations as an important element of all laws and regulations. The following specific measures have been taken:

- The Basic Governance Law requires close monitoring and assurance of proper use of all government funds; spending, collecting and protecting. In addition, monitoring extends to measure the performance of all government agencies and assure their good governance (articles 79 and 80).

- The Court of Grievances Law provides the basis for any person to appeal against any administrative decision, including violation of rules and regulations and abuse of power.

- The Public Audit Bureau Law stipulates that the public audit bureau's responsibilities are: "to ensure that all state revenues and receivables in the form of funds and services have been collected in accordance with the applicable regulations and that all expenses are in accordance with the annual budget and all administrative, financial and accounting laws", and that "all state movable and fixed funds are used for the purposes they are intended for by the relevant authorities and that these authorities possess the proper processes to ensure the safety of these funds and their proper use" (article 8, paragraph 1 and 2).

- The Authority for Monitoring and Investigation is responsible for monitoring the performance of all government employees in their duties and the investigation of cases of poor performance. The authority aims to ensure the good performance of the government and public institutions and to hold the underachievers accountable for their performance. Similarly, the Authority is

[10] The *Qur'an* reads, "cooperate on purity and devotion, not on sin and enmity" (5:2)
[11] Decree of Council of Ministers (43) (7/b/5657) on 1/2/1428 H
[12] By Royal Decree No. M /36 dated 29/12/1412.
[13] Council of Ministers Resolution No. 2111 / 8 to 1/12/1400H.

responsible for investigating crimes of bribery, fraud and crimes related directly to the use public funds and other offenses[14]. In addition, the financial monitoring department of the monitoring and investigation authority handles all cases referred to it in relation with financial violations. The department conducts examinations of these cases depending on the needs of the Authority's investigations and follows-up on the financial violations raised by other control bodies.

- Among the initiatives seeking to promote the values of transparency and integrity in the Saudi community, the Saudi government adopted a civil society initiative related to a good example prize that is awarded to companies, institutions and governmental and non-governmental authorities that create a transparent and fair decision making process qualifying as a role model. This award promotes proper ethical conduct in transactions with the objective of enhancing the level of performance and achieving the best interest and benefit of everyone.

1.2 General Situation of Money Laundering and Financing of Terrorism

Money laundering

66. Saudi authorities indicate that no criminal (trend) analysis has been undertaken but nevertheless believe there is a limited level of crime in the Kingdom. The authorities also state that it is too difficult to assess the size of the ML problem in the country. This is said to be due to the fact that every ML crime is connected to a predicate offence. The authorities consider that the majority of illegal proceeds within the Kingdom is generated from unlicensed business activities that violate commercial and labor laws. The Saudi government places a high priority on combating narcotics abuse and trafficking in narcotics and related crimes are punished harshly. As a result, the country says it does not have an appreciable illicit drug problem and is not a significant drug transit country. Therefore, proceeds generated from illicit drugs are said not to represent a major source of illegal funds and are thus not considered a problem.

Terrorist financing

67. Saudi Arabia's quest to modernize while respecting its traditional values and its relations with the West have caused some unrest in some instances. Minority groups seek to have more influence in the nation's governance. The presence of more than 6 million foreign workers also is thought by some to represent a risk to the national identity.

68. In the 1970s, a small group of people claimed that Saudi Arabia had abandoned its traditionalist roots in favor of Western corruption and tried to seize the Grand Mosque in Mecca. The Kingdom and its residents have been a victim of many more terrorist attacks. Since 1995, about 40 terrorist attacks have killed at least 160 citizens and government security personnel[15]. Terrorists have attacked foreign and Saudi citizens alike.

69. Networks originating in Saudi Arabia are said to provide financial backing for terrorist groups that operate in the Kingdom, the Middle East and around the world. This is in line with the indication of the authorities that the sources of funds used to finance terrorism and terrorist activities come from legal origins through the collection of donations, suspicious contributions and direct provisions. In February 2005, Saudi Arabia hosted its first-ever Counter-Terrorism International Conference. The government also

[14] Set forth in Royal Decree No. (43-1953).
[15] Not counting casualties among terrorists, where possible.

began a public relations campaign discouraging religious radicalism and terrorism. In addition, KSA also started an extensive terrorist rehabilitation program that is designated to counter the ideologies behind extremist movements.

70. The authorities indicate that one of the challenges in KSA's war on terrorism is the prevalent reliance on cash in the country (as opposed to other payment methods such as credit cards, electronic payment, checks, etc.), which makes it challenging to detect or follow TF cases. In addition, the sources of funds used to finance terrorism and terrorist activities mostly come from legitimate origins, e.g. through the collection of donations, suspicious contributions and direct provisions to terrorists.

1.3 Overview of the Financial Sector and DNFBP

Overview of the financial sector

71. The financial sector in the Kingdom is ruled by *Shari'ah*, which has an effect on the types of activities that can be undertaken. This *Shari'ah* based system is better known by its common name *Islamic Banking*. Not all financial activities are available in Saudi Arabia, although some non-Islamic financial activities are available, but not enforceable before court. All other non-Islamic financial activities are available under a modified contractual form (and name). The table below provides an overview that links the FATF terminology with the terminology used in the Kingdom. This report follows the terminology applied by the Saudi authorities.

Types of financial activities to which the FATF Recommendations apply	**Types of financial institutions in Saudi Arabia that conduct these specified financial activities**	**Legal basis for licensing (not necessarily financial sector supervision purposes)**	**Supervisor**
Acceptance of deposits and other repayable funds from the public	Banks	• Recommendation from SAMA. • Approval by the Ministry of Finance. • Approval by the Council of Ministers. • Obtaining a commercial registration from the MOCI and then a final approval from SAMA to start operation	SAMA
Lending			
Issuing and managing means of payment (e.g. credit and debit cards, cheques, travelers' cheques, money orders, bankers' drafts, electronic money)			
Financial guarantees and commitments			
Trading in money market instruments (cheques, bills, CDs, derivatives etc.); foreign exchange; exchange, interest rate and index instruments; transferable securities; and commodity futures trading			
Safekeeping and administration of cash and liquid securities on behalf of other persons			

Types of financial activities to which the FATF Recommendations apply	Types of financial institutions in Saudi Arabia that conduct these specified financial activities	Legal basis for licensing (not necessarily financial sector supervision purposes)	Supervisor
The transfer of money or value	Banks and class A money exchange	• Recommendation from SAMA. • Approval by the Ministry of Finance. • Approval by the Council of Ministers. • Obtaining a commercial registration from the MOCI and then a final approval from SAMA to start operation	SAMA
Money and currency exchange	Banks and class B money exchange		
Financial leasing	Financial Leasing Companies	• Recommendation from SAMA. • Approval by the Ministry of Finance. • Obtaining a license from SAMA. • Approval by the MOCI	SAMA
Underwriting and placement of life insurance and other investment related insurance	Insurance Companies	• Recommendation from SAMA. • Approval by the MOCI. • Approval by the Council of Ministers • Initial public offering by CMA • Obtaining a commercial registration from MOCI and then a final approval from SAMA to start operation.	SAMA
Participation in securities issues and the provision of financial services related to such issues	Investment Companies	• Recommendation from CMA • Approval by the MOCI • Approval from the Investment commission • Obtaining a license from CMA	CMA
Individual and collective portfolio management			
Otherwise investing, administering or managing funds or money on behalf of other persons			

72. As is shown in the table above, financial activities in KSA are provided by 4 types of FIs: *(i)* banks (commercial banks, money exchange and transfer of funds); *(ii)* insurance companies; *(iii)* financial leasing companies; and *(iv)* securities and investment firms. Banks, insurers and financing companies are supervised by Saudi Arabian Monetary Agency (SAMA), securities and investment firms by the Capital Market Authority (CMA). The number and types of financial services available in Saudi Arabia are strictly controlled. The majority of financial activities are concentrated within the commercial banking sector, and in money remittance and exchange services (which are in turn mostly offered by commercial banks).

73. Registration/establishment of financial institutions, as can be seen in the table above, is done at the MOCI. This procedure applies to all companies (establishment of financial institutions as companies is a prerequisite for licensing), and can be compared with some countries' domestic company registration procedures. In the case of FIs, SAMA and CMA license businesses for financial sector supervision and business-conducting purposes. Banks are all licensed by SAMA, and it seems that CMA has completed the licensing of securities firms. Leasing companies are not licensed, and only half of the insurance sector is licensed. The Implementing Regulations of the AMLS (Article 6.1) give AML/CFT-related supervisory powers to supervisory authorities vis-à-vis both FIs and non-FIs. As for actual on-the-ground supervision, banks are supervised, also for AML/CFT purposes. It is unclear if leasing companies are supervised. Securities firms have just been licensed and regular supervision is yet to start. The same is true for insurance firms; about half of the existing firms are by now licensed, but regular supervision has not yet started.

Banking sector

74. The banking sector in the KSA consists of commercial banks, money transfer and exchange businesses. SAMA is the supervising authority for the banking sector. In December 2008, 23 banks were operating in the Kingdom (12 domestic banks, 5 branches of banks from other Gulf Cooperation Council (GCC) member states, and 6 branches of foreign banks). The banks offer the full range of commercial banking services, and in some cases banks own other companies that offer insurance and securities services (through separate legal entities). Foreign banks are currently prohibited from operating directly within the Kingdom. Banking within Saudi Arabia is regulated by SAMA, in cooperation with other authorities (see table above). SAMA also issues and controls currency, regulates money supply and manages foreign assets.

75. Money transfer and exchange businesses are considered part of the banking sector, but are separately licensed and supervised. Supervision is undertaken by SAMA, but it is the MOF and the MOCI that issue the licenses (upon recommendation by SAMA). Based on the Banking Control Law[16] (BCL), the MOF offers two types of licenses, one that allows business to offer money transfer and exchange services (6 institutions), and a second license that only allows for exchanging money (24 institutions).

76. In this report, the term banks or banking sector applies to commercial banks, money transfer and money exchange businesses, unless otherwise indicated.

Insurance sector

77. Insurance services were first offered only by branches of foreign banks (before foreign banks were prohibited from operating directly) and branches of foreign companies. In time, mandatory health and car insurance, created a need for a domestic insurance company, which in time created the need for a legal and supervisory framework. This framework was completed in July 2003 with the Cooperative Insurance Companies Law[17] (CICL) and April 2004 when the MOF issued the supporting Insurance Regulations[18] (IR). The CIC only allows for cooperative insurance companies by locally incorporated public joint stock companies to offer general insurance, health insurance, life insurance (also known as "protection and saving insurance", or *takaful*, or Islamic insurance). Commercial for-profit insurance is not allowed.

[16] 1966.
[17] Royal Decree No. (m/32) on 2/6/1424 H.
[18] Resolution from the Ministry of Finance on 1/3/1425 H.

SAMA is the regulatory entity, in cooperation with other authorities (see table above). By December 2008, 18 businesses had received a license, of which 16 have foreign shareholders (who can own a maximum of 49% of all shares). 15 more companies are in the process of acquiring a license; six of those have started offering insurance business before the issuance of the CICL and SAMA becomes in charge of their supervision. Of the 18 licensed companies, 4 offer life insurance. There are 47 insurance intermediaries (brokers, agents, damage experts) operating in the Kingdom. SAMA issued AML/CFT regulations for the insurance sector in January 2009. As SAMA is still licensing the insurance sector, regular supervision has yet to begin[19].

78. It should be noted that the insurance sector is the KSA consists mainly of non-life insurance. Only 5% of the market consists of life insurance (premiums 2008: SAR 500 million), of which most is said to be group life. The assessment team notes this as it also notes the healthy growth in this sector over the last years and its potential to grow.

79. The legal gaps for insurance companies (lack of licensing, absence of regular supervision) have a negative impact on all FATF (Special) Recommendations that are targeted towards FIs. Those gaps are only repeated in the rating boxes for each FATF (Special) Recommendation (where applicable), not in the description of each sector.

Financial leasing companies

80. The Kingdom has two financing leasing companies (dealing in real estate financing and mortgaging, and in sale on installments company). SAMA is the supervisory authority for this sector, based on a MOF resolution[20] of 1999. However, there is no other legal framework for this sector, which inhibits further economic growth in this area.

81. The legal gaps for financial leasing has a negative impact on all FATF (Special) Recommendations that are targeted towards FIs. This gap is only repeated in the rating boxes for each FATF (Special) Recommendation (where applicable), not in the description of each sector.

Securities sector

82. The securities market, the Saudi depositing centre and the Saudi stock exchange (*Tadawul*) are supervised by the CMA. This agency was established in 2003 (Capital Market Law, CML). The CMA has licensed 114 entities under de CML, performing all kinds of securities services (stock exchange dealers, management companies, depositary institutions and securities firms). Any license will specify the services a company is allowed to provide, and the CMA maintains a publicly available register on its website. The securities sector is developing fast in the Kingdom (more products and more customers), which also increases the possible ML/TF risk that this sector can pose.

Overview over the DNFBPs Sector

83. There are real estate agents, dealers in precious metals and stones, lawyers, accountants and trust and company service providers in the Kingdom. Although the FATF Recommendations do not require

[19] It should be noted that, according to the authorities, those unlicensed insurance businesses are also supervised. However, as the assessment team did not meet with such unlicensed companies, this could not be verified.
[20] Minister of Finance's Resolution No. 1/1566 on 21/7/1420 H.

licensing for non-casino DNFBPs, authorities stressed that licensing is a key feature of the Saudi AML/CFT system for DNFBPs. Although the licensing is not undertaken for AML/CFT purposes (all business activity in the Kingdom is licensed) and does not directly relate to the AML/CFT system, it is a helpful tool for the authorities to identify and reach out to DNFBPs. This equally applies to the supervision that any business activity in the Kingdom is subject to.

Casinos, including internet casinos

84. Casinos and internet casinos are prohibited under Saudi law.

Real estate agents

85. There are real estate agents in the Kingdom, licensed for general purposes by the Ministry of Commerce and Industry (MOCI). Registration with the Ministry is compulsory, although compliance with the requirements is said to have been low[21]. There are 2810 real estate agents active in the Kingdom. All real estate businesses are subject to know your customer, record keeping and reporting requirements of the AMLS.

Dealers in precious metals and stones

86. There are 5407 dealers in precious metals and stones in the Kingdom, licensed for general purposes by the MOCI. It is illegal to trade in precious metals and stones without a license from the Ministry. The precious metals and stone market in Saudi is the largest in the Middle-East. All companies dealing in precious metals and stones are subject to know your customer, record keeping and reporting requirements of the AMLS.

Lawyers

87. There are 1200 lawyer's offices in the Kingdom, licensed for general purposes by the Ministry of Justice (MOJ). All lawyers are subject to know your customer, record keeping and reporting requirements of the AMLS.

Notaries

88. Although notaries exist in Saudi Arabia, these are always MOJ employees, and therefore considered not to be notaries as defined by the FATF. The task of notary offices would be best compared to those of cadastre offices in other countries.

Accountants

89. There are accountants in the Kingdom, licensed for general purposes by the MOCI. Registration with the Ministry is compulsory. All accountants are subject to know your customer, record keeping and reporting requirements of the AMLS.

[21] Arab news *Al Jasser* may usher in new banking era, Monday 2 March 2009 (6 Rabi al Awwal 1430).

Trust and company service providers

90. Trust[22] and company services (TCS) are not subject to independently/specifically tailored legal requirements and therefore are not existent under such name. However, TCS can be provided in the Kingdom by a non-regulated and non-defined group of persons and businesses. Some authorities and private sector bodies confirmed the existence of businesses that provided company services, and others indicated that in the absence of a legal framework to regulate Company Service Providers (CSPs) these services could be provided by anyone – although it is likely that these would be provided by lawyers and authorized persons. Some of the businesses defined as TCSP businesses by the FATF Recommendation seem to match services that need authorization by the CMA (providing an office and acting as a nominee shareholder), which means that these TCSP services would be covered by the securities sector requirements.

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

Commercial legal entities

91. There are some rules that are equal for any commercial legal entity in the Kingdom. All commercial legal entities need to be established at the MOCI. They are defined by the law as a group of persons and finances for which an independent, personal entity is available, aiming at achieving a certain purpose and has a legal personality in the limit of this purpose. All commercial entities share the following characteristics: they *(i)* are a group of persons and finances with independent personal liability; *(ii)* are established for a certain purpose or objective and seek to achieve this purpose and objective; *(iii)* are acknowledged by law, which means that they meet the criteria for obtaining legal personality and request to be granted this status; and *(iv)* have approved a memorandum of association and Articles of association. Each commercial legal entity also must have a name, a domicile and the capacity to act.

92. The following commercial legal entities can be established in Saudi Arabia: *(i)* joint partnership company; *(ii)* simple partnership company; *(iii)* venture company *(iv)* shareholding company *(v)* limited share partnership company; *(vi)* limited liability companies; *(vii)* companies with a variable capital; *(viii)* and legal companies. It is unclear what the exact differences between these different types of companies are, as the Saudi authorities did not explain this in detail. It is also unclear to what level these legal entities can or cannot be misused for ML or TF, and for what reasons. The Saudi authorities did not express any views about potential misuse for AML/CFT.

Non-profit legal entities

93. The following non-profit legal entities can be established in Saudi Arabia: *(i)* general charities; and *(ii)* educational charities[23].

94. General charities, which can be charitable societies or special charity institutions, are registered, licensed and supervised by the Ministry of Social Affairs (MOSA).

[22] The official name for the type of legal arrangement that exists in the Kingdom is private *waqf*. In this report, the term trust is also used to denote a private *waqf*.

[23] Note that a general *waqf* is an NPO, while a private *waqf* is a legal arrangement.

95. The Ministry of Islamic Affairs is responsible for registering, licensing and supervising the educational charities and the general trusts. There are two types of such charities, those which run *Qur'an* schools and *da'wahs* which have the task of promoting religion.

Legal arrangements

96. Private *waqfs* are set up like Anglo-Saxon trusts, with the exception of the addition of a judge who supervises the particular trustee(s) and trust.

1.5 Overview of strategy to prevent money laundering and terrorist financing

1.5.a AML/CFT Strategies and Priorities

97. The authorities indicated in the questionnaire that led up to this assessment that they are well aware of the possible risk that ML and FT pose to the Kingdom, including the possible shame it brings on the Kingdom. Preventing ML, TF and the negative side effects is a priority for the authorities. There is no single overarching national policy or strategy paper or document that would set out the government's AML/CFT strategy and priorities, but separate bodies, such as the PCCML, have set out their implementation strategies.

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

Ministries

Ministry of Interior

98. The Ministry of Interior (MOI) is the primary ministry responsible for internal security matters. It is the main responsible body for the AMLS. Formally, it shares the AML/CFT policy-making and implementation functions with the MOF, in practice this means SAMA and CMA. The MOI executes actions under international treaties and security cooperation agreements with other countries, including mutual legal assistance. It oversees communications and relations with counterpart security agencies in other countries and with Interpol. The MOI chairs the Permanent Committee on Combating Terrorism (PCCT). Law enforcement bodies are generally part of MOI, with some exceptions.

Ministry of Justice

99. The Ministry of Justice (MOJ) supervises the judicial system in the KSA. It is also responsible for ensuring that the notaries (its employees) comply with the AML/CFT requirements (including registration and authentication of real estate transfers) and for supervising the bar system.

Ministry of Foreign Affairs

100. The Ministry of Foreign Affairs (MOFA) is the receiving authority for assistance applications from other countries if sent through diplomatic channels (urgent requests are dealt with via Interpol, which is handled by MOI).

Ministry of Commerce and Industry

101. The Ministry of Commerce and Industry (MOCI) has oversight over implementation of commercial laws. It issues licenses to natural and legal persons desiring to undertake commercial activities in the Kingdom. The Ministry also is responsible for issuing AML/CFT directives for relevant businesses in the non-financial sector

Ministry of Social Affairs

102. The Ministry of Social Affairs (MOSA) is responsible for licensing, registration and supervision of general charities while the MOIA is responsible for the licensing, registration and supervision of educational charities as well as awareness.

Ministry for Islamic Affairs, Endowment, Da'wah and Guidance

103. The Ministry for Islamic Affairs, Endowment, *Da'wah* and Guidance (MOIA) is responsible for the licensing, registration and supervision of educational charities as well as awareness.

Ministry of Finance

104. The Ministry of Finance (MOF) drafts laws, policies and regulations for the financial and banking sectors in the Kingdom in coordination with the SAMA. It shares the responsibility with the Ministry of Interior for developing and implementing AML/CFT policies and procedures. Customs is part of the Ministry of Finance.

Policy coordination

Permanent Committee on Combating Money Laundering

105. The PCCML was established by Cabinet's Resolution[24] in May 1999. It is based at SAMA headquarters in Riyadh and is chaired and supervised by H.E. the Governor of SAMA. The PCCML is responsible for all AML/CFT related policy coordination, including ensuring implementation of the FATF Standards. The Committee heads the Saudi delegation to FATF, MENFATF and other international bodies. It has six members from the MOI (one for each law enforcement branch, including the FIU) and one member each from MOFA, MOJ, MOCI, MOF, Customs, the Prosecution Authority, CMA and SAMA. The Committee employs a vice president and secretarial staff.

Permanent Committee on Combating Terrorism (PCCT)

106. The PCCT was formed in December 2001[25] and has an oversight and coordination role for efforts in Saudi Arabia to combat TF. The four permanent members of the Committee are from MOI, General Intelligence, MOFA and SAMA. Six other (non-permanent) members may participate as appropriate. The Committee is chaired by a senior official from the General Intelligence Directorate (which is part of the MOI). The PCCT receives, examines and executes requests from other countries and international

[24] No. (5) on 17/1/1420 H.
[25] Royal Decree S/20167, dated 10/10/1422 AH (25 December 2001).

organizations in relation to the fight against terrorism. Foreign requests may be received through Interpol, MOFA, MOI or SAMA.

Permanent Committee on Mutual Legal Assistance (PCMLA)

107. The Permanent Committee on Mutual Legal Assistance (PCMLA) is chaired by the MOI. Its membership consists of representatives from the MOJ, the BIP, MOF, MOFA and SAMA. Its role is to process requests from foreign states for international cooperation or mutual legal assistance. SAMA is the gateway through which law enforcement agencies are able to obtain information from FIs.

Law enforcement bodies

Saudi Arabia Financial Intelligence Unit

108. The Saudi Arabia Financial Intelligence Unit (SAFIU or FIU[26]) is a law enforcement body under the MOI. It is supervised by the MOI Assistant Minister for Security Affairs. All the law enforcement bodies may be requested by the FIU for information or may investigate cases pertaining to their field of expertise and authority at the request of the FIU. Also the FIU has the authority to request to request the PA to execute seizures.

The Prosecution Authority

109. The Prosecution Authority (PA) is the body responsible for investigation and prosecution of crimes in the KSA, including ML/TF cases under the AMLS. In cases where other law enforcement bodies investigate cases, the PA is the supervisory body.

The Directorate of Public Security

110. The Directorate of Public Security (PSD) is the law enforcement body under the MOI that is responsible for combating all predicate offences that are not the responsibility of other bodies, such as the General Investigations Department.

The General Intelligence Directorate

111. The General Intelligence Directorate (GID) is the law enforcement body under the MOI, responsible for investigating terrorism, TF and bribery cases. It also investigates reports from the FIU on ML and TF.

The Anti-Drugs Directorate

112. The Anti-Drugs Directorate (ADD) is the law enforcement body under the MOI responsible for combating drugs. It also follows up on reports from the FIU, in cases where drugs may be involved.

[26] In this report, SAFIU and FIU both designate the Saudi Arabia Financial Intelligence Unit, unless otherwise indicated.

Saudi Customs

113. Saudi Customs is responsible for checking and clearing all travelers and goods that enter or leave the Kingdom. It has specific powers to enforce its laws. It is part of the MOF.

Financial supervisory bodies

Saudi Arabia Monetary Agency

114. SAMA is the monetary authorities/central bank of Saudi Arabia, a G20 country. It is the supervisory and regulatory body for all FIs in the Kingdom, except for the securities sector. As the SAMA chairs the PCCML, it is also the leading agency for AML/CFT matters. H.E. the Governor of SAMA has a cabinet rank.

Capital Market Authority

115. CMA, established in 2004, is the supervisory and regulatory body for the securities sector, which includes the Saudi Stock Exchange (*Tadawul*), on all matters, including AML/CFT. CMA's status is equal to that of a Ministry. It is also the sole depositary institution in KSA.

1.5.c Approach concerning risk[27]

116. Saudi Arabia has not formulated a risk-based approach to define which sectors should or should not be designated (which is an option, not a requirement, for countries). The KSA did not choose to limit applications of any FATF Recommendations on the basis of risk or on the basis of a limited size of a sector. This means that the Kingdom considers that all (Special) Recommendations fully apply to all FIs and DNFBPs (where these sectors exist in the Kingdom), regardless of the size and ML/TF risk of the sector.

1.5.d Progress since the last mutual evaluation

117. This is a joint mutual evaluation by the Middle East and Northern Africa Financial Action Task Force (MENFATF, مينافاتف) and the Financial Action Task Force (FATF). This is the first mutual evaluation of Saudi Arabia by MENAFATF.

118. This is Saudi Arabia's second assessment report by the FATF. The first assessment by the FATF was based on the previous standard (the 1996 FATF 40 Recommendations and 2001 FATF VIII Special

[27] An important consideration underlying the FATF Recommendations is the degree of risk of money laundering or terrorist financing for particular types of financial institutions or for particular types of customers, products or transactions. A country may therefore take risk into account and may decide to limit the application of certain FATF Recommendations provided that defined conditions are met (see FATF Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations).

Recommendations) and was conducted in cooperation with the Gulf Cooperation Council Secretariat[28]. The on-site visit took place in September 2003 and the report was discussed in February 2004.

119. The overall result of the previous evaluation was that Saudi Arabia demonstrated a high compliance with the FATF Recommendations. The authorities report that they have worked over the past years to address the few deficiencies identified in the previous report. The authorities indicate that they have significantly expanded the legal framework, adjusted and enhanced preventive measures, improved institutional cooperation, and invested in training and awareness raising. However, as was noted in the previous report, many elements of the AML/CFT system were still very recent. Examples are the AML Statute, which had just been adopted at the time, and the FIU, which had not yet fully functioning. This means that the previous assessment could not take implementation into account. In addition, the FATF Standards have significantly changed and the current 2003 FATF 40 Recommendations and 2004 IX Special Recommendations (as applicable at the time of the onsite visit) have set new thresholds for compliance in many (but not all) areas. Furthermore, previous assessments did not yet take effectiveness into account as current assessments do. This means that previous evaluations conducted under the old Standard and under the old Methodology should not be used as a benchmark to assess the level of progress of any country, especially with respect to the ratings.

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

The money laundering offence

120. As indicated in Section 1 of this report, the sources of law within the Kingdom of Saudi Arabia are *Shari'ah* (*Qur'an* and *Sunnah*), which is the primary basis for the legal system, and statutes (*i.e.*, written law, such as royal or ministerial decrees, regulations, international conventions, etc.) that have been issued or endorsed by the executive power. This second source of law must not contradict the precepts of *Shari'ah* law to be valid. It is important to be aware of the existence of the two sources, forming one inseparable legal framework, in order to understand properly the manner in which Saudi Arabia has approached establishing the offence of ML.

The money laundering offence

121. The offence of ML according to the *Shari'ah* is based on the principle that prohibits the dealing in monies that have been gained illegally. Saudi officials indicated that legal scholars find that evidence of prohibition of ML in the *Shari'ah* is plentiful whether from *Qur'an*, the *Sunnah* or from the entire body of *Shari'ah* jurisprudence (*fiqh*). Moreover, they stated that *Shari'ah* law was applied in ML cases prior to the

[28] The Gulf Cooperation Council (GCC) is a member of FATF; Saudi-Arabia is a member of the GCC. Therefore, evaluations of GCC member states were conducted by the GCC in cooperation with the FATF. At the time of the previous evaluation, the MENAFATF did not exist.

enactment of the AMLS in 2003. In an example provided by the Saudi authorities, a ML case was prosecuted as a *ta'zir* crime[29]. The case involved individuals who had transported or moved funds related to narcotics trafficking through bank accounts in the Kingdom. The penalty imposed in this case was fifteen years imprisonment (currently, the ordinary penalty for ML provided by the AMLS is up to ten years imprisonment).

Criminalisation of ML on the basis of the UN Conventions

122. Saudi Arabia has an Anti-Money Laundering Statute (AMLS) that was brought into effect in August 2003. The text of the law consists of 29 Articles. Interwoven into the statute is the AMLS Implementing Regulations. The Implementing Regulations provide additional rules and clarify definitions. The difference between both documents is that the Implementing Regulations are somewhat easier to amend. However, for the purpose of assessing Saudi Arabia's compliance with the FATF Recommendations, both documents are considered to form one document: AMLS.

123. The Vienna and Palermo Conventions require countries to establish as a criminal offence the following intentional acts: conversion or transfer of proceeds; concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to proceeds; and the acquisition, possession or use of proceeds [Vienna Article 3(1)(b) *(i)–(ii)* and (c) *(i)*, and Palermo Article 6(1)(a)*(ii)* and (b)*(i)*].

124. In Saudi Arabia, ML is criminalized by Articles 1.1 and 2 of the AMLS. Article 1.1 defines the act of ML as "Committing or attempting to commit any act for the purpose of concealing or disguising the true origin of funds acquired by means contrary to *Shari'ah* or law, thus making them appear as if they come from a legitimate source". This definition is the basis for the criminalisation of ML as further defined in Article 2[30].

125. Article 2 of the AMLS fully covers the requirements of the UN Conventions with respect to transfer, conversion, concealment or disguising, as well as acquisition, possession or use (Article 2 a – c AMLS). While the English translation of the AMLS seems to cover transfer and conversion of proceeds only partially, the language used in the Arabic original of the AMLS exactly copies the terms used in the Arabic versions of the Vienna and Palermo Conventions. Knowledge is also covered (see on Recommendation 2 in this section).

Property

126. The authorities indicated that *Shari'ah* defines property as everything a person owns and can benefit from. The AMLS defines funds as to include "assets of property of any type". This includes property rights and the proceeds from property rights (AMLS, Articles 1.2 and 1.3).

127. The AMLS is silent on the need to obtain a prior conviction for a predicate offence in order to convict anyone for ML. The authorities stated that it is sufficient for the proceeds to have been obtained in

[29] Court ruling Attorney General vs. X , 17/09/1419AH (4 January 1999).
[30] See the Annexes for a complete copy of the AMLS.

the context of the commission of a criminal offence under Saudi law and that there is no need for a prior conviction to have been obtained. The authorities' view is confirmed through case law[31].

Predicate offences

128. Saudi Arabia follows an all crime approach. Thus, all activity constituting a crime punishable by *Shari'ah* or statute is a predicate offence for ML. The AMLS lists examples of predicates offences (Articles 1 and 2.3.a – r), however, this list is not exclusive and does not replace the actual criminalisation of the predicates.

129. The following table shows for all predicate offences that are listed as "designated predicate offences" by the FATF (Glossary to the FATF 40 Recommendations, and shows if and how these are designated as predicate offence under Saudi law. As can be seen the 20 categories are covered as predicate offences, either in *Shari'ah* or by Royal statutes, with the possible exception of terrorist financing (see for the criminalisation of terrorist financing section 2.2 of this report). A full overview of the criminalisation of all predicate offences (including the language of the criminalisation) can be found in the annexes to this report.

Crime	Text from the Holy Quran	Text from the law
Being part of an organized criminal group and exacting money	Al MAEDA Verses (33) Al MAEDA Verses (2) Al BAQARA Verses (188)	Several agreements of the Kingdom criminalize the participation in an organized terrorist group and the provisions of article (17) of the AML law.
Terrorism including financing terrorism	Al MAEDA Verses (33) Al MAEDA Verses (2)	From the AML Law, article 1.2
Human trafficking and migrant smuggling	AN-NOUR Verses (33) AL- ISRA Verses (70)	United Nations Convention against Transnational Organized Crime (Palermo)
Sexual abuse including sexual abuse of children	Al MAEDA Verses (87) AL- ISRA Verses (32)	
Trading Narcotic Drugs and Psychotropic Substances	Al MAEDA Verses (90) AL-ARAF Verses (157)	Article 3 of the Law to Combat Drugs and Psychotropic Substances
Illegitimate arms trade	AN-NISA Verses (59) Al MAEDA Verses (2)	Articles 34 to 49 of the Arms & Munitions Law
Illegitimate trade of stolen commodities & other commodities	Al MAEDA Verses (38)	Crimes that the sentence is decided by virtue of the Sharia and therefore does not require the issuance of a law
Corruption and Bribery	Al BAQARA Verses (11-12) AL-ANFAL Verses (27)	Article 1 of the Law to Combat Bribery
Fraud	ASH-SHURA Verses (42)	Article 1 of the Law to Combat Commercial Fraud
Counterfeiting currency	Considered as an assault on currency that the Sharia protects and considers one of the five necessities	Anti-Forgery Law issued by virtue of Royal Decree no. 12 on 1379 no. M/38 on 23/10/1421 H. stipulating a sanction of prison for a minimum period of five years and a fine varying between 30000 and 500.000 Saudi Riyal.

[31] Case 76/28, General Court of Riyadh, 29/03/1429 H.

Crime	Text from the Holy Quran	Text from the law
Piracy of products and counterfeiting	Al MAEDA Verses (87) AT-TAWBA Verses (188)	Article 79 of the Law to Combat IT crimes Article 41 of the Copyright Law Along with the provisions of Paris Convention for the protection of Industrial Property and Berne Convention for the protection of Literary and Artistic Works
Environment and crime	AL-ARAF Verses (56)	Articles 13 and 14 of the Environment Law
Murder and causing severe bodily injuries	AL- ISRA Verses (33) AN-NISA Verses (93) Al MAEDA Verses (54)	Crimes that the sentence is decided by virtue of the Sharia and therefore does not require the issuance of a law
Kidnapping and forcible abduction and hostage taking	Al MAEDA Verses (87) Al MAEDA Verses (33)	International Convention Against the Taking of Hostages that the Kingdom joined by virtue of Royal Decree no. M/21 on 15/7/1410 H.
Robbery or theft	Al MAEDA Verses (38)	Crimes that the sentence is decided by virtue of the Sharia and therefore does not require the issuance of a law
Smuggling	AN-NISA Verses (59) Al MAEDA Verses (2)	Article 142 of the Customs Law
Extortion	Al MAEDA Verses (87) AL- BAQARA Versus (188)	
Forgery	Saying of Allah "So shun the fifth of idols and shun the false speech".	Article 5 of the Law to Combat Falsification
Piracy	AL-MAEDA Versus (23)	The Kingdom is committed to the related conventions and treaties according to the Basic law of Saudi Arabia articles (70) and (81)
Internal Trading and market manipulation	AL-BAQARA Versus (188)	Articles 49, 50, 57, 59 of the Saudi Capital Market Authority issued by virtue of Royal Decree no. M/30 dated 2/6/1424 H.

Foreign predicate offences

130. In the view of the authorities, jurisdiction to prosecute ML extends to predicate offences that occurred outside the territory of Saudi Arabia, as long as the asset generating offence (the activity) is considered an offence under Saudi law (it does not need to be criminalized in the jurisdiction where the act was committed). The statute does not make this explicit, as this is a principle that is covered by *Shari'ah*[32]. The authorities provided three cases where Saudi nationals were convicted for severe crimes (*i.e.* murder) committed abroad against Saudi nationals, however, there is, as yet, no case law applying the principle to offences that would traditionally be regarded as money laundering predicates.

Self money-laundering

[32] "Do not transgress limits, for Allah does not love transgressors" (*Qur'an* 5:87) and "Help you one another in righteousness and piety, but help you not one another in sin and rancour".

131. There is no legal distinction between laundering or self-laundering under Saudi law (Article 2 AMLS). Several persons are said to have been convicted for self-laundering and the authorities provided jurisprudence[33] to support their view. In this case, all four defendants were convicted for ML (possessing unexplained amounts of cash, transferring amounts on behalf of a third person) and drugs possession. However, the case does not establish that the persons are convicted for the laundering of proceeds gained through the possession of these drugs. In other words, the conviction of laundering is not based on the predicate offence of possessing drugs, which means that this is not a self-laundering case. In the absence of a clear self-laundering case, the assessment team sticks to its doubts as to whether self-laundering is covered.

Ancillary offences

132. The AMLS includes several forms of ancillary offences. Any natural person participating by way of agreement (including conspiracy/association), assistance, incitement, advice, counsel, facilitation, collaboration, covering, or attempt in committing a ML crime is deemed a perpetrator of ML and faces the same sanctions as the main perpetrator (Article 2.e AMLS), which is all in line with the FATF Standards.

Recommendation 2

Natural persons that knowingly engage in ML activities

133. The ML offence under the AMLS applies to all natural persons that engage knowingly in ML. There are no limits to this provision.

Inference from objective factual circumstances

134. The AMLS states that "knowing can be inferred from the objective and factual conditions and circumstances; thus creating an element of criminal intent constituting one of the crimes provided for in Article 2". This means that, in order to be able to prove the intentional element on the basis of factual circumstances, knowledge also has to be proven. Nevertheless, despite the language of the statute, Saudi Arabia provided jurisprudence that knowledge can also be inferred from objective factual circumstances (should have known)[34].

Criminal liability for legal persons

135. Article 3 of the AMLS establishes criminal liability of FIs and DNFBPs that commit a ML crime. Article 1.5 AMLS defines FIs and DNFBPs and Articles 1-2 and 1-3 of the AMLS list which specific FIs and DNFBPs are subject to the AMLS (see Section 1 of this report for a list of FIs and DNFBPs that are covered by the AMLS).

136. The Saudi authorities indicated that, in their view, the term "Financial and Non-Financial Institutions" in Article 1.5 includes all legal entities present in the Kingdom. However, the same term is used to define the entities that are subject to CDD, record keeping and reporting requirements, and it is safe to say that not all legal entities are covered by the AMLS requirements for CDD, record keeping and STR

[33] Case 76/28, General Court of Riyadh, 29/03/1429 H.
[34] Case 120/34, General Court of Riyadh, 10/06/1428 H

reporting. This means that the term only extends to FIs and DNFBPs, but that the criminalisation of ML does not extend to all legal entities. While on-site, the authorities were requested to provide jurisprudence (an example of a legal entities being criminally convicted), but such an example was not available.

137. No FI or DNFBP has ever been prosecuted or convicted for ML, but the penalty would be a maximum fine of SAR 5 million. After the on-site, the authorities indicated that at that time, four entities were subject to ML investigations, however, that does not mean that the legal entities themselves will be ultimately convicted under criminal law.

138. In the absence of a fundamental principle of law that would prohibit criminal legal liability for all legal entities, the authorities cannot resort to civil or administrative liability to comply with this feature of Recommendation 2. Nevertheless, it is unclear to the assessment team if civil or administrative liability exists, as the authorities made no references to such a framework.

Sanctions for ML

139. The sanction for ML under the AMLS is maximum ten year imprisonment and a maximum fine of SAR 5 million. Whether or not a fine is combined with imprisonment is up to the judge's discretion. The judge may also increase the maximum penalty by five years imprisonment, or a SAR 2 million extra fine if the ML act was committed *(i)* by a criminal organisation (consisting of at least three persons)[35]; *(ii)* or involved the use of arms ; *(iii)* or was committed by a civil or public servant in connection to his position; *(iv)* or if the act involved the exploitation of minors; *(v)* or if the crime was committed through a correctional, charitable or educational institution or through a social service facility; or *(vi)* if the perpetrator has a criminal record (especially for ML).

140. It is possible to obtain a conviction for ML under *Shari'ah*. The punishment for ML in that case is always equal to the punishment for the predicate offence (which could be more severe than the statutory punishments). It is up to the judge's discretion to determine the penalty for *ta'zir* crimes.

141. All ML cases are judged before the General Court, which is composed of three judges. There is a General Court in every large city of the Kingdom. There are 13 regional General Courts comprising approximately 400 judges that received specialized training on ML.

142. There is an exemption to the sanction. If a perpetrator ("*owner, possessor or user of the funds*") informs the authorities of the existence of the criminal funds prior to their knowledge, and informs the authorities of the source of the funds and the identity of accomplices, without ever having benefitted from the funds (or their proceeds), the General Court may decide not to apply a penalty (AMLS Article 16).

Statistics

143. The following table gives an overview of the ML cases before court between 2004 and 2008. These 237 court cases are based on 208 investigated cases. It should be noted that, under the AMLS, there is no difference between ML and TF. It is unclear how many of these cases are ML cases, and how many

[35] The Saudi authorities referred to definition of organised crime contained in the Palermo Convention, but no legal provision has implemented this definition at national level. In practice, this does not seem to pose a problem for the Saudi authorities. However, the failure to implement international conventions makes this issue rather vague and the extent to which it can apply in practice under Saudi law is consequently ambiguous.

are TF cases. That makes it difficult for the team to fully confirm that all these cases relate to ML and not to TF.

Statistic on investigated and convicted ML cases 2004 - 2008				
Year	**No. of Investigated Cases**	**Accusation**	**Kept Cases**	**No of Convictions**
2004	41	13	28	١٠(3)
2005	65	26	39	٢٦(0)
2006	45	39	6	35(4)
2007	130	41	89	34(4)
2008	225	48	95	24(2)

Number of ML cases before courts (2004 – 2008)					
City	**Cases before court**	**Total number of suspects**	**Convicted suspects**	**Acquitted suspects**	**Cases pending**
Assir	**4**	4	4	0	0
Tabouk	**3**	3	3	0	0
Mecca	**6**	6	6	0	0
Riyadh	**95**	68	47	8	13
Jeddah	**105**	204	82	75	47
Damman	**14**	26	19	0	7
Khobar	**1**	1	1	0	0
Medina	**9**	9	0	3	6
Total	**237**	**321**	**162**	**86**	**73**

Effectiveness

144. The Saudi authorities appear to have achieved an acceptable number of prosecutions and convictions in ML cases, despite the fact that TF is considered to be ML under the AMLS (which makes it difficult for the authorities to distinguish between ML and TF cases[36]. As a result it is difficult to fully confirm the effectiveness of the ML provisions as some of these may be TF cases. The maximum penalties in the law are adequate and harsher than in other countries. The cases that the team received suggest that the penalties that are applied by the courts are in general lower than the maximum penalty, but not too low to be ineffective. However, overall statistics on penalties are not available. Additionally, the number of convictions compared to the number of investigated cases is disproportionately lower.

[36] Specialized Criminal Court, decisions no. 40010083026290003 (date 23/12/1429H) and no. 060010123027290001 (date 25/12/1429H).

2.1.2 Recommendations and Comments

145. The Saudi authorities should be more precise in the formulation of the ML criminalisation and should strive for clear provisions that establish, without ambiguity the issues in relation to foreign predicate offences and the criminalisation of self-laundering. The authorities are also urged to make a conceptual distinction in the AMLS between the ML and TF. This difference would also be useful to gauge and enhance the effectiveness of the AML system, which is currently not fully possible (see also section 2.2 for similar problems related to TF).

146. The all crimes approach for predicate offences to ML is to be commended, which should ensure that the implementation of Special Recommendation II would confirm to the criminalisation of all 20 categories of designated predicated offences.

147. Criminal liability for legal entities should extend to all legal entities.

2.1.3 Compliance with Recommendations 1 & 2

	Rating	Summary of factors underlying rating
R.1	**LC**	• The AMLS / jurisprudence do not clearly cover self-laundering and do not clearly extend to predicate offences - that would traditionally be regarded as predicate offences - committed abroad. • Effectiveness of ML provisions could not be fully confirmed (definition of ML and TF). • Shortcoming in of criminalisation of terrorist financing possibly limits the number of designated predicate offences to 19.
R.2	**LC**	• Criminal liability does not extend to (all) legal entities and the extent to which administrative or civil sanctions apply is unclear. • Effectiveness of ML provisions could not be assessed (penalties)

2.2 Criminalisation of Terrorist Financing (SR.II)

2.2.1 Description and Analysis

Criminalisation of terrorist financing

148. Terrorism and terrorist financing are criminalized under *Shari'ah*[37]. Terrorism is considered an anti-society offence, for which the most severe penalties apply. Under *Shari'ah*, financing of terrorism is considered a window to terrorism, inseparable from terrorism. According to Shari'ah one of the most serious offences is killing others, which is closely linked to *corruption on earth*. While statutes could make a legal or conceptual distinction between the terrorist and his financier, under *Shari'ah* they are both considered terrorists[38] since any form of cooperation is considered as a terrorist offence and not an

[37] *Qur'an*: "The punishment of those who wage war against Allah and His Messenger, and strive with might and main for mischief through the land is: execution, or crucifixion, or the cutting off of hands and feet from opposite sides, or exile from the land"

[38] *Qur'an*: "Help you one another in righteousness and piety, but help you not one another in sin and rancour", "the one who clean in the house of corrupted people is not an associate, is one of them" since the TF is a form of professional assault according to what the Almighty says: "do not transgress, indeed Allah does not like the

associate crime. If the terrorist act would never be committed, the financing of the act would still be punishable. See also the first paragraph of Section 2.1 of this Report. KSA provided three case examples of persons being convicted for terrorism and / or financing of terrorism based on Shari'ah provisions.

Terrorist financing characteristics

149. In addition to the criminalisation of terrorism and TF under Shari'ah, there is also a reference to TF in the AMLS. This reference has not changed since the last FATF evaluation in 2004. AMLS Article 2(d) refers to "financing terrorism, terrorist acts and terrorist organisations" as a form of ML. In other words, TF is framed as a type of ML crime. It is not an independent offence and in most cases Article 2(d) is referred to as a predicate offence. Based also on the Arabic original language of the AMLS, it is the view of the assessment team that Article 2(d) should indeed be considered as one of the predicate offences to money laundering (relating to Article 1.7 AMLS), and not as a statutory criminalisation of terrorist financing. Nevertheless, the assessment team also noted that there is jurisprudence available that refers to terrorist financing cases under the AMLS. For example in one case, the conviction for terrorist financing was 10 year imprisonment and 500 lashes. However, the body of the case refers to the provisions of Shari'ah and not to the elements of the AMLS. Only the sentence at the end partially refers to ML (as defined in Article 2(d) of the AMLS). The boundaries between the statutory TF provision and Shari'ah are not clearly delineated.

150. Article 2 of the TF Convention is simply referenced in Article 2(3)(c) of the AMLS Regulations. It does not transpose Article 2 as a freestanding offence under Saudi law. In its current form, therefore, the Saudi statutory offence for the financing of terrorism does not appear to conform to international standards and requirements as expressed in the TF Convention.

151. The Saudi authorities explained that there is no need for a specific statutory offence because terrorist financing is already punishable under *Shari'ah*. Article 2(d) AMLS is thus merely a complementary statutory provision, which further elaborates on and is to be interpreted in line with the Shari'ah offense. As already stated in the previous assessment report, Article 2 (d) AMLS by itself is considered insufficient to meet the very detailed and specific provisions of the FATF Standards and the TF Convention. As a result, in 2004 Saudi Arabia was encouraged to promulgate a specific statute dealing with TF. However, based on the fact that FT is already punishable under the Shari'ah, no such law has been put in place and the current provision in the AMLS is considered by the team to constitute a predicate offence to ML. The current formulation of the FT offence in the KSA legal system has an effect on the overall assessment of this Special Recommendation, especially in those cases where the authorities referred to provisions of the AMLS to establish that elements of Special Recommendation II are met. These includes *(i)* an insufficiently broad definition of funds (not in line with the TF Convention); *(ii)* uncertainty if funds have to be used for a specific terrorist acts or linked to a specific terrorist act; and *(iii)* no clarity if the provision in the AMLS covers carrying out a terrorist act by a terrorist organisation of less than 3 persons.

152. The Kingdom has ratified 13 out of 13 terrorism related UN Conventions, but the authorities could not establish that the conventions have been implemented, especially with respect to the criminalisation of the criminal conduct (see also Section 6 of this report). As with all FATF assessments,

transgressors" and information contained in Specialized Criminal Court, decision no. 40010083026290003 (date 23/12/1429H) (the conviction is for ML).

the statement that an International instrument becomes part of the national law through ratification is not considered to equal (effective) implementation.

Terrorist financing as a predicate offence for ML

153. TF is punishable as ML through Article 2(d) of the AMLS (see above). In addition, Article 1.1 and 1.7 AMLS both indicate that any act contrary to *Shari'ah* (and TF is contrary to *Shari'ah*) is considered to be a predicate offence for ML.

Jurisdiction over TF offences

154. The Saudi authorities indicated that there was no obstacle to the prosecution of offences that had occurred in another state, based on Shari'ah provisions. See also on the criminalisation of foreign predicates in Section 2.1 of this Report.

Inference from objective factual circumstances and criminal liability for legal persons

155. In a TF case, in order to be able to prove the intentional element on the basis of factual circumstances, knowledge also has to be proven, whereby the prosecution can rely on objective factual circumstances) [39].

156. Criminal liability for legal persons does not extent to legal entities other than FIs and DNFBPs and it is unclear whether legal persons are subject to civil or administrative sanctions under Saudi law (see on Recommendation 2 in this section of the report).

Sanctions

157. As explained above, in some cases the behavior of the suspect is sentenced on the basis of the AMLS, even though the act is proven on the basis of *Shari'ah*. It should also be noted that the judge has full discretion under *Shari'ah* to apply whatever sanction is deemed appropriate for the act that was proven to have been committed. This means that the sanctions below are not in all cases the maximum sanctions. See for example the above mentioned case, where the defendant was sentenced to 10 years imprisonment in conformity with the AMLS, and in addition to 500 lashes in conformity with *Shari'ah*. The sanctions for TF under the AMLS are equal to those for ML (see Section 2.1 of this report) and range from ten years imprisonment and a fine of SAR five million for regular TF to 15 years and a fine of SAR seven million for aggravated forms of TF. The possibility to be pardoned by court in case of preventive cooperation with the authorities also applies to financing of terrorism.

158. Possible punishments for TF under terrorism are: i) execution; ii) crucifixion; iii) amputation of hands and feet from opposite sides; or iv) deportation (into exile). The sentence for TF punishment depends on the type of the terrorist act.

Statistics

159. Saudi authorities reported that a total of 478 persons were prosecuted for terrorism, of which 74 for TF. Of those 74, 60 persons were convicted, representing a total of 27 cases. The authorities indicated

[39] Case 120/34, General Court of Riyadh, 10/06/1428 H

that all convictions were based on the AMLS. As with the statistics for ML, there is some statistical uncertainly about the difference between ML and TF. For example, during the discussions with the authorities, the authorities presented TF cases as ML cases (and vice versa) and different authorities would present different views as to what would constitute a ML case or a TF case under the AMLS. It is unclear what the time period is for those 60 convictions. In addition, the 478 persons that were prosecuted include 166 persons that were included in a terrorism related law enforcement watch list (see also Section 2.4 of this report).

Effectiveness

160. It is difficult to assess the effectiveness of the TF provision because of the statutory ML provisions that are used to convict terrorist financiers for ML, even if the act has been proven under the terrorism and terrorist financing provisions of *Shari'ah*. The provisions of the AMLS on TF are identical for those for ML; and the provisions of *Shari'ah* for TF and terrorism are identical. This makes it difficult for the assessment team to gauge if the TF provisions are as effectively used as they should be. Overall it is sufficient; however, the assessment team also believes that effectiveness could be further improved if the authorities would enact specific provisions to criminalize TF.

2.2.2 Recommendations and Comments

161. The Saudi authorities are advised to enact a full statutory criminalisation of TF, structuring it as a separate offence from the ML offence, to replace the current reference to TF in Article 2(d) of the AMLS in order to meet the requirements set out in Article 2 of TF Convention but also to clearly distinguish money laundering and terrorism financing offences. Furthermore, unless the KSA authorities enact a specific provision to criminalize TF, the effectiveness of the legal framework cannot be properly assessed (as abovementioned, the AMLS provisions are used to convict terrorist financiers for ML even if the criminal activity was criminalized as TF under Shari´ah) All elements of Special Recommendation II and the TF Convention should be covered in KSA, something which the assessment team was unable to establish, but which the authorities insist is the case for the Shari'ah provisions. In addition, the mere ratification of the TF Convention without proper implementation is insufficient; and the TF Convention needs to be specifically implemented into statutory law.

162. However, notwithstanding the lack of legal provisions which criminalize TF in line with the TF Convention, the team also notes that terrorist financiers are prosecuted and convicted and that the system produces results. The Saudi authorities have also shown a commitment in the fight against terrorism financing by establishing an *ad hoc* court which deals with this offence and already has issued a significant number of convictions. In view of the lack of legal provisions adequately criminalizing TF, in line with the TF Convention, the rating would have been NC, regardless of the number of prosecutions and convictions issued in the Kingdom and steps taken by its authorities. However, in this particular regard, the assessment team is fully aware that this rating does not properly reflect the KSA authorities' commitment and efforts to achieve results in terms of convictions but rather reflect the state of play of its legal framework in relation to the criminalisation of TF and the TF Convention. For this reason, the final rating is set at PC.

2.2.3 Compliance with Special Recommendation II

	Rating	Summary of factors underlying rating
SR.II	**PC**	• No stand alone statutory TF offence • TF not criminalized in line with the TF Convention • TF as a ML offence does not extend to all legal entities • Insufficient definition of funds as required by TF Convention • TF as a ML offence does not cover acts by terrorist organisations of less than 3 persons • Unclear if funds have to be used for a specific terrorist act or linked to a specific terrorist act. • The term "financing" does not clearly cover the collection of funds. • The term "terrorism or terrorist act" does not clearly cover the acts contemplated by Article 2(1)(b) of the FT Convention. • The financing of terrorist acts contemplated by Article 2(b) of the FT Convention in relation to conventions not yet ratified by the KSA are not covered. • Financing a terrorist organisation or individual terrorist for any purpose (*i.e.* not related to a terrorist act) is not covered.

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

2.3.1 Description and Analysis

Introduction

163. Saudi Arabia has two frameworks for confiscation, freezing and seizing of proceeds. The first framework is based on provision of *Shari'ah* and applies to all proceeds of crime. The second framework is based on the AMLS, targets the proceeds of ML (as a part of the sanction provisions for ML).

Confiscation of proceeds of all crimes

164. Under *Shari'ah*, it is not relevant who owns criminal property (criminal or a third party), the law permits the confiscation of properties related to the offence regardless of whom it is held by. This includes any proceeds of crime, psychotropic substances, and instrumentalities used for the commission of an offence. This is a fundamental principle of the *Qur'an* and the teachings of the Prophet. To better understand the legal reasoning, one might compare the way proceeds are treated under *Shari'ah* to the way prohibited goods (like illegal guns or drugs) are treated in most jurisdictions. In both cases, the goods are treated as an illegal good that can be confiscated because it is a prohibited good.

Confiscation pursuant to the AMLS (ML cases only)

165. The AMLS contains specific provisions for confiscation in AML/CFT proceedings. It is defined as the "expropriation of funds, proceeds or instrumentalities used in the crime pursuant to the ruling of a competent court". Confiscation is a mandatory sanction in ML/TF cases (AMLS Articles 1.9, 15-16). The confiscation provisions cover i) proceeds; ii) instrumentalities used in; and iii) instrumentalities intended to use for.

- The definition of proceeds is "any funds generated or earned directly or indirectly from ML and predicate offences". Funds is defined as "assets or property of any kind, tangible or intangible, movable or immovable, as well as legal documents or instruments proving ownership of assets or any right to it". (AML Articles 1.2 and 1.3).

- Instrumentalities is defined as "anything used or meant to be used in any way in committing a crime subject to sanctions hereunder" (AMLS, Article 1.4).

166. Property of corresponding value may be confiscated if the proceeds of crime have been "mixed" with legitimate property. Where the proceeds have been dissipated, the relevant authority must estimate their value by seeking the assistance of experts before a judgment may be rendered (AMLS, Article 16). As with any other good that is subject to confiscation under *Shari'ah*, it is irrelevant if the asset is held or owned by the criminal or a third party (see below).

Provisional measures (AMLS and CPC)

167. The AMLS, that provides a definition on provisional measures in Article 1.8, only enables SAFIU to request the Prosecution Authority to freeze or seize any funds for a maximum of 20 days (Article 12). For this, SAFIU needs to be able to confirm that the STR is indeed, suspicious. SAFIU has to be informed within 48 hours if its request is granted. The 20 days may be extended by court order, on request of the Prosecution Authority. Despite the fact that it might appear that only SAFIU is empowered to apply for the adoption of provisional measures, under Article 12.10, the monitoring agencies and authorities in charge of combating money laundering may request the Financial Intelligence Unit in ML cases to impose the preventive seizure in compliance with the period specified in the Law. It should be highlighted that there are no corresponding provisions on freezing or seizing any funds regarding predicate offences/TF because the FIU does not deal with predicate offences.

168. KSA authorities also pointed out that seizing measures may also be applied in the course of criminal investigations or upon request by other law enforcement authorities (CPC, articles 24, 26, 27 and 43). For this measure, it is not necessary that a request from SAFIU is being received. According to these provisions, investigation officers under supervision of the Bureau of Investigation and Prosecution may arrest "information and evidence necessary for the investigation and indictment", thus including property that is or may become subject to confiscation. However, the objective of this power seems to be to preserve evidence or information in view for a potential indictment. This power does not refer to ML/predicate offences and the assessment team could not confirm the effectiveness of this mechanism with figures.

169. Supervisory authorities may also request SAFIU to initiate a freezing request to the Prosecution Authority (AMLS, Article 12.10).

170. Seizure applications are dealt with on an *ex-parte* basis (unilaterally and without prior notice of the owner of the funds). This is based on the fact that the CPC does not require any prior notification.

Powers to identify and trace property (AMLS and CPC)

171. Articles 24 to 29 of the Law on Criminal Procedure provides that law enforcement authorities, under the supervision of the Prosecution Authority, may search for, collect and seize information and evidence necessary for the investigation of an indictment for a crime. Article 56 of the Law on Criminal Procedure provides that the Prosecution Authority may issue seizing orders relating to mail, publications

and parcels, whereby the order is valid only for 10 days. Article 12 of the AMLS also provides the FIU with the necessary powers to identify and trace property subject to confiscation

Bona fide third parties

172. The authorities indicate that any confiscation procedures based on the AMLS explicitly exclude bona fide third parties. However, *Shari'ah*[40] and the AMLS (article 21) only provide that the punishment (confiscation is a sanction under the AMLS) will not apply to those who could have been prosecuted, but are not because they violated the law in good faith. However, that excludes the much wider circle of bona fide third parties that did not violate any law, like creditors or persons but happen to be in the possession of the property that is subject to confiscation.

Authority to void actions and contracts

173. Under *Shari'ah*, all actions, contracts, conducts, and activities are subject to the provisions of Islam, thus what is consistent with Islam is left untouched, or otherwise it is prevented. This is no different from general provisions found in civil law countries.

Statistics

174. In view of the number of convictions for ML (162 convictions between 2004 and 2008) and the provisions for mandatory confiscation in ML cases, the number of applications between 2005 and 2008 (54 applications) for provisional measures is not significant. The authorities did not provide comprehensive figures to show the monetary amounts that have been confiscated (or the corresponding amount in the case of confiscated goods) (see below). In addition, it appears that the Saudi authorities do not distinguish between domestic applications for confiscation and provisional measures and those resulting from the implementation of foreign requests and the implementation of UNSCR 1267 and 1373 (478 individuals whose accounts were seized) which makes it even more difficult to interpret the figures. While there are provisions for seizure in the CPC (as part of the powers to collect evidence), there are no separate statistics available on the use of these provisions (that would apply to ML, TF and predicate offences). Without a comprehensive overview of these figures, it is not possible to confirm the effectiveness of the system. The figures that are available (see below) are insufficient to establish the effectiveness of the system.

175. The following statistics are available. It is unknown if these statistics are based on the AMLS or the CPC: In ML cases, the authorities report that between 2005 and 2008, an annual average amount of SAR 5.5 million was seized and SAR 800 000 was confiscated in ML cases. Additional, over the entire period, 28 (9) cars, 34 (12) mobile phones and 19 (9) computers were seized (confiscated). In TF cases, the authorities have confiscated between 2005 and 2008 an annual average amount of SAR 71 000. In narcotics cases, the ADD confiscated between 2004 and 2008 and annual average amount of SAR 3.5 million (23 cases total). In other predicate offences, the authorities confiscated between 2004 and 2008 an annual average amount of SAR 500 000 (alcohol smuggling), SAR 20 000 (forgery), SAR 62 000

[40] Al-Zumar 39:7: If you become ungrateful, then (know that) indeed Allah is Independent of you; and He does not like the ungratefulness of His bondmen; and if you give thanks, He is pleased with it for you; and no burdened soul will bear another soul's burden**;** you have then to return towards your Lord – He will therefore inform you of what you used to do; undoubtedly, He knows what lies within the hearts.

(counterfeiting currency), SAR 500 000 (prostitution), SAR 6 million (fraud and embezzlement), and SAR 110 000 (bribery).

Effectiveness

176. The Saudi authorities provided the assessment team with statistics and information on confiscation and provisional measures. As confiscation is a mandatory sanction in ML cases, one should expect more confiscation cases. In addition, the assessment team has some concerns over the scope of the confiscation provisions. Currently, the authorities solely use the confiscation provisions as sanction (repressive tool). However, the purpose of confiscation is also to restore a situation (as it was before a crime took place) and it is also a preventive investigative tool. The cases that the assessment team discussed, funds were usually seized and later confiscated as the instrumentalities of the ML crime found *in flagrante delicto* (caught in the act), and the team was not made aware of a policy of the authorities to focus on financial investigations and targeting all possible criminal property of a launderer. The authorities confirmed that no provisional seizure request (AMLS, Article 12) has ever been rejected, even though the provisional powers available under the AMLS are too limited and can only be used in STR/ML cases.

2.3.2 Recommendations and Comments

177. There is a mechanism for provisional seizures (AMLS, Article 12) with a clear procedure allowing the FIU upon substantiating suspicion to request the Prosecution Authority to apply such measures. The procedure is only open to the FIU, although this body could send the application for provisional measures following a request of other law enforcement agencies. Considering the low number of cases that passes through the FIU (compared to the total number of criminal cases in the Kingdom) and considering that the FIU would mainly deal with ML cases and not with predicate offences, the statutory system is too narrow. The authorities could also not explain how the provisions based on the AMLS and the evidence preserving provisions of the CPC relate and interact.

178. A further difficulty arises with the protection of third parties acting in good faith because the legal framework does not afford adequate protection ("the punishment shall not apply to those who violate in good faith"). This measure should be accompanies by complimentary measures that protect those acting in good faith regardless of whether such persons are involved in any violation.

179. The effectiveness of the system for seizure and confiscation of funds related to ML, TF and predicate offences could not be established. There are some statistics available, however, these are incomplete, and the number and amount of confiscations is insufficient in light of the mandatory provisions of the AMLS and insignificant in relation to the overall amounts confiscated. The authorities should take steps to ensure a broader application of seizure and confiscation measures.

2.3.3 Compliance with Recommendations 3

	Rating	Summary of factors underlying rating

R.3	**PC**	• Insufficient protection of bona fide third parties
		• Effectiveness of the CPC is not established:
		  o due to the lack of implementation (insignificant number and amounts)
		  o due to lack of experience with the CPC provisions
		• Effectiveness of the AMLS system is limited because:

	Rating	Summary of factors underlying rating
		○ the confiscation provisions are not implemented as widely as their mandatory nature suggests • The framework to request for provisional measures does not clearly cover predicate offences • Interaction between AMLS and CPC unclear.

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

2.4.1 Description and Analysis

180. The intent of Special Recommendation III is preventative[41], as is explained in paragraph 2 of the Interpretative Note to Special Recommendation III. As described in more detail below, there is no proper legal basis for the implementation of UNSCR 1267. The legal framework that does exist for implementing UNSCR 1267 and 1373 places responsibility for implementation of these resolutions on ministries and not FIs or DNFBPs. This is because government ministries are the entities that regulate issues pertaining to the functioning of FIs and DNFBPs; such entities are therefore responsible for ensuring compliance with the requirements of UNSCR 1267. Although this does not amount to effective implementation and falls short of the standard set forth in SRIII, it must be noted that the Saudi asset freeze obligations that are in place deal with funds or other assets in the context of a criminal, civil or administrative investigation or proceeding (as is for example required by the Vienna and Palermo Conventions). Further, it should be underlined that the KSA has implemented a repressive and preventative framework for dealing with UNSCR1267 which does yield results on the basis that the KSA takes law enforcement action to respond to UN 1267 designations. This does not, however, apply to UNSCR 1373. It will be recalled that UNSCR 1373 requires states to establish a domestic framework for implementation; it is not possible for states to respond to an international decision, as there are no such decisions to respond to. No such domestic framework is in place in the Kingdom.

181. The foregoing must be borne in mind when reviewing the system for freezing funds used for terrorist financing in the Kingdom, in particular when reading the discussion on some of the sub-criteria of Special Recommendation III set forth below. The description below analyses the system as it is and explains the statistics that have been produced; it acknowledges that the system that has been put in place has in fact produced some results,

[41] FATF Interpretative Note to Special Recommendation III, paragraph 2 reads: "*The objective of the first requirement is to freeze terrorist-related funds or other assets based on reasonable grounds, or a reasonable basis, to suspect or believe that such funds or other assets could be used to finance terrorist activity. The objective of the second requirement is to deprive terrorists of these funds or other assets if and when links have been adequately established between the funds or other assets and terrorists or terrorist activity. The intent of the first objective is preventative, while the intent of the second objective is mainly preventative and punitive. Both requirements are necessary to deprive terrorists and terrorist networks of the means to conduct future terrorist activity and maintain their infrastructure and operations".*

Legal requirements under UNSCR 1267

182. The backbone of the Saudi freezing regime is Royal Order S/2496 of 19 March 2003. The order directed the MOI, MOJ, MOCI, MOFA and MOF to "*freeze all funds or other assets of any individual or entities listed on the lists issued by the UN and not to restrict the freezing to bank accounts only*". It should be noted that the legal obligation (which is to communicate with FIs and DNFBPs) in the Royal Order targets ministries, not any FI, DNFBP or other person. As indicated above, this is because ministries are the entities that regulate issues pertaining to the functioning of FIs and DNFBPs and are responsible for ensuring compliance with the requirements of UNSCR 1267 and 1373. Although the authorities may consider that freezing is an implicit requirement in the Saudi context for FIs, DNFBPs and any other entity, implicit freezing regimes form an insufficient basis for requiring compliance with UNSCR 1267 and SR.III.

183. The abovementioned Royal Order does not refer to UNSCR 1373. The Royal Order was repeated by a telegram[42] of the MOI in June 2007, with the specific requirement that competent authorities had to examine the consolidated UNSCR 1267 lists on the website of the UN. A few months later, another telegram[43] directed MOF, MOJ, MOCI, SAMA and CMA to comply with UNSCRs 1267, 1333 and 1390 and to report any findings to the MOFA. The assessment team was informed that SAMA issued a circular for banks on 29 September with instructions regarding UNSCR 1267[44].

184. About one month after the on-site, the authorities provided the assessment team with a Royal Order[45] containing the mechanism for implementing aspects of UNSCR 1267. This document establishes a working mechanism which involves the competent authorities in order to freeze without delay the funds and financial assets of groups or individuals designated by the Al-Qaida and Taliban Sanctions Committee established pursuant to United Nations Security Council Resolution 1267. This working mechanism identifies authorities and procedures to implement this Resolution and the de-listing procedure is opened to individuals or entities, on the basis of an ex parte application, whose designation has been considered.

Legal requirements under UNSCR 1373, examining and giving effect to freezing mechanisms of other countries

185. There is no specific legal basis for freezing funds pursuant to UNSCR 1373. Some authorities indicated that lists of terrorists based on UNSCR 1373 had to be dealt with in the same way as UNSCR 1267. However, UNSCR 1373 does not have a list of designated entities, so a clear distinction with UNSCR 1267 should be established. Other authorities indicated that any 1373-related request should be treated as any AML-related mutual legal assistance request, on the basis of AMLS Article 23. However, no examples of any such request could be given. A third group within the government hinted at the existence of a domestic watch list, however, other authorities insisted that the domestic watch list was a regular domestic "most wanted criminals" law enforcement list (for arrest and prosecution, not for freezing assets).

186. The view shared by most authorities was that UNSCR 1373 requests should be treated like any other mutual legal assistance request. Any such request would be considered by the authorities, on the

[42] Telegram by His Royal Highness, minister of interior, No (S1/35831) of 25/5/1428.
[43] Telegram of His Royal Highness, minister of interior, No (S1/51196) of 6/8/1428.
[44] Circular 120/ MAT/ 12872, 12 Rajab 1422H
[45] Royal Order and Mechanism 3125 of 10-04-1430H

basis of AMLS Article 23. The AMLS indicates that the request would be considered by the PCMLA, the PCMLA however indicated that the request should be considered by the PCCT. If granted, the request would initiate a one-off law enforcement search for the designated entity. This means that the designated entity could conduct transactions or be the beneficiary of transactions at a later stage without being detected. So far, no request has been made (according to some sources, including the PCMLA), or requests have been made but there were no hits (according to other sources, including the PCCT). Besides, the AMLS does not add a requirement for any FI, DNFBP or any other entity to freeze any assets or funds in case of a positive match.

Institutional framework and sharing of lists (UNSCR 1267 only)

187. Based on the information provided to the assessment team for the purposes of the on-site visit, the MOFA is responsible for receiving updated 1267 lists and forwarding them to the PCCT. This committee, established to implement UNSCR 1373, in fact currently deals with UNSCR 1267 cases. The PCCT forwards the lists to SAMA, which in turn forwards the lists to the banking community (to SSC, which represents all banks in the Kingdom). In case of a match, banks must freeze the account and inform SAMA, which in turn informs PCCT of the freezing measure.

Definition of funds (UNSCR 1267 only)

188. The Royal Order requires freezing of all funds or other assets of any individual or entities listed on the lists issued by the UN under UNSCR 1267, not restricted to the freezing of bank accounts. The authorities further pointed out that Shari'ah law also defines property as everything a person owns and can benefit from. They stressed that as this definition extended to all types of property and that there was no need to continually refer back to such a definition in all legal documents. The AMLS defines funds as to include "assets of property of any type", including property rights and the proceeds from property rights. It is unclear if only ownership is targeted, or also control of funds, whether this applies to directly and indirectly held or controlled assets, if persons acting on behalf or at the direction of the designated entities are also covered, and if assets in the Kingdom or also elsewhere would be covered. It is also unclear if funds wholly or jointly owned or controlled are covered, and if funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons, terrorists, those who finance terrorism or terrorist organisations are targeted. In addition, there are no provisions to ensure the freezing without delay and without prior notice[46]. Special Recommendation III and UNSCR 1267 and UNSCR 1373 are very specific as to the definition of what funds have to be frozen.

Communicating actions to the financial sector (UNSCR 1267 only)

189. There is a mechanism for sending lists to the banking sector (through the SSC) and, in case of a hit, back to SAMA. That mechanism seems to work well, although the banking sector entities that the team

[46] SR.III / UNSCR 1267 requires "freeze without delay the funds or other assets owned or controlled by Al-Qaida, the Taliban, Usama bin Laden, or persons and entities associated with them as designated by the United Nations Al-Qaida and Taliban Sanctions Committee established pursuant to United Nations Security Council Resolution 1267(1999), including funds derived from funds or other assets owned or controlled, directly or indirectly, by them or by persons acting on their behalf or at their direction, and ensure that neither these nor any other funds or other assets are made available, directly or indirectly, for such persons' benefit, by their nationals or by any person within their territory."

met indicated that in practice they relied on lists provided as part of transaction monitoring software tools, because these included lists of other jurisdictions and supranational bodies. Also, although some of the banks were aware of the fact that any hit would need to be communicated back to SAMA through the SSC, others indicated that they would simply call the FIU. There are no systems in place for non-banking FIs or DNFBPs, but most of those met indicated that they would call the FIU in case of a positive match.

Guidance to FIs and DNFBPs (UNSCR 1267 only)

190. The authorities indicate that the SSC provides the guidance to the banking sector for dealing with terrorist lists. The members of the SSC are certainly aware of the existence of requirements for freezing assets. Also, although the team requested copies of guidance issued by government authorities or the SSC, no evidence of guidance has been provided to the team. There is no guidance available for non-banking FIs or DNFBPs.

Publicly known procedures for de-listing requests and for unfreezing the funds of de-listed persons (UNSCR 1267 only)

191. In relation to UNSCR 1267, the mechanism 3125 issued on 10/4/1430 establishes a procedure to de-list and unfreeze the funds of de-listed persons. According to this procedure, the PCCT receives the requests from the individuals or their lawyers in order for the release of a part of the funds of the person listed. Once the request has been received, the PCCT studies the request and informs the Royal Authority about it. If appropriate, the Royal Authority transfers the request to the MOFA that sends it to the permanent KSA delegation in the UN and the SC Committee in order to study the case. Upon the approval of this Committee, the PCCT addresses the competent authorities in order to release the amount approved by the SCC. In addition to this, Article 13 of the Court of Grievances Law provides the basis for any person to appeal against any administrative decision, including a freezing action.

Publicly-known procedures for unfreezing the funds or other assets of persons or entities inadvertently affected by a freezing mechanism (UNSCR 1267 only)

192. There are no publicly known procedures for unfreezing the funds or other assets of persons or entities inadvertently affected by a freezing mechanism. However, as with the de-listing procedure, Article 13 of the Court of Grievances Law provides the basis for any person to appeal against any administrative decision, including a freezing action.

Authorizing access to funds for certain basic expenses in accordance with UNSCR 1452 (UNSCR 1267 only)

193. There are no specific procedures in place to authorize access to funds, but regular administrative appeal procedures (art 13 of the Court of Grievances Law) can be used. The authorities initially indicated having made two requests to the UNSCR 1267 Committee for authorizing access to funds. One of those requests was successfully granted, although there are no records of the requests. The other request was still pending. It should be noted that the 1267 Committee would decide to approve a request by negative consensus after 48 hours passes, so it is difficult to understand for the assessment team what case would be pending before the 1267 Committee. Nevertheless, at a later stage the authorities indicated that three requests had been made to the UN and that these requests were granted.

Protecting bona fide third parties (UNSCR 1267 only)

194. The authorities indicate that any confiscation procedures based on the AMLS explicitly exclude bona fide third parties. However, *Shari'ah*[47] and the AMLS (article 21) only provide that the punishment (confiscation is a sanction under the AMLS) will not apply to those who could have been prosecuted, but are not because they violated the law in good faith. However, that excludes the much wider circle of bona fide third parties that did not violate any law, like creditors or persons but happen to be in the possession of the property that is subject to freezing.

Monitoring compliance with freezing obligations (UNSCR 1267 only)

195. The AMLS contains a provision (Article 18) that administratively punishes failure to obey the administrative provision contained in Articles 4 – 10 AMLS, which for the Saudi authorities forms the basis to monitor compliance. There are no direct and clear provisions that require FIs, DNFBPs and any other persons to freeze the assets of designated entities (all requirements only target government entities)[48].

Statistics (UNSCR 1267 only)

196. Despite the absence of a comprehensive legal basis for the implementation of UNSCR 1267, the system that was put in place by the ministries acting in compliance with the Royal Order and the mechanism 3125 seems to produce results regarding UNSCR 1267. Through statistics provided to the assessment team, the authorities indicate that based on UNSCR 1267, 94 bank accounts, 11 investment products (accounts, funds and portfolio) and 24 credit cards belonging to 13 Saudis have been frozen. The total amount of seized banking assets was almost USD 6 million. Since the Kingdom, in general, does not allow non-residents to open bank accounts in Saudi Arabia, those 13 Saudis must have lived in the Kingdom at the time of the bank account freeze and it is therefore likely that these persons had other assets that would have also been subject to UNSCR 1267. And in fact, the authorities indicated that the related belongings in 16 businesses and 6 real estate titles were frozen.

Effectiveness (UNSCR 1267 only)

197. UNSCR 1267 is generally effectively implemented by banks (although not to the same degree by other sectors), generally also because of the use of commercial compliance monitoring software products by banks.

2.4.2 Recommendations and Comments

198. The preventive freezing of terrorist assets is an undeveloped tool in the Kingdom. Nevertheless, the Kingdom is subject to all UNSCRs and has subscribed to the FATF (Special) Recommendations, which means that it needs to implement effective laws and procedures accordingly.

[47] Al-Zumar 39:7: If you become ungrateful, then (know that) indeed Allah is Independent of you; and He does not like the ungratefulness of His bondmen; and if you give thanks, He is pleased with it for you; and no burdened soul will bear another soul's burden*;* you have then to return towards your Lord – He will therefore inform you of what you used to do; undoubtedly, He knows what lies within the hearts.

[48] The team also notes that even if there would be a legal requirement for FIs and DNFBPs to freeze, the monitoring of this requirement would suffer from the same shortcomings in supervision as described in Section 3.10 of this report.

199. UNSCR 1373 is not implemented in the Kingdom. There is no legal framework and no implementation of the requirements. Unlike with UNSCR 1267, where there was a procedure that produced results before the legal basis was put in place, no such effective mechanism was put in place for UNSCR 1373. The lack of implementation of UNSCR 1373 has a significant negative impact on the rating of this Special Recommendation. The Saudi authorities should establish a clear legal basis and procedure for the implementation of UNSCR 1373, identifying the competent authorities with responsibility for implementation and a procedure to monitor the freezing of funds as well as a procedure for the implementation of penalties should the financial authorities fail to comply with their duty to freeze funds.

200. Saudi Arabia has set up a system to implement UNSCR 1267. In particular, the mechanism put in place to implement UNSCR 1267 (taken together with Article 13 of the Court of Grievances Law) provide the legal basis for the implementation of the procedure to freeze terrorist funds or other assets of persons and entities designated by the UN Al Qaida and Taliban Sanctions Committee. In addition to this, the team notes that in relation to UNSCR 1267, Saudi FIs and Saudi state authorities have in fact followed-up on listings of terrorist by the UNSC, even before the legal basis was put in place. Authorities have also engaged with the UN in requests for allowing access to frozen property. Therefore, the authorities have shown effective commitment in the fight against entities targeted by UNSCR 1267 which has led to results.

201. Notwithstanding the legal basis for UNSCR 1267, a few shortcomings remain. The role of the different actors involved in the implementation of these UNSCRs is not very clear for the assessment team. In certain cases, the lack of clarity seems not to be due to a misinterpretation of the legal provisions but to the fact that they are not applied in practice (or so it would appear). PCMLA and PCCT do not have clearly separated competences, and this is not only a problem in relation to this SR but to international cooperation in general.

202. Further, there was a high degree of mixing between international cooperation on freezing of terrorist assets, regular mutual legal assistance and INTERPOL-based law enforcement cooperation. Although the private sector representatives met were usually aware of the existence of requirements to freeze (terrorist) assets, in practice they were not often aware of the difference between names UNSCR 1267-based lists and names on regular domestic "most wanted criminal suspects" lists. Compliance with the legally non-existing requirements was low and non-compliance was not sanctioned.

203. The deadlines for freezing funds are not clear. These should be revised to ensure consistency with the wording of the UN resolutions, which specify that funds should be frozen "without delay".

204. There is no definition of the funds that should be the subject of freezing orders that is consistent with the TF Convention or with the UNSCRs.

2.4.3 Compliance with Special Recommendation III

	Rating	Summary of factors underlying rating
SR.III	**PC**	Regarding UNSCR 1373: • UNSCR 1373 is not implemented (no legal basis, no procedure) Regarding UNSCR 1267: • Freezing actions do not apply to a sufficiently broad range of funds or other assets. • No communication mechanisms for non-bank FIs and DNFBPs. • No guidance for non-bank FIs and DNFBPs.

	Rating	Summary of factors underlying rating
		• Protection does not extend to a sufficiently broad range of bona fide third parties • Lack of clear monitoring and sanctioning procedures to verify implementation of freezing requests

Authorities

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

2.5.1 Description and Analysis

General description

205. Saudi Arabia has had the requirement to report suspicious transactions since 1975. The requirement was established in order to detect possible illegal remittance operations in particular through banks located in Mecca, Medina and Jeddah. Reports were made by FIs directly to the police with a copy furnished to SAMA as the financial supervisor in the Kingdom. In 2001, the obligation was reaffirmed in another SAMA Circular; however, all banks and bureaux de change were henceforth required to report suspicious transactions to their nearest provincial branch of the Anti-Drugs Directorate (ADD), again with a copy provided to SAMA.

206. In September 2002, the MOI made the formal decision to create a financial intelligence unit (FIU) that would eventually take over the role played up to then by ADD. The basic structure and mission for the FIU were developed in coordination with the PCCML, and the Saudi Arabia Financial Intelligence Unit (SAFIU) was established on 7 July 2003 as an autonomous authority under the General Security Department of MOI, and became fully operational on 10 September 2005 pursuant to executive regulation and SAMA Circular. During this same period, Saudi authorities were elaborating the AMLS, which received final approval on 23 August 2003. This law provides in article 11 the legal basis for the new FIU. SAFIU reports to the Assistant Minister for Security Affairs who reports to the Minister of Interior; it is a law enforcement entity within MOI. SAFIU is member of the PCCML. It is located in Riyadh and has no branches.

207. With the legal and institutional framework[49] in place, Articles 11 to 13 of the AMLS list all legal power and duties of SAFIU: *(i)* receiving suspicious reports on ML/TF from FIs, Designated Non-Financial Business and Professions (DNFBPs), other governmental parties, and individuals; *(ii)* establishing and updating an STR database; *(iii)* requesting and exchanging information with other FIUs, if this does not breach financial confidentiality rules; *(iv)* issuing standardized STR reporting forms; *(v)* analyze STRs, if necessary with the assistance of other MOI law enforcement bodies; *(vi)* forwarding STRs for investigation to other law enforcement bodies; *(vii)* request the Prosecution Authority (PA) to preventive freeze of possible ML/TF transactions; *(viii)* file STRs that have not been found suspicious; *(ix)* assist supervisory institutions in assessing compliance of reporting institutions; *(x)* prepare awareness raising programs on ML/TF; *(xi)* signaling structural problems in the AML/CFT system to the PCCML; *(xii)* conclude MOUs with other FIUs; and *(xiii)* preparing for membership of the Egmont Group.

[49] Circular No. 1 Sh/46287 of 1/8/1426 AH of the Minister of Interior.

Receiving and analyzing STRs

208. SAFIU is empowered to receive, analyze and disseminate STRs from FIs, DNFBPs and other government agencies (about 14% of all STRs are submitted by other government agencies) on ML and TF. Reporting entities are required to submit a copy of STRs to their respective supervisory entity.

209. Reports are received by the Reports Division and checked for completeness. If found complete STRs are forwarded to the Information and Studies Division. This division enriches the reports with information obtained from SAFIU's own database and from the databases of other government entities to which SAFIU has direct access. Once reports are considered to be final at this second stage, the file will pass through the Evaluation Committee whose task it is to determine whether a report will be taken up for onward ML/FT analysis by the Information Gathering and Analysis Division. The Evaluation Committee consists of financial, intelligence and legal experts, the deputy director and is chaired by the director of SAFIU who takes the final decision. Despite the relative low number of STRs, combined with the relative high number of staff and the de facto outsourcing of certain analytical tasks to other investigation authorities (such as on-site investigations), the statistics indicate a rather high backlog of STRs that was still being analyzed at the time of the on-site: approximately one third of all STRs of 2007 and 2008 was still being analyzed at that time (but STRs from 2006 and older had been closed).

210. Reporting to SAFIU is done in two stages. At the first stage, reporting entities submit a STR on the reporting form. The information needed to complete this form is limited to: *(i)* the name, address and phone number of the suspected subject; *(ii)* a statement of the suspected transaction(s), its parties, detection circumstances and current status; *(iii)* the (sum of the) transaction(s) and the relevant account information; and *(iv)* the reasons for suspicion.

211. After the STR is submitted, FIs have at the second stage ten days to submit the following information: *(i)* account statements (minimum of 6 months); *(ii)* copies of account opening records; *(iii)* documents that support suspicion and *(iv)* data related to the nature of the transactions. Non-FIs have to submit a similar file, but only on request of SAFIU. SAFIU staff indicated that it takes on average 7 working days for any reporting entity to submit the supporting files.

212. SAFIU and law enforcement staff noted that files of reported STRs are always complete, or can be completed upon request. This view is supported by statistics and by views of other agencies. The assessment team notes the discrepancy between SAFIU receiving all necessary documents, and the shortcomings related to the implementation of CDD measures (see Section 3.2 of this report) which could preclude this. However, it is the assessment team's view that this CDD-related shortcoming does not preclude that those STRs that are reported contain all necessary information, and that this does not have a negative effect on the assessment of SAFIU.

213. Within SAFIU, the Evaluation Committee has drawn up criteria for analyzing STRs. At the first stage, the STR is analyzed against *i)* social characteristics of the suspect (such as age, nationality, place of residence and other civil status data); *ii)* the information available in the security database (such as criminal records); *iii)* cross-border money transfer data; *iv)* the car registry; *v)* immigration authority's data; and

reports in the FIU. At the second stage, the STR is analyzed against a range of 19 different typologies. The authorities provided a one-paragraph summary for each of these 19 criteria[50].

214. The SAFIU has processed the following number of STRs since its inception.

Processed STRs 2004 – 2008				
Year	Received STRs	*of which on ML*	*of which on TF*	Disseminated to investigation
2004	350	*348*	*2*	43
2005	451	*444*	*7*	69
2006	405	*351*	*54*	69
2007	743	*649*	*94*	113
2008	1019	*955*	*64*	201
Total	2968	*2747*	*221*	495

215. Most STRs are received from banks. The following tables show from which sort of reporting entity the STRs have been received.

STRs from reporting entities 2004 – 2008								
Year	**FIs**		**DNFBPs**			**Government**	**Individuals**	**Total**
	Bank	**Exchange**	**Accountants**	**Dealers in precious metals and stones**	**Other**	***(See next table for details)***		
2004	311	30	-	-	-	5	4	**350**
2005	418	12	-	-	-	13	8	**451**
2006	303	13	1	4	9	14	61	**405**
2007	546	20	3	8	21	45	100	**743**
2008	769	18	2	6	20	133	71	**1 019**
Total	**2 347**	**93**	**6**	**18**	**50**	**210**	**244**	**2 968**

216. The following table shows from which government agency STRs were received. Note that most government STRs are received from other bodies within the Ministry of Interior (due to the fact that the MOI is responsible for investigating most predicate offenses for ML/FT).

STRs from government entities 2004 – 2008						
	2004	**2005**	**2006**	**2007**	**2008**	**Total**
Ministry of Interior (total)	5	13	10	42	112	**182**
of which						

[50] Publishing these criteria would give possible money launderers too much insight into the work of SAFIU.

STRs from government entities 2004 – 2008							
		2004	**2005**	**2006**	**2007**	**2008**	**Total**
	MOI (other)	*-*	*-*	*2*	*7*	*15*	*24*
	Anti-Drugs Directorate	*-*	*2*	*3*	*22*	*22*	*49*
	Public Security Body	*5*	*11*	*-*	*-*	*3*	*19*
	Prosecution	*-*	*-*	*3*	*8*	*57*	*68*
	Al-Mabahith (intelligence police)	*-*	*-*	*2*	*5*	*12*	*19*
	General Intelligence	*-*	*-*	*-*	*-*	*1*	*1*
	Passport Directorate	*-*	*-*	*-*	*-*	*1*	*1*
	Ideological Security	*-*	*-*	*-*	*-*	*1*	*1*
Ministry of Finance		-	-	1	-	-	**1**
Customs		-	-	1	2	2	**5**
Customs (declaration forms)		-	-	-	-	7	**7**
Ministry of Industry and Commerce		-	-	-	-	2	**2**
SAMA		-	-	1	-	-	**1**
CMA		-	-	-	-	8	**8**
Provinces (Riyadh)		-	-	1	-	2	**3**
Council of Ministers Court		-	-	-	1	-	**1**
Total		**5**	**13**	**14**	**45**	**133**	**210**

217. SAFIU has the power to request the Prosecution Authority for a preventive freeze in case of a ML or TF suspicion. In 2006, this was necessary in 4 cases, in 2008 in 3 cases (all for ML only).

Guidance regarding the manner of reporting

218. SAFIU has prepared standard reporting forms which were disseminated to all reporting entities (AMLS, Article 11.3). Reports may be sent by fax, post or by hand delivery. Electronic delivery is not (yet) possible. Reporting entities are also allowed to call SAFIU to report a STR. The reporting forms request basic information on the transaction and client. SAFIU is staffed 24 hours a day on all weekdays and reporting can be done during all these hours.

219. The reporting forms have been made available to the reporting entities. SAFIU has held meetings with the different supervisory bodies to explain and discuss the reporting forms and that it had received positive feedback on the forms from the reporting entities. SAFIU provided the assessment team with a copy of a Guidance Manual for reporting entities. It contains information on the manner of reporting, and copies of reporting forms along with information on the obligation to report and, very important, a number of typologies. The manual was issued for the first time in early 2009, The guidance regarding the manner of reporting confirms the legal duty to report and lists the address, fax number and phone number of the FIU to enable reporting entities to file a report.

Access to information

220. SAFIU has access to a domestic law enforcement database, which holds information on drugs cases, criminal records, travelers, foreigners, sponsored persons, passports and prohibited and wanted persons. The members of the assessment team received a real time demonstration of this system, which appeared to be fast and comprehensive. The system is based on an application maintained by MOI. The application provides access to various parts of the database on a needs basis to domestic law enforcement bodies. According to the staff of SAFIU, it has access to all components of the system. SAFIU has no direct access to other domestic governmental databases. SAFIU can request information from other databases (the MOCI corporate SAMA registration database, the financial information database, the MOJ real estate database, the CMA securities' information database, the MOIA and MOSA NPO databases and the Customs' currency database), but the access is on request only, and is granted on a case by case basis and the request has to refer to a specific case, person or entity. Nevertheless, the request is executed through liaison officers (who later formalize through a written request). SAFIU indicated that requests have never been denied so far. All in all SAFIU has access to law enforcement, administrative and financial databases, be it that the means of access differ from each other.

Requests for additional information from reporting entities

221. The AMLS stipulates clearly the right of SAFIU to request further information from reporting entities (AMLS Article 8, and 8.1 – 8.3). Any such request overrides financial secrecy or financial confidentiality provisions. Reporting entities have to submit documents and records and any other available information. All requests from SAFIU are indirect as requests and answers will pass through the AML units of the authorities that also have supervisory powers (SAMA, CMA, MOCI, MOIA, MOSA and MOJ). The AMLS indicates that all information to SAFIU should be sent to the FIU without delay. It is unclear how long the execution of a request may take.

222. The authorities indicated that information is usually submitted without delay, and that all information that is requested is submitted.

Dissemination of reports

223. If there is sufficient suspicion of ML/TF (AMLS, Article 11.3.g) SAFIU must disseminate the respective STRs to the Prosecution Authority for ML or the Secret Police for FT cases. Since its establishment, SAFIU disseminated a total of 495 ML/TF cases. In the written answers to the assessment team, the authorities also indicated that since its establishment, SAFIU has forwarded 117 non-ML/FT related reports: 97 to the MOI on suspicion of corruption, 8 to the GID on suspicion of terrorism, 3 to SAMA, 7 to MOCI and 2 to another entity.

224. During the on-site, SAFIU provided the assessment team with more statistics. The following table shows the number of disseminated STRs. STRs are either disseminated to law enforcement authorities (for investigation) or to other government bodies (for information), or closed or still being analyzed.

STRs disseminated, ongoing analysis and closed: 2004 -2008[51]														
	Disseminated for ML/TF investigation			Disseminated for information (including non AML/CFT)								Ongoing analysis	Closed STRs	Total
	PA	AM	Total	PS	MOCI	SAMA	CMA	PR	AM	ADD	Total			
2004	41	2	**43**	44	70	-	-	-	-	-	**114**	-	193	306
2005	65	4	**69**	46	74	-	-	-	-	-	**120**	-	262	451
2006	45	24	**69**	85	1	2	-	-	-	-	**88**	-	248	405
2007	95	18	**113**	1	9	2	2	33	-	-	**47**	208	375	743
2008	183	18	**201**	22	214	2	4	32	15	7	**296**	305	217	1019
Total	**429**	**66**	**495**	**198**	**368**	**6**	**6**	**65**	**15**	**7**	**665**	**513**	**1295**	**2968**

225. The statistics reveal an average of 600 STRs per year with a strong increase in 2007-08. Almost 30% of the STRs received in these years are still open for analysis. It is not sure what causes this, but it may be an effectiveness issue. The assessment team is of the view that SAFIU has sufficient staff (111 staff and 20 vacancies) and is sufficiently knowledgeable, so a lack of resources or training can be ruled out. It might be caused by a lack of quality STRs, but that has been ruled out by SAFIU. The authorities are, however, advised to analyze this issue.

226. The authorities indicated that a team within SAFIU is responsible for taking the final decision on disseminating of reports. The team includes the deputy director. Ultimately, the Director of SAFIU is responsible for disseminating STRs. There are no internal guidelines, criteria or rules that determine which STRs should be forwarded to the Prosecution Authority; this is done on a case by case basis depending on the STR.

227. The assessment team discussed the output of SAFIU with investigation authorities. With the exception of the Prosecution Authority (that receives most STRs) not much feedback could be offered on the STRs they had received, except for the fact that files had indeed been received. Whether or not the output of SAFIU does not match the needs of other agencies, or whether or not receiving authorities should be educated in using the information could not be established, but certain is that more needs to be done. On the other hand, no agency had any complaint about the output of SAFIU.

Operational independence

228. SAFIU reports to the Assistant for Security Affairs to the Minister of Interior and has its own and independent budget (separate from MOI). The spending of the budget is determined by the SAFIU's Supervisor who also has independent powers to recruit, promote, and grant moral and material incentives.

229. Reporting entities also submit a copy of each STR to their supervisor. Ultimately the assessment team could not establish that the copying mechanism does not have a negative effect on the full operational

[51] Key: PA: Prosecution Authority for ML cases; AM = Al-Mabahith (Secret Police) for FT cases; PS = Public Security, PR = Public Rights (MOI)

independence of SAFIU and on the confidentiality of STRs. Even whether or not SAFIU is the one national centre for receiving STRs (notably the majority of STRs from non-government institutions is reported by FIs and one supervisor receives a copy of 95% of all STRs)[52]could not be confirmed.

Protection of information

230. The AMLS provides that the SAFIU database is confidential (Article 11.3.b). Access to the database is secured and restricted to authorized persons only. STRs can be submitted on a 24/7 basis. The database is securely connected to database applications within the MOI and it has no access to internet. The servers of the SAFIU are based at the secured, free standing, premises of SAFIU, which cannot be approached and entered without detection.

231. There are no specific rules for guaranteeing confidentiality other than those that require confidentiality for all public servants. The authorities indicated that no breaches have been detected and that breaches would be punished. Nevertheless, due to the fact that all STRs are copied to supervisors the assessment team is of the opinion that there is a confidentiality issue. First, supervisors have access to STR information and there are no specific rules for ensuring the confidentiality of the copies of these STRs. Second, as a result of the outsourcing of supervision of FIs to accountant firms (reporting entities themselves), the pool of entities that have access to STRs is even larger. The assessment recognizes that outsourcing is an internationally accepted practice.

Public reports

232. The SAFIU has publicly released three annual reports (2006 – 2008) containing information about its legal basis, the organisation and STR-related statistics, and recently the Guidance Manual with typologies for reporting entities and other relevant subjects. The typologies are of a reasonably good quality and cover a number of possible forms of ML and (to a lesser extent) of TF. Overall and compared to what is required from a FIU this manual is a good starting point. Since its inception in 2003 SAFIU has published 3 annual reports (2006 - 2008). The reports merely maintain information on the legal foundation and the tasks of it, the reporting forms and a number of statistics. The latter only over the year under review and the year before. No typologies and trends are shown in the reports and there is no mentioning of current and future planned activities.

233. SAFIU also has a public website[53], with background information for reporting entities and interested citizens. The Guidance Manual, the annual reports and the reporting forms (for banks, corporate and accountants) can all be found on this site.

[52] The authorities, in particular SAMA, indicated that submitting a copy of a STR to supervisors serves statistical purposes. However, it should be sufficient if SAFIU would keep STR statistics, and not any of the supervisory agencies. Additionally, the authorities stated that having a copy of a STR enables supervisors to assess compliance with the AMLS. However, the assessment team believes that it would be sufficient for the supervisory authorities to be able to check within the records of a FI whether or not a transaction has been reported. For these reasons the assessment team was not convinced by the authorities' arguments.

[53] The website can be found at: http://www.moi.gov.sa

Egmont Group

234. SAFIU has applied for Egmont Group membership. Its application is sponsored by three Egmont members. The authorities stated that SAFIU is committed to the Egmont Group Statement of Purpose and its Principles for Information Exchange, and that it is adhering to these as part of its accession bid. It is expected that membership will be obtained in 2009[54].

235. SAFIU has not yet made many requests for information to other FIUs. SAFIU is not subject to a requirement to conclude an MOU with other FIUs, information can also be exchanged on the basis of reciprocity (AMLS, Article 22).

Resources and internal organisation (Recommendation 30)

236. SAFIU management consists of 12 staff (one director, one deputy director, 7 heads of division and 3 consultants). There are four divisions: *(i)* Reports Division (11 staff); *(ii)* Information Gathering and Analysis Division (42 staff); *(iii)* Information Exchange and Follow-up Division (7 staff); *(iv)* Information and Studies Division (18 staff); *(v)* Training Division (4 staff); *(vi)* Financial and Administrative Affairs Division (10 staff); and IT Division (7 staff). The current total number of staff is 111, with 20 vacancies. The annual budget is SAR 100 million.

237. The Reports Division's main task is to receive STRs. If an entity reports a STR by phone, this division is required to record all data without delay in writing. All STRs receive a file number and are forwarded to the Information Gathering and Analysis Division via the Information and Studies Division and after having passed through the Evaluation Committee.

238. The Information Gathering and Analysis Division checks incoming STRs for completeness. It can also request additional information from other government agencies/authorities. If, after analyzing a STR, the Division determines that the STR is sufficiently suspicious, it can ask investigation authorities to use their powers to gather more evidence to support the analysis. If the additional data thus gathered support the initial analysis, the Division will forward the file to the PA or the Secret Police. The Division can also ask law enforcement bodies to freeze funds (for a maximum of 20 days). Finally, the Division archives all STRs from the database that are not deemed suspicious after analysis (which keeps the STRs accessible for analytical and search purposes).

239. The Information Exchange and Follow-up Division is responsible for domestic and international cooperation.

240. The Information and Studies Division keeps all databases, such as those on received, analyzed and disseminated STRs. It also records information on ML convictions, the number of foreign requests, and the number of STRs that are kept in the databases (with the reason for keeping). It is also responsible for detecting typologies, and for drafting policy solutions. It prepares the annual report, and organizes awareness raising programmes.

[54] SAFIU joined Egmont Group at the 17th annual meeting in Doha 24 - 28 May 2009. The admission document was signed on Thursday, 18 May 2009. This was outside the time framework of this assessment, however it should be noted that Egmont membership is not a requirement under the FATF Recommendations anyway.

Professional standards (Recommendation 30)

241. SAFIU employees are bound by the secrecy and confidentiality rules that apply to all civil servants in the Kingdom (Civil Service Law and the Officers and Individuals' Service Law).

242. Employees are not allowed to keep official documents for themselves or disclose any professional information if not required by their professional duties. Employees are also not allowed to accept gifts, honors, grants, loans or scholarships from businesses that have any relation to the work of the employee[55]. No breaches were detected.

Training (Recommendation 30)

243. The number of training programmes and their participants have been boosted over the last two years. Training courses take between one and 20 days, and are given at SAFIU, by SAFIU, at other agencies, in the Kingdom and abroad. The following table shows the number of trainees over the last four years.

Training for SAFIU staff (number of trainees 2005 – 2008)					
Topic	**2005**	**2006**	**2007**	**2008**	**Total**
CFT	-	10	18	42	**70**
AML	-	4	74	13	**91**
Predicates	1	1	2	9	**13**
General training	10	5	45	67	**127**
Other	-	-	19	23	**42**
Total	**11**	**20**	**158**	**154**	**343**

Effectiveness

244. SAFIU has a large exposure thanks to its membership of the PCCML. The assessment team could establish that the PCCML is kept in high regard within the government as well as in the reporting community. For SAFIU this exposure has an indirect character though. From the interviews with FIs and other reporting entities and from certain government agencies it could be detected that for most institutions and agencies contact with SAFIU is rarely on a direct basis. It would enhance SAFIUs exposure and effectiveness if contacts would increase to be on a much more direct basis.

245. The Guidance Manual contains useful information on a number of subjects. It is advisable to keep the manual up to date on a continuing basis so as to reflect the latest developments on subjects such as typologies. It is also advisable if the guidance manual would add some information on methods and trends and other guidance material. This will make the manual an effective tool.

246. The percentage and absolute number of STRs at the end of a year that have not yet been taken up for analysis or is in the process of being analyzed seem high compared with the total number of STRs. It

[55] Royal decree M/43 on 28/8/1393 (Article 7), Royal decree No M/9 on 24/3/1397 (Article 60) and Royal decree no M/49 on 10/7/1397 (Article 12.1).

would warrant to investigate the cause for these backlogs in order to determine possible inefficiencies in the operational processes. The fact that SAFIU has a shortage of some 20 staff on its approved formation not necessarily needs to be the reason for the backlog.

Resources (Recommendation 30)

247. SAFIU appears to be well equipped with (brand new) IT systems and the team was informed by the director that it gets the budget approved that it needs. The present number of employees is 111 with an approved formation of 131. As in many places experts are not readily available in the market and it is not different in Saudi Arabia. Training in SAFIU gets a lot of attention, and training facilities on the premises looked adequate and SAFIU staff is knowledgeable. When SAFIU started operations SAMA supplied a number of seasoned financial experts to be part of the staff complement.

Statistics

248. In its annual reports SAFIU publishes quite a number of statistics. In the most favorable case they cover a time span of two years. Others do not and cover the year under review.

2.5.2 Recommendations and Comments

249. The numbers of STRs and disseminations seem low, taking into account the size of the population, the very large numbers of visitors (mainly pilgrims), the size of the remittance sector (the second largest in the world), the number of reporting entities and more particularly the large number of FIs (licensed and in the near future to be licensed). SAFIU and PCCML should step up the supply of information on ML/FT typologies, methods and trends to reporting entities and to supervisory bodies. This will enhance the position and tasks of SAFIU and will increase overall awareness. It is advisable to continuously to update the current Guidance Manual in order to help to reach these goals.

250. The backlogs at yearends of STRs that have not yet been analyzed require to be analyzed as inefficiencies may exist in the operational processes. The existence of the backlogs (and continuation thereof) point at an effectiveness issue. In the Kingdom FT is considered a form of ML in the AMLS. It is important that all reporting entities, supervisory bodies and other government bodies are made aware of the fact that TF in practice is not equal to ML. A distinction should also be made between ML and FT in the statistics.

251. It would be more comprehensive if statistics pertain to longer periods of time in order to cater for historical data so as to help understand developments in reporting, analysis and dissemination. This will also serve feedback and increase substance.

252. Statistics could be more precise and informative and could show which indicators / criteria were used for reporting, analysis and dissemination, as well as the outcome of investigation and law enforcement and convictions.

253. To enhance the visibility of SAFIU and the usefulness of the annual report, the annual report should list current and planned activities and cases and typologies, methods and trends.

254. SAFIU has sufficient access to a variety of databases; however, only to one of these databases the access is direct. While the FATF Recommendations allow indirect access, and while the one database that SAFIU has direct access to is the most important database, SAFIU's work would become more efficient if other authorities would give SAFIU direct access to their databases.

2.5.3 Compliance with Recommendation 26

	Rating	Summary of factors relevant to s.2.5 underlying overall rating
R.26	**LC**	• Effectiveness is under pressure by the insufficient number of processed STRs. • Annual reports lack most of the required information.

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 (Designated law enforcement and prosecution authorities)

255. Overall law enforcement powers have been stipulated in the Criminal Procedure Statute (CPS)[56]. It authorizes in Article 16 the Prosecution Authority (PA) with the power to initiate and follow-up criminal action before the competent courts. In addition, Article 26 stipulates that proceedings relating to criminal investigation are to be conducted by members of the PA and certain officials within the police as well as within those entities that have the general power to investigate each within their own jurisdiction; these are public security generals, public research officers, passports officers, intelligence officers, civil defense officers, directors and officers of prisons, border guard officers, special security forces officers, national guards generals, and armed forces officers and members of the religious police. Captains of Saudi vessels and airplanes and certain natural and legal persons due to special regulations have similar powers.

256. ML and TF are considered like any other crime, which means that all investigation authorities are designated to fight ML and TF, on the basis of Articles 14 and 26 of the CPS. In practice, however, there is a degree of specialization within the Saudi investigation and law enforcement community. All entities that specialize in ML and TF are discussed below, including an overview of the available resources.

Prosecution Authority

257. The Prosecution Authority has overall responsibility for investigation and prosecution within Saudi Arabia (Article 14, CPS) and it is the main body designated to fight against ML and TF (AMLS, Article 27). The PA is connected, but not subordinate, to the Ministry of Interior.

258. The PA combines investigative and prosecution powers (its full name translated from Arabic is "Investigation and Prosecution Authority" and was created in 1989[57]. The PA is located in Riyadh with 13 branches (one in each province). The branches in Riyadh, Mecca and the Eastern Province have a more complicated structure than the other branches. The PA has the duty to: *(i)* to investigate crimes, *(ii)* to refer

[56] Articles 14, 24 and 26 AMLS.
[57] Royal Decree No (M/56) on 24/10/1409 AH

criminal cases to other investigation agencies or to decide to take no action, *(iii)* to prosecute criminal cases before the competent courts, *(iv)* to appeal against sentences, *(v)* to see to it that sentences are executed and *(vi)* to ensure that prisoners and detainees are treated according to the law (PA Statute, Article 3).

259. The other investigation authorities to which the PA can refer certain criminal cases to, or from which the PA can receive cases, are the Directorate of Public Security (PSD), the General Directorate of Investigation (GDI) and the General Directorate of Anti-Drugs (ADD). All resort under MOI. These authorities investigate most ML/FT criminal cases. Saudi Customs (which resorts under the Ministry of Finance) may also receive cases from the PA as may SAMA.

260. The PA supervises the investigation of all criminal cases (article 25 CPS) and prosecutes all cases before the courts, including ML/FT cases. To ensure proper coordination, the PA has 13 liaison officers in other agencies in MOI. Ways of operational cooperation are laid down in MOUs. Coordination with non-MOI entities (like SAMA and Customs) takes place through bilateral agreements and through its membership of the PCCML. All investigation authorities have the duty to promptly notify the PA of any development in a case under investigation (Article 27 CPS).

261. The PA coordinates with SAFIU on a case-by-case and bilateral basis.

262. The majority of AML staff can be found at the Prosecution Authority. The following is a breakdown of the staff number for each province. It is unclear how these numbers relate to the overall staff numbers of the PA. No information on its budget is available.

AML staff in the PA (as of December 2008)			
Province	**Investigators**	**Prosecutors**	**Total**
Riyadh	10	4	**14**
Mecca	8	4	**12**
Al Medina Al Munawara	2	1	**3**
Al Sharkiya	5	2	**7**
Al Kuseim	8	3	**11**
Assir	4	2	**6**
Jazzan	2	1	**3**
Najran	2	1	**3**
Hail	2	1	**3**
Tabuk	2	1	**3**
Northern borders	2	1	**3**
Al Jawf	2	1	**3**
Al Baha	2	1	**3**
Total	**51**	**23**	**74**

Ministry of Interior

263. The following directorates have investigation authority and are tasked with AML and CFT. No information about the Secret Police was made available.

The Directorate of Public Security (DPS)

264. DPS is one of the investigation authorities that reports to the Assistant Minister for Security Affairs in MOI. In 2003, the Department for Anti Organized and Economic Crime was established within DPS. This department is located in Riyadh and has a staff of 19 officers, 90 investigators and 380 field teams throughout the Kingdom. The main task of this agency is to investigate predicate offences relating to organized and economic crimes. It focuses on non-drugs cases such as smuggling alcohol and weapons, prostitution, financial sector crimes, robbery, internet and computer piracy. It also cooperates with similar bodies in other countries, and in domestic typologies studies. It has AML-sections in the regional police offices. It is unclear how many staff are available for ML/FT investigations.

The General Directorate of Investigation (GDI)

265. The GDI is the investigation authority concerned with bribery, ML and terrorism. Within the GDI, the Administrative Intelligence Offices (AIO) is specialized in ML and terrorism cases. AIO was created in 1980[58]. It is located in Riyadh and reports to the Minister of the Interior directly. It has branches in all regions of the Kingdom and employs 345 officers and 2 356 regular staff, besides civilian staff. In order to strengthen the focus on counter terrorism and FT, the Financial Investigation Department[59] was created in 2007 within AIO. This department has 54 staff, located throughout the country. It is designated to conduct FT investigations and it is allowed to review bank accounts, review STRs, check bank accounts of persons already under arrest, order freezing and seizure of funds and goods and investigate the activities of charities. It should be noted that the authorities, in another section of the questionnaire that was submitted before the on-site mission, indicated that the AIO had only just been established and had no staff yet.

The General Directorate of Anti-Drugs (ADD)

266. ADD was separated from DPS in 2007[60]. It has its main seat in Riyadh, where it employs 39 officers and 85 investigators, and has 321 field teams throughout the Kingdom. It reports to the Assistant Minister for Security Affairs. The directorate has the task to combat the possession, smuggling, trafficking and using of drugs and psychotropic substances in all its forms and appearances. It operates an AML Division which has departments in the regional offices of ADD. It is unclear how many staff is available for ML/FT investigations.

[58] Ministerial resolution No (2111/8) on 1/12/1400 H

[59] Telegram No. -/-/3/4879- in 1/6/1427, and Resolution No 12554 on 6/6/1427 of the Director of the Research office.

[60] Ministerial resolution of His Royal Highness, the minister of interior No. 7117 on 13/9/1428 AH pursuant to the High Order No (--/ 5664) on 23/6/1428 AH

Saudi Customs

267. Saudi Customs has the authority to investigate cases as a result of violation of its laws, including the AMLS. It employs 7.007 staff and is headquartered in Riyadh. It has not a general investigation authority, but bases its powers on the circumstances of a case. Saudi Customs would normally only detect an ML/FT case, and then forward the case for investigation to other competent authorities (of MOI or PA). Saudi Customs is further described in section 2.7 of this report.

Effectiveness of investigation and law enforcement entities

268. There is quite a number of investigation authorities in the Kingdom, each with its own legal stature and fields of expertise. The PA is the body that supervises all investigation officers (article 25 CPS). The different policy committees (PCCML, PCCFT and PCMLA), bilateral consultations, the MOUs, the liaison officers and the legal requirement to consult the PA assist in achieving proper supervision. Apart from the PA, the assessment team could only meet with policy staff at law enforcement bodies. At that level, policy coordination seemed to be the most important task while there seemed very little sharing of information about the day-to-day work of investigation authorities. In order to have and maintain a good grip on all cases under investigation the PA can involve (article 65 CPS) any of the other investigation authorities in any case in which such authority has (legal) competency, knowledge and expertise. The assessment team was informed that this happens all the time.

Powers to postpone arrest or seizure

269. The CPS and the AMLS authorize and empower PA, as the main designated authority for investigation and prosecution of ML/TF cases, to arrest, postpone or suspend the arrest of suspects. All investigators and prosecutors have these powers in the cases they are responsible for (CPS Articles 25, 62 and 103 and AMLS Article 27). In addition, SAFIU may request PA to carry out preventive seizure of funds, properties and means when related to cases of ML/FT (AMLS, Article 12). These powers may be used by investigation authorities only if of benefit to the investigation. These powers can also be used in relation to the seizure of money.

Additional elements

270. Saudi investigation authorities may use a variety of special investigative techniques The CPS (Articles 55 to 57) permits the PA to issue orders to intercept or seize mail, cables or scripts and records of any sort of communication and to exercise surveillance. As the PA is the main designated authority to investigate and prosecute ML/FT cases such special investigation techniques may also be used in these cases.

271. All investigation authorities are said to be able to form investigative groups on a case-by-case or on a project basis, without a need for MOUs. Formation of such groups or defining such projects is said to be the result of the deliberations in the different policy committees (PCCML, PCCFT, PCMLA) or of bilateral contacts. However, the assessment team was not presented with any specific case to illustrate the work of a joint group.

272. Typologies, methods and trends are studied and reviewed by SAFIU (AMLS, Article 11.4.Fourth.2) and then forwarded to the policy level (PCCML).

Recommendation 28 (Law enforcement powers)

273. Both the CPS and the AMLS give investigation officers the possibility to request or to obtain evidence.

274. The CPS provides the basis for investigation officers to obtain warrants to search persons and dwellings. In case of refusal or resistance by occupants of such dwelling the officers may use all lawful means to enter. Search may be for all items relative to the crime. Arresting suspects and seizure of items may take place at the time of the entry and search (CPS, Articles 41, 42, 45 and 46). The law also provides for the possibility to enter a dwelling and search it and its occupants and arrest suspects and seize items in case of the reporting (of the commitment) of a crime (CPS, Articles 79 - 81 and 85).

275. Article 8 of the AMLS requires designated reporting entities to promptly submit any documents, records and information if so required either by the judicial authorities, PA or by SAFIU. None of the reporting institutions may use the principle of confidentiality of the identity of clients, accounts and of records as a reason not to divulge any information.

Effectiveness (law enforcement powers)

276. While the investigation and law enforcement authorities have all necessary powers available in the CPS and AMLS, it is unclear to what extent these powers are used for AML/CFT purposes, as it seemed as if not much practical experience with these specific legal provisions exist.

Resources (Recommendation 30)

Overall

277. The authorities indicated that all agencies are well funded and reasonably well staffed and that they all have access to modern equipment and facilities. They also indicate that currently about 60 investigators and 27 prosecutors have sufficient financial (investigation) knowledge so that they may get involved in ML/FT cases when such is required. However, while the assessment team has no reason to doubt an overall lack of resources for law enforcement entities in the Kingdom, given the fragmented information relating to the *i)* overall number of law enforcement staff and budget and *ii)* dedicated AML/CFT staff and budget for units specialized in AML/CFT, the assessment team is unable to confirm that there are sufficient resources for AML/CFT investigations and prosecutions.

Professional standards (Recommendation 30)

278. All regular government employees, including investigation and law enforcement staff, are bound by the secrecy and confidentiality rules that apply to all civil servants in the Kingdom. Government employees are not allowed to keep official documents for themselves or disclose any professional information if not required by their professional duties. Employees are also not allowed to accept gifts, honors, grants, loans or scholarships from businesses that have any relation to the work of the employee[61]. The authorities indicated that there have been cases of corruption and breaches of confidentiality within

[61] Royal decree M/43 on 28/8/1393 (Article 7), Royal decree No M/9 on 24/3/1397 (Article 60) and Royal decree no M/49 on 10/7/1397 (Article 12.1).

law enforcement bodies: in 2004, 29 cases and 87 convictions; in 2005, 32 cases and 100 convictions; in 2006 40 cases and 139 convictions; and in 2007 77 cases and 227 convictions. It therefore seems that corruption cases are dealt with effectively and that corruption is not an issue that should impede the effectiveness of law enforcement.

Training (Recommendation 30)

279. The authorities have provided the following training to their employees.

280. At the PA, from 2005 to 2008, 117 trainees received a total of 579 days of training on investigation of developed financial crimes, investigating ML and TF, combating economic crimes and (mostly) general AML training.

281. At DPS, from 2000 to 2008, 346 trainees received (mostly) one-day (mostly college level) training on AML, organizational rules for combating drugs and ML, AML methods, organized crimes, combating economic crimes, ML risks, methods of combating economic crimes, organized trans-national crime, and financial qualification training for security and investigations authorities. Additionally, 67 trainees received general AML training that lasted between a few days and a few weeks, either in Saudi Arabia or abroad.

282. At GDI/AIO, 18 training sessions were held for 54 trainees. The trainees received almost 11 years of training time, on a variety of relevant subjects relating to ML, TF and general economic crime.

Additional elements

283. Between 2002 and 2008, MOJ and SAMA have organized 21 training sessions for 339 current judges at college level on ML and TF offences. MOI has also organized 15 training session for 419 newly incoming judges between 2004 and 2008 on ML and TF.

2.6.2 Recommendations and Comments

284. Overall, criminal investigation and law enforcement in Saudi Arabia seems effective. There are a few issues, however. It is illustrative that the authorities were not able of giving the assessment team a comprehensive overview of which investigation authorities work on which ML/FT cases, and no example of a case could be produced. Given the fragmented statistics relating to the numbers of (AML/CFT) staff and budgets, the assessment team is unable to confirm that sufficient resources are available. Also the team was not able to establish that investigation authorities other than the PA have sufficient awareness and knowledge of ML/FT to ensure that offences are properly investigated. The operational basis for the PA to work with other investigation authorities is by the conclusion of MOUs with these authorities.

2.6.3 Compliance with Recommendations 27 & 28

	Rating	Summary of factors relevant to s.2.6 underlying overall rating
R.27	**LC**	• Unclear if all investigation authorities other then the PA have sufficient awareness and knowledge to properly investigate ML/FT. • Operational effectiveness could not fully be established as statistics are not specific.
R.28	**LC**	• The effective use of powers for purposes of fighting ML and the effectiveness of

	Rating	Summary of factors relevant to s.2.6 underlying overall rating
		operational law enforcement cooperation could not be established.

2.7 Cross Border Declaration or Disclosure (SR.IX)

2.7.1 Description and Analysis

General

285. The Kingdom has implemented a declaration system for AML/CFT purposes since June 2007. The system replaces a similar system with higher thresholds and is thus fairly new[62].The new system appears to reach its final stages of taking effect and introduction to the public.

286. The legal basis is in the AMLS (Article 14). The article is very extensive and covers all features of the Saudi system. The law covers cash, bearer negotiable instruments[63] and precious metals valued over SAR 60,000 (or an equivalent amount in foreign currency), to be declared when entering or leaving the Kingdom. Only travelers with cash, bearer negotiable instruments or precious metals exceeding the declaration threshold need to submit a completed form, other travelers do not need to declare. The declaration form, however, includes a warning that non-declaration will expose the traveler to legal questioning. A reflection of the system is in the "Declaration Procedure Guide for cash amounts, transferable monetary instruments or precious metals" (the Guide).

287. The FATF describes a threshold of not more than USD / EUR 15,000. The SAR is floating against the EUR and the Saudi threshold of SAR 60,000 is currently below the EUR 15,000 threshold. The SAR is pegged against the USD against a rate of USD 1 : SAR 3.75, and since 1986, SAR 60,000 is worth USD 16,000, which is above the threshold. Considering that Saudi Arabia's main trading partner is the US, that its commodity exports are traded in USD (commodities account for 90% of all export earnings) and because of the long standing currency peg of the SAR against the USD.

288. Declaration forms are available for each traveler arriving or leaving the Kingdom. Upon arrival the assessment team did not note forms or signs to inform travelers of their duty to declare. When leaving the country the assessment team did notice signs but did not see forms at the airport.

289. The declaration forms are available in Arabic and English, and both versions are easy to complete. However, the forms only refer to the duty to report cash and precious metals, omitting bearer negotiable instruments. This is not in line with the AMLS, which includes BNIs. The authorities were made aware of this omission by the assessors, and indicated the desire to correct the form after exhaustion of the already printed stock of five million forms. The assessment team received a copy of the corrected declaration form within 2 months after the on-site.

[62] Before, KSA had a currency control declaration system with a threshold of SAR 100,000.

[63] While Articles 14.1 to 14.12 AMLS refer to cash, bearer negotiable instruments and precious metals, Article 14 of the AMLS only refers to cash and precious metals. This is not a legal gap, because Article 1(2) of the AMLS defines legal documents and deeds proving ownership of the assets or any right pertaining thereto as cash. In addition, Article 1.1.1 AMLS defines as cash bearer negotiable financial instruments, endorsed without restriction, including in favour of an unknown or beneficiary, such as traveller's checks, checks, promissory notes and payment orders.

290. It is uncertain why Customs and SAFIU (or the PCCML as some authorities indicated) did not design a form in line with their own law and why this mismatch with the law remained undetected for 21 months. This raises concerns about the full implementation of the system and it suggests a lack of sense of ownership.

291. The authorities have commenced a media awareness raising campaign, to educate and inform the public of the new declaration requirements at the borders. These advertisements include a reference to BNIs.

292. It is important to note that, due to restrictions for some goods to be brought into the Kingdom (*e.g.* alcohol, pork, non-Muslim religious items), every incoming passenger's baggage is scanned and checked by Customs. This lowers the risk of cash being smuggled into the Kingdom. For outgoing passengers there is an at random check performed by personnel of the Directorate of Public Security who will refer any traveler not fulfilling the declaration requirements to an official of Customs.

293. The declaration system refers to cash, postal parcels and consignments, meaning goods, thus covering all forms and sorts of cargo. It is interesting to note that where SR IX is about persons the Saudi system applies the obligation to declare equally to persons and to FIs and DNFBPs, including *Hajj* and *Omra* organizers and companies involved in the transit of cash. The authorities explained that all these parties were included as a consequence of a conscious policy decision to make sure that such parties indeed are obliged to make declarations in case their employees cross the border or hand over cash to someone at the other side of the border.

Powers of competent authorities upon discovery of a false declaration/disclosure or suspicion of ML/FT

294. Travelers are prohibited from entering or leaving the Kingdom when carrying cash, bearer negotiable instruments, or precious metals in excess of the threshold without filling out the declaration form. In case a traveler is caught carrying such after having failed to submit a declaration, he is referred by the concerned Customs-agent to a Customs-officer who will investigate the reasons of the non-declaration. In case the Customs-officer is satisfied with the explanation provided, he must require the passenger to fill out a declaration form, complete the remaining declaration formalities and he will allow the traveler to depart or enter with whatever this person was carrying.

295. If the Customs-officer is not convinced of the explanation or in case a traveler repeats a previous non-declaration or submits a false declaration, the concerned Customs-officer must prepare a seizure report of the incident and refer the traveler to the competent investigation officer at the port and notify SAFIU giving full details of the incident/declaration. In case of cash, Customs will only keep the amount in excess of the SAR 60,000 threshold, precious metals and BNIs will be retained as well, pending the outcome of the ensuing court case. The possible criminal sanction for false or non- declaration is a maximum imprisonment of six months and / or a maximum fine of SAR 100,000 (article 20 AMLS). There are no other sanctions for false or non-disclosure, unless there is a suspicion of a crime, such as ML/FT.

296. Custom officials can stop and interview the traveler in case of a non-declaration. In case of ML/FT suspicion, the traveler will be handed over to the competent investigation officer at the port. In that case all regular CPS law enforcement powers apply, including the power to stop or restrain cash, BNIs or precious metals for a reasonable time awaiting the outcome of the court case.

Information collected, retained and shared

297. On the declaration form, travelers need to submit: *(i)* name; *(ii)* nationality; *(iii)* date of birth; *(iv)* passport or ID number and place and date of issue; *(v)* address and telephone number in the Kingdom or in country of destination; *(vi)* purpose of travel; *(vii)* place of arriving from or departing to; *(viii)* port of entry or departure; *(ix)* flight number and *(x)* currency type and amount; *(xi)* precious metals and value, *(xii)* source and purpose of the cash or precious metals. Customs keeps this information, irrespective of whether or not the declaration was deemed true or false or a ML/TF suspicion has arisen.

298. The AMLS provides that copies of all declarations have to be submitted to SAFIU (Article 14.7). However, Customs only directly (same day) sends notifications of incidents/suspicious declarations to SAFIU; a copy of the seizure report and a copy of the declaration form of the traveler, as well as a copy of the passport or ID are submitted to SAFIU. All other (copies of) declaration forms are submitted, as agreed between Customs and SAFIU, once a month (on a CD)[64]. While this is sufficient for compliance with this Special Recommendation, it remains unclear what the criteria for suspicion are. The assessment team received a variety of statistics on the reporting of STRs by Customs to SAFIU. However it was not possible to extract from these the number of incidents/ notifications of suspicious declarations submitted on a direct basis as no distinction is made. This makes it difficult to assess the information flow. Considering the impressive IT systems of Customs and SAFIU that would easily enable a real time information flow between SAFIU and Customs, the monthly reporting on a CD seems not very efficient and causing statistics to be unclear.

Coordination among domestic competent authorities

299. At the border, Customs and Immigration authorities work in close vicinity as do the Border Troops[65]. The latter two belong to the MOI and are represented in PCCML and PCCT. The law enforcement authorities (that have a presence in the ports and to which Customs hands over the traveler and the seizure report) and SAFIU (which receives notification thereof) are also part of MOI, making cooperation easier. Nevertheless, as stated, the declaration requirements are at a late implementation stage and the law gives every traveler who did not make a declaration in fact a (second) chance to submit a declaration as yet. It should be noted though that, Customs officials will check the Customs IT system for any past incidents. There is no second chance for those that repeat the omission to declare or submit a false declaration. The assessment team could not fully establish what number of travelers had been referred to the investigation authorities and on which charges and what the outcome had been. The team was told about (examples of) several cases.

International cooperation and assistance

300. The World Customs Organisation (WCO) has opened one of its RILO (Regional Intelligence Liaison Offices) offices in Riyadh. It supports exchange of information between Bahrain, Jordan, Kuwait, Lebanon, Oman, Qatar, Saudi Arabia, Syria, the United Arabic Emirates and Yemen. All international

[64] Declaration Procedure Guide in art.01.01.06 and 02.04, and in the Circular to the Tax Directorate by the General Director of Taxes, No.579/21/ of 09/07/1428 AH

[65] The assessment team visited the Border Troops at Janadriyah (in the greater Riyadh area). Although there was no opportunity for a Q&A session, the team received an introduction to the work and resources of the Border Troops. Overall, the Border Troops seems to be well equipped and dedicated.

cooperation by Customs is through WCO. No information on specific cross-border cooperation is available.

Sanctions

301. In case a traveler entering or leaving the Kingdom fails to declare and fails to explain this omission, repeats a previous non-declaration, or submits a false declaration, the Customs official must prepare a seizure report of the incident and refer the traveler to the competent investigation officer at the port and notify SAFIU. The possible criminal sanction for non- or false declaration is a maximum imprisonment of six months and / or a maximum fine of SAR 100,000. There are no other sanctions possible as no administrative or civil sanctions exist. The assessment team is of the opinion that the range of sanctions is too limited and as a consequence of its possibilities restrictive. This means that the present sanction regime is not adequate and that the regime in place would be more effective, proportionate and dissuasive if more sanction possibilities exist. Administrative sanctions will enhance the speediness of handling cases as no investigation and law enforcement authority needs to be involved, while civil sanctions could make it possible to get paid for damages brought to the system which otherwise could not be recuperated. As is the case now and in case of a suspicion of a crime, including ML/ TF, Customs will forward the case and the traveler/suspect to investigation authorities. See for the effectiveness of the sanctions for ML/TF Section 2.1 and 2.2 of this report.

Confiscation

302. Customs is not empowered to confiscate any goods. It has the power to seize goods. Any seizure case would be (part of) the start of a criminal case and handled by the PA. Confiscation is only possible in case of a crime, including ML/TF. See for an overview of the confiscation regime section 2.3 of this report. At the time of the on-site, Customs had experience with seizure of cash, but not yet received feedback from law enforcement or the courts about the confiscation of these funds.

Freezing terrorist assets

303. See section 2.4 of this report for an overview of the regime for freezing of terrorist assets (per Special Recommendation III). The shortcomings identified in this section apply equally to this section. Customs staff indicated knowledge about the existence of UNSCR 1267 and its list. There was no other information available, including whether or not the knowledge about the existence of the list is based on the actual dissemination of that list within Customs. There are also no statistics available and there have been no positive or negative matches against a list.

Gold and silver

304. The Kingdom has opted to include all precious metals in the declaration system (but not precious stones). This goes beyond the requirements of Special Recommendation IX. In addition, in case of gold, precious metal and stones smuggling, Customs would inform counter parts through the WCO RILO network. No information was available as to the implementation of this policy.

Safeguarding information

305. All information that is collected by Customs is electronically stored at Customs main office in Riyadh and on a backup-server at an unidentified location. The information is securely protected and only accessible to those who have been authorized to access.

Resources (Recommendation 30)

306. Customs has 7007 staff. A legal advisor is tasked to work on ML/FT issues at the Legal Department at Customs headquarters. There is a technical team consisting of several specialized units at the main Customs Centre, headed by the legal advisor from the Legal Department, for the follow-up of ML/FT cases. The team includes legal advisors trained on AML/CFT who address ML/FT cases. These cases are considered as a crime to be addressed by the department as are smuggling of contraband, tax evasion, and trade fraud. In addition, there are specialists at each Customs point in charge of the implementation of declaration procedures. Other than for these officials, AML/CFT is considered to be part of the regular duties of any staff in Customs.

Professional standards (Recommendation 30)

307. All Customs staff are subject to the confidentiality requirements that apply to all civil servants. No further information was available.

Training (Recommendation 30)

308. All Customs staff receive regular training on a range of issues. 313 (2007) and 91 (2008) staff have been specifically trained on the new declaration system. In addition, 19 staff have received an AML course (2008 only). Finally, about 110 staff attended an AML symposium at SAMA in February 2009. While training on the declaration procedure obviously was a priority for Customs, it is the policy of Customs that as many staff as possible are trained on AML/CFT: these courses are comprehensive and not be limited to declaration procedures.

Statistics

309. Statistics submitted to the assessment team include information on BNIs but do not appear independently as such as they are included in the cash amounts since BNIs are legally considered to be cash. They will only appear in reports showing each currency separately. The statistics further showed declarations per port location. Statistics on the number of reports submitted to SAFIU combined with information on investigation/law enforcement authorities, and in case of suspicious transactions indicating the reason(s) thereof, the amounts or values involved and port location were not submitted. The table below shows a differentiation between declarations by regular travelers and FIs/banks. The amounts reported under 'Travelers' include the declarations made by the employees of banks carrying cash/ (traveler) cheques. This results in a very high average per traveler! The amounts under 'Banks' represent the declarations made by banks transporting cash/(travelers) cheques by (armored) car (services). The conclusion is that these statistics are not very clear and hamper the ability to draw workable (AML/CFT) conclusions from it.

Declaration forms 2 June 2007 – 28 February 2009					
			Incoming	**Outgoing**	**Total**
Travelers	**Cash**	**Declarations**	4 620	3 958	8 578
		Total value	SAR 4 508 524 982	SAR 2 816 787 640	SAR 7 325 312 622
		Average value	SAR 975 871	SAR 711 669	SAR 853 965
	Cheques	**Declarations**	2	6	8
		Total value	SAR 689 250	SAR 784 313	SAR 1 473 563
		Average value	SAR 344 625	SAR 130 718	SAR 184 195
Banks	**Cash**	**Declarations**	5 494	4 677	10 171
		Total value	Unknown	Unknown	Unknown
		Average value	Unknown	Unknown	Unknown
	Cheques	**Declarations**	8	Unknown	Unknown
		Total value	SAR 5 990 050	Unknown	Unknown
		Average value	SAR 748 756	Unknown	Unknown

Effectiveness

310. The AMLS and the Guide refer to 'traveler' (and sometimes 'passenger') as the party who should declare. According to the former, this term can be explained to include any individual (including a pilgrim) and any (non-)FI, which would include companies involved in the transportation of cash, postal parcels and consignments. In the statistics this distinction is only partially made. It would be beneficial for the AML/CFT-system as a whole and for Customs and SAFIU alike if statistics would show the different categories of travelers and also include the data which are mentioned above. The lack of comprehensive statistics make it difficult for the assessment team to confirm the effectiveness of the system. Overall, the team cannot confirm that the system has been effectively implemented as meant by SR IX.

2.7.2 Recommendations and Comments

311. The non-inclusion of bearer negotiable instruments on the declaration form and the not clear presence of signs and forms at the airport of Riyadh suggest a lack of effective implementation of the new declaration system.

312. The Kingdom, due to the large number of transient workers, appears to be the second largest market for remittances. As is indicated in Section 3 of this report, the strict rules for banking in the Kingdom make it likely that a considerable part of the remittance sector may be underground. Illegal remittance networks may well exist by the grace of trade based money laundering and illegal cash couriers. Also against this background, the assessment team considers the lack of comprehensive statistics worrisome.

313. The overall sanctions for false or non-declaration are low, and seizure provisions only target cash amounts above the threshold of SAR 60,000. This is ineffective and helps to keep the cost of doing

business for illegal cash couriers low. There are no administrative or civil sanctions possible and the available (criminal) sanctions are too restrictive. There is no sanction regime in place that can be considered to be effective, proportionate and dissuasive.

314. The deficiencies related to Recommendation 3 and Special Recommendation III have an impact on the rating of this recommendation.

315. The authorities have presented the assessment team with different sets of statistics, too many to be able to conclude that reliable and comprehensive statistics exist. The authorities should improve on this.

2.7.3 Compliance with Special Recommendation IX

	Rating	Summary of factors relevant to s.2.7 underlying overall rating
SR.IX	**PC**	• There is no effective, proportionate and dissuasive sanctions regime in place. • The overall effectiveness of the system could not be established due to a lack of comprehensive statistics that inform and support the AML/CFT regime. • Statistics to include a comprehensive overview of cases under investigation/law enforcement and sanctions. • The failings of Recommendation 3 and Special Recommendation III have a negative impact on the rating of this Recommendation.

3. PREVENTIVE MEASURES – FINANCIAL INSTITUTIONS

316. The Saudi Arabian financial sector comprises (1) the banking sector, (2) the insurance sector, (3) the financing sector and (4) the sector of investment companies. Whereas the first three sectors are supervised and regulated by SAMA, the CMA regulates and supervises the fourth sector. The AMLS and its implementing regulation (AML Regulation) apply to all four sectors. With respect to the financing and investment sectors, Article 1(5) of the AMLS provides that in addition to the expressly referenced entities, the definition of "financial and non-financial institutions" would also include "any institution in the Kingdom undertaking one or more of the financial, commercial or economic activities or any other similar activity specified by the Implementing Regulations of this Law."

317. In addition to the AMLS and the AML Regulation, each sector is subject to a range of obligations relating to AML/CFT as contained in various Rules and Regulations:

The banking sector

318. In addition to the AMLS and the AML Regulation, the banking sector, which includes money exchange businesses, is subject to the provisions of the Rules Governing Anti-Money Laundering and Combating Terrorist Financing (AML/CFT Rules for Banks and Money Exchangers[66]) and the Rules Governing the Opening of Bank Accounts and General Operational Guidelines in Saudi Arabia (CDD Rules). The relevant provisions of such rules will be outlined in the appropriate sections of this report. The RBME have first been enforced in 2003 and the CDD Rules in 2001. Both sets of rules were updated in 2008. Furthermore, SAMA issued a Compliance Manual for Banks that contain provisions relevant to AML/CFT.

[66] RBME.

The insurance sector

319. The Implementing Regulation for the Insurance Law ("Insurance Regulation") contains some provisions relevant to AML/CFT. Furthermore, SAMA issued AML/CFT Rules for entities licensed pursuant to the Insurance Law.

The financing sector

320. SAMA is issued AML/CFT Instructions for Financing Companies.

The investment sector[67]

321. The CMA issued two regulations relevant for AML purposes, the "AML/CFT Rules for Authorized Persons[68]" (RAP) and the "Authorized Persons Regulation" (APR).

AMLCFT Legal and Regulatory Instruments Issued for Financial Institutions				
Issuance	**Issuing authority**	**1st date of issue**	**Date of last update**	**Sector Covered**
AMLS	Royal Order	2003		All financial sectors
AML Regulation	Minister of Interior & Minister of Finance	2005	2008	All financial sectors
Banking Control Law	Royal Order	1966	-	Banking sector
Rules for enforcing the provisions of the Banking Control Law	Minister of Finance	1986	-	Banking Sector
AML/CFT Rules	SAMA	1995 (guidelines) / 2003 (rules)	2008	Banking sector and licensed money exchange businesses and remittance service providers
Rules for opening accounts and general rules for operating them (CDD Rules)	SAMA	2001	2008	Banking sector
Compliance Manual for Banks	SAMA	2008	-	Banking Sector
Insurance Law	Royal Order	2003	-	Insurance sector
Implementation Regulations for Insurance companies	Minister of Finance	2004	-	Insurance sector
AML/CFT Rules for Insurance Companies	SAMA	2009	-	Insurance sector

[67] The investment sector denotes the securities sector.
[68] Authorised person denotes any entity licensed by CMA (mostly securities sector entities).

AMLCFT Legal and Regulatory Instruments Issued for Financial Institutions				
Issuance	**Issuing authority**	**1st date of issue**	**Date of last update**	**Sector Covered**
Capital Market Law	Royal Order	2003	-	Capital Market Sector
Authorized Persons Regulation	CMA	2005	-	Capital Market Sector
AML/CFT Rules for Authorized Persons	CMA	2008	-	Capital Market Sector
Circular for Exchange institutions	SAMA	2000+2003 (circulars)	AML/CFT Rules for Banking Sector 2008	Licensed exchange institutions
Ministerial Decision for Financing Companies	Minister of Finance and National Economy	1999	-	Financing Companies
AML/CFT Instructions for financial companies	SAMA	2008	-	Financing Companies

322. According to Article 6-1 of AML IRs, the competent supervisory authorities sets and develops the appropriate regulatory instructions and rules to be applied against the crimes prescribed by AMLS and the means and controls necessary to measure compliance of financial and non-financial institutions with laws, rules and regulations to combat ML and TF. Both SAMA and CMA therefore are empowered by the AML IRs to issue regulatory measures, to supervise their implementation and to sanction non compliance.

323. In light of the above, AML/CFT Rules and Regulations issued by SAMA and CMA are considered as other enforceable means, being issued by competent supervisory authorities designated by AMLS and its implementing regulations. However, most of these regulations are fairly new and been introduced recently or recently updated, so the effectiveness of such regulations could not be (fully) established during the visit.

324. In addition to the above instruments, SAMA issued in 1995 an AML/CFT Guidance Book, in which it provided basic introduction of ML and TF concepts and techniques and the basic duties of financial institutions to prevent such activities.

325. SAMA circulated in 2005 the compliance principles of Basel and requested banks to abide by them. In 2008, SAMA issued the official Compliance Manual, which the authorities state has covered Basel's principles and AML/CTF regulations. The authorities stated that such Manual is in line with other supervisory requirements and the nature of the banking sector.

Customer Due Diligence & Record Keeping

3.1 Risk of money laundering or terrorist financing

326. The Saudi authorities have not conducted a national risk assessment of the vulnerability to and risks of, money laundering and terrorist financing through the various sectors of the financial system in the Kingdom (see also section 1.5.c of this report) and therefore they do not apply a risk-based approach to the application of the preventive measures on a sector-specific basis. Consequently, no sectors have been specifically exempted from the provisions under the AML/CFT law and regulations on the basis of a risk assessment.

327. The authorities noted that certain practices mitigate the risk of ML and TF abuse in Saudi Arabia's financial sector. In particular, they noted that financial services cannot be offered to non-residents, with the exception of GCC nationals[69]. According to Article 200-2-3 of the Rules Governing the Opening of Bank Accounts, however, Saudi banks and branches of foreign banks operating in the Kingdom are able to open accounts for non-residents with the prior approval of SAMA. The specific policies and procedures defining the mechanism used by SAMA to grant such approval were not provided to the assessment team. As such, it was noted that the lack of an assessable procedure for the opening of accounts by non-residents presents a possible loophole. As the Kingdom continues to position itself as a major economic player in the region, introducing robust economic reforms and encouraging foreign investment, such possible existence of an informal shadow system and the risk it may carry is of concern.

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

3.2.1 Description and Analysis

328. Article 4 of the AMLS and its Implementing Regulations (AML IRs) (Issued by Royal Decree M/39 dated 23/08/2003) draws the general framework of customer identification duties falling on financial institutions (among other institutions): identification, verification, data updating, profiling, enhanced due diligence (EDD), etc.

329. Banks and money exchange businesses are also expected to abide by additional obligations listed in the RBME issued by SAMA such as the adoption of a risk-based approach, KYC standards and customer risk assessment, as well as detailed procedures stemming from the Rules governing the opening of bank accounts and general operational guidelines in Saudi Arabia (CDD Rules for Banks).

330. Insurance companies are required to observe conditions for business relations acceptance and customer identification, among other requirements stipulated in SAMA's AML/CFT Rules for Insurance Companies" (RIC). In addition, insurance companies are subject to the Cooperative Insurance Companies Supervision Law and its Implementing Regulations (Insurance IRs), which cover some AML/CFT related issues.

[69] GCC nationals, other than Saudis, are foreigners, but enjoy some privileges that are not offered to nationals from outside the GCC countries.

331. Financing (leasing) companies are required to follow SAMA's AML/CFT Instructions for Financing Companies (IFC) by which KYC and CDD requirements are expressed similarly to those issued for insurance companies.

332. The AML/CFT Rules issued by the CMA require authorized persons to apply a risk-based approach to client acceptance policies and due diligence measures. Possible reduced and enhanced diligence measures are detailed within Article 9. Authorized persons are also subject to a more general set of requirements, the Authorized Persons Regulations (APR), which include CDD related obligations (record keeping, KYC, etc.).

333. Overall, the AMLS, its IRs, and the set of regulatory rules provide a satisfactory CDD legal framework.

334. This said, much of the remaining description on CDD will focus on the degree of implementation. Concerns may result from a variety of factors, such as the difficulties reported by some financial institutions in persuading clients to comply with CDD requirements.

335. The focus on the verification of effectiveness is also based on a number of other reasons; for instance, it was possible to observe a heavy reliance on automation and specialized software in tackling risk profiling, while that did not seem to be complemented with necessary customization of risk parameters in order to administer the customer due diligence process in a more comprehensive way. On the other hand, the prevailing interpretations of AML- and CFT-related customer/transaction/product risks proved to be limited to cash-sensitive dealing for many financial institutions, which calls in to question the validity of classifications and CDD measures applied accordingly. The assessment team found that the quality and level of implementation varied greatly between bank and non-bank financial institutions, as well as among institutions belonging to the same sector. Finally, the presence of a monitoring threshold parameter (among others) of SAR 60,000 (USD 16,000 / EUR 12 300) for banks and money exchange businesses, in conjunction with a heavy reliance on automated monitoring systems (in banks) likely means that many risky transactions or accounts may go by unnoticed.

Prohibition of anonymous accounts

336. Article 4 of the AMLS stipulates that a financial institution shall not conduct any financial or commercial transaction under a false or unknown name. The definition of the term “transaction” includes any action involving money or cash and therefore extends to any dealings with any client. The verification of identity is mandatory at the outset of dealing with these clients, which eliminates the possibility of opening accounts in anonymous or fictitious names.

337. The AMLS does not prohibit financial institutions from maintaining numbered accounts, and although these institutions stated that they were not offering such service, this practice remains possible in the insurance, securities and leasing sectors. As to banking institutions and money exchangers businesses, the identification requirements and due diligence procedures in the RBME prohibit the opening of numbered accounts. On the other hand, it should be noted that Article 4.5.5 of RBME forbids banks to open account in fictitious or anonymous names or numbered accounts for private banking customers.

338. With respect to the capital market sector, Article 39 of the APR provide that authorized persons must, before dealing with, advising, or managing assets for a customer, obtain a minimum of information

including name, date of birth, ID number, citizenship, phone number, address, as well as information on the employer, such as the employer name, address, and phone number. The APR also provides that "such information must be obtained as a precondition to providing such services". Article 8.1 of AML/CFT Rules forbids opening anonymous accounts or accounts using false names or fictitious names, but does not address numbered accounts.

339. With respect to the insurance sector, Article 71 of the Insurance IRs require entities licensed pursuant to the Insurance Law to maintain separate registers for each class of insurance, including the insured person's name and address, the policy number, date of issuance, policy period, type of risk and property or activity insured as well as insurance premium and premium paid. Article 14 of RIC forbids providing products and services to persons having anonymous or fictitious names.

340. Similarly, Article 3.2 of the IFC forbids performing any transactions financial or commercial relations or any other operation with an unknown or fictitious name.

341. Given that no provisions deal with numbered accounts in particular, the opening of such accounts remains a possibility in financial institutions other than banks and money exchangers businesses. There is no specific guarantee in a primary or secondary legislation that, in case such accounts are opened, financial institutions (other than banks and money exchangers businesses) are required to maintain them in such a way that full compliance with the FATF Recommendations can be achieved. However, the overall CDD measures applicable would not differentiate between such accounts and other types of accounts, and therefore the financial institution would be required to identify and verify the identity of the customer and beneficial owner of the numbered account. In practice, it seemed that financial institutions do not keep anonymous or numbered accounts or accounts in fictitious names, however the lack of legal framework does not preclude this as indicated above.

When CDD is required

342. Article 4 of the AMLS stipulates that identification must occur "at the outset of dealing with these clients or when concluding commercial deals".

343. Article 4.2 of the IR of the AMLS requires that the identity and legal status of clients and beneficiaries is to be established for all customers upon opening an account or initiating a transaction. A "transaction" is defined as "any action involving money, property or cash or in kind of proceeds, including deposit withdrawals, transfer, selling, buying, loaning, safekeeping or the like". Article 4-3 of the IR of the AMLS also provides that the measure should be repeated "whenever there is doubt of the accuracy or adequacy of the customer data obtained at any stage of dealing with the actual client or true beneficiary, or whenever there is a suspicion of money laundering or terrorism financing regardless of the amounts", knowing that "data related to the verification of identity shall be updated periodically".

344. On the other hand, the CDD Rules for Banks require that "dealings between banks and their customers must start and continue in all aspects based on valid ID documents". These Rules require, under Articles 3-1 and 4, the updating of identification documents and account information database at least every five years for Saudi nationals. For non-Saudi customers (*e.g.*, non-residents, corporations), a period of sometimes no more than 6 months to a maximum of 3 years has been defined for updating and validating customer identification records. In case these documents expire or the personal data is not

updated, the bank has to freeze the account. SAMA follows up on the statistics regarding the updating of account data at the end of each year.

345. Article 4.3.2 of the RBME forbids banks and money exchange businesses from opening new accounts or accepting business relationships or transactions whenever CDD cannot be conducted and requires them to report these cases to the Saudi Arabian FIU (SAFIU), with a copy sent to SAMA. RBME also requires further due diligence if there are doubts about the integrity or adequacy of previously obtained customer identification data. In such cases, re-verifying the identity of the customers and re-assessing the relationship should be undertaken. Article 5.1.2 stipulates that "banks and money exchangers should always have adequate information about the originator/remitter" of wire transfers and to accept these transfers "only from customers with accounts or other relationship agreement" (*e.g.*, express remittance service).

346. With respect to the capital market sector, Article 39 of the APR provides that authorized persons must obtain cited information "*before* dealing, advising, or managing for a customer", and "as a *precondition* to providing such services".

347. The completeness and effectiveness of implemented CDD measures was at times questionable: incidences of postponing / limiting / ignoring the implementation of such measures with respect to establishment of relationships with transient customers (in the case of money exchange businesses) were indicated. In cases where a suspicion is detected, the general practice that seemed to be followed is to conduct internal investigation or simply report to SAFIU, thus preferring not to involve the customer in a CDD process that might raise tipping-off concerns, according to most financial institutions. As for the updating of previously obtained customer data, the efforts reported by financial institutions were rather focused on their regular updating programs and blocking activity on accounts with expired identification documents, which suggests that performing CDD measures based on doubts about the veracity of previously obtained information is possibly not being implemented. Finally, as is also explained in Section 3.7 of this report, the monitoring threshold parameter of SAR 60,000 (AML/CFT Rules 4.6.3) means that most customer relationships may stay below the radar, which would exclude the requirement to undertake CDD measures when there is a suspicion of money laundering or terrorist financing below this threshold. However, the authorities reported that many suspicious transactions under this amount have been detected and reported. Similarly, the RIC (Article 8) specify a monitoring threshold parameter of SAR 10,000, however, it does not seem to effectively impede the detection of suspicious transactions below the threshold.

Required CDD measures

Identification and verification

348. Article 4 of the AMLS states that "the identity of the clients shall be verified against official documents" and that "institutions shall verify the official documents of the corporate entities showing the name of the institution, its address (etc)".

349. Article 4-1-1 of the AML IRs provides for the verification of "identities of all permanent or occasional clients against valid officially certified original documents proving their identities" and provides a set of these documents for both categories of clients: Saudi nationals and individual expatriates. This includes information on the address of the person and the place of residence/work.

350. The assessment team found that financial institutions are aware of their duty to identify clients, however, the team also noted instances in which customer identification files were incomplete (for example missing copies of official identification documents). This suggests that the identification and verification process is insufficiently implemented.

Identification of legal persons

351. With respect to the identification of an authorized representative, Article 4-4 of the AML IRs requires that financial institutions should "determine whether any customer is acting on behalf of another person and to take measures to identify and verify the identity of that person, with particular attention to accounts and business relationships operated under power of attorney".

352. Article 4 of the AMLS stipulates that covered institutions "shall verify the official documents of the corporate entities showing the name of the institution, its address, names of proprietors and managers authorized to sign on its behalf".

353. Article 4-1-1 of the AML IRs requires covered entities to verify the identities of legal persons based on obtained copies of the Articles of Association, the commercial registration, the license issued by the relevant issuing authority, as well as a list of persons authorized by the owner to deal with the accounts based on the Articles of Association, a power of attorney issued by a notary public, or an authorization given at the bank and to obtain a copy of the identification document of each authorized person.

354. Concerning banks, Article 3-1-3 of the CDD Rules requires monitoring of the validity of the ID cards of the directors and authorized signatories of the accounts of legal entities. This requirement is also applicable to owners of private establishments and companies (except joint stock companies). According to Article 8, banks should understand the true relationship of individual customers who open accounts as guardians, agents, trustees or authorized representatives, and ensure that such sponsors, nominees, trustees or authorized representatives do not act only as a "front" for other individuals or intermediaries or on their behalf.

355. As to capital market authorized persons, Article 8 of the AML/CTF Rules requires obtaining copies of the following documents for legal persons: commercial register, Articles of association, identification card of the manager in charge, issued resolution forming the board of directors, board resolution evidencing the approval of the opening of the account and conferring authorization on the signatories, list of the persons authorized who are qualified to deal with the accounts, pursuant to what is provided for in the commercial register, and a copy of the identification card of each.

356. For insurance companies, Article 16 of the RIC requires obtaining copies of the commercial registration and identity card of the manager in charge in licensed companies, enterprises and shops.

357. Concerning leasing companies, according to Article 3 of the AML/CFT Instructions, financing companies shall obtain, when dealing with licensed companies and establishments, copies of the Commercial Register, the articles of association, the national ID card of the owner of the licensed commercial or service facility, the list of persons authorized by the owner to operate the accounts according to what is stated in the commercial register document or by virtue of a power of attorney and a copy of the ID card of each of the said persons shall also be obtained.

358. The assessment team found that many financial institutions do not obtain information concerning the directors of legal entities. For example, some institutions adopted KYC forms that do not contain inquiries about such information, however the information may be collected separately. Proof of incorporation of these entities has not been retained in several instances. The authorities noted that most banks' automated system do not allow the creation of a new account unless all information fields are completed including these mandatory fields.

Beneficial ownership

359. Article 4 of the AMLS requires that the identity of the clients must be verified "at the outset of dealing with these clients or when concluding commercial deals whether directly or on their behalf".

360. Article 4.2 of the AML IRs further provides that the identity and legal status of the actual clients and beneficiaries, defined as the natural person ultimately owning or controlling a customer and/or on whose behalf a transaction is being conducted, has to be obtained and verified for all customers.

361. Article 4.4 of the AML IRs requires covered entities to "determine whether any customer is acting on behalf of another person and to take measures to identify and verify the identity of that person".

362. Concerning banks and money exchange businesses, Article 4.3.3 of the RBME requires understanding the structure of the company sufficiently to determine the provider of funds, principal owners of the shares and those who ultimately own or have control over the assets, *e.g.*, the directors and those with the power to give direction to the directors of the company. For a joint stock company, it is required to establish the identity of all shareholders who own 5% or more of the company's shares. Documentary evidence of the legal entity and existence along with the identity of the beneficial owners including the actual natural persons owning or controlling the entity should be obtained.

363. As to authorized persons, Article 8.2 (b) of the CMA's AML/CTF Rules requires the identification and verification of beneficial ownership and control using original documents. Article 8.4 (b) requires obtaining sufficient information about the ownership and control structure of legal entities to identify the individual(s) that ultimately own(s) or control(s) the client.

364. For insurance companies, Article 15 (b) of the RIC stipulates inquiring about the actual beneficiaries and dominating parties on the insurance transaction. Article 24 stipulates that for legal persons, companies should know the ownership and responsibility structure and determine natural persons who fully own or dominate the applicant.

365. Concerning leasing companies, pursuant to Article 3 of the IFC, these shall obtain sufficient information about the nature of the business and the customer's ownership structure for legal entities.

366. In practice, financial institutions demonstrated a flawed understanding of the requirement to obtain and verify beneficial ownership. Some institutions did not seem to inquire the client about it. When some financial institution proved to be verifying ownership, it stated to perform it "up to the third level", and in other instances "up to first level"; as for understanding the control structure of legal entities, it seemed that institutions knew little about it. It was frequently noted that adopted KYC forms do not contain fields by which such information can be retained; institutions appeared to be satisfied with reliance on received copies of official documents (mainly commercial registration and Articles of Association) to

collect the information required above (which does not makes it possible for shareholders of bearer shares companies).

Purpose and intended nature of the business relationship

367. Concerning banks and money exchange businesses, Article 4.3.4 of the RBME requires the creation of a customer profile which includes, amongst other things, information on the "purpose and the intended nature of business relationship, information of the business activities, financial information, capital amount, source of funds, source of wealth, branches, countries and products dealing in, etc". It also stipulates the creation of a transaction profile "to capture the number of transactions expected to be used by a customer, and the value of transactions for an average month, for each product and service". In addition, Article 4.3.2 (11) expects from banks to not accept new and terminate any existing client accounts, relationships or transactions if information on the purpose and intended nature of the business relationship cannot be obtained. CDD Rules repeatedly requires banks to inquire about the purpose of establishing the business relationship.

368. For the capital market sector, Article 39 of the APR provides that before an authorized person deals with, advises, or manages assets for a customer, information on the customer's financial situation, investment experience and investment objectives relevant to the services provided has to be obtained. In addition, Article 8 (2) of the RAP requires that information on the purpose and intended nature of the business relationship is obtained.

369. For the insurance sector, Article 15 (c) of the RIC requires that information is being obtained on the purpose and the nature of the business relationship.

370. As to the financing sector, Article 3 Section 2.1. AML/CFT Instructions sets out detailed CDD measures and requires finance companies to keep a credit file for all its customers indicating, amongst others, the purpose of the financing and the nature of the customer's activities.

371. It appeared that most financial institutions inquire their customers about the intended nature of the business relation and expected transactions, however, this is done in a formal manner.

Ongoing due diligence

372. The AMLS and IRs do not explicitly require financial institutions to conduct ongoing due diligence on the business relation*ship. However, Article* 4.3 of the AML regulation provides that "Data related to the verification of identity shall be updated periodically": it is not clear if the extent of identity verification covers the set of due diligence measures. While the AMLS and IRs include general provisions requiring due diligence, the supervisory authorities have issued detailed regulations related to ongoing due diligence procedures to be implemented by financial institutions.

373. For the banking sector and licensed money exchange businesses, Article 4.3.4 of the RBME requires that the information used to establish the client and transaction profiles should be kept updated at least annually or upon suspicion of illegal activity. It also requires that activity and transactions should be monitored throughout the business relationship to ensure that the activity and transaction is consistent with the bank's or money exchange business's knowledge of the customer, including the source of the funds and the level of risk associated with the customer.

374. For the capital market sector, Article 8 of the AML/CFT Rules requires that ongoing due diligence and scrutiny is applied, *i.e.* that ongoing scrutiny of transactions and accounts throughout the course of the business relationship is applied to ensure that the transactions being conducted are consistent with the authorized person's knowledge of the client and the client's profile, taking into account, where necessary, the client's source of funds. Article 18 of the RAP clearly stipulates that identification data collected under the CDD process should be kept up-to-date, accurate and relevant. Annual or *ad hoc* reviews of existing records must be undertaken, particularly for higher risk categories of clients or business relationships, or when trigger events listed in the provisions occur.

375. For the insurance sector, Article 15 (c) of the RIC establishes clearly that the existence of proper information is a pre-requisite for conducting ongoing due diligence. Article 15 (d) requires that this diligence occurs in a continuous manner, such as continuous audit in all operations concluded during the working relation period to guarantee that all operations comply with the knowledge and the data of the customer. Article 27 of the RIC requires that companies must continue to make a maximum effort to inquire about the customer during the whole working relation period and to update the data of all customers on a regular basis. Article 22 further provides that data received in accordance with CDD measures have to be updated to ensure their accuracy and safety. A periodic review or a review based on the need for additional records should be performed, in particular with respect to high risk customers or business relationships.

376. For the financing sector, Article 3 (para. 2.2) of the AML/CFT Instructions provides that basic due diligence shall be conducted on all customers on a continuous basis to verify the accuracy of the business relationship with the information provided to the Company. Article 4 (para. 6) of the IFC requires that data, records and documents obtained through the CDD measures are to be kept updated by undertaking reviews of those files periodically or as necessary.

377. As explained above, the ongoing due diligence requirement is not provided explicitly by primary or secondary legislation. The assessment team found that scrutiny of transactions for consistency with due diligence data is not being conducted routinely by non-bank financial institutions. Many banks reportedly rely on specialized transaction monitoring software for such scrutiny. The transactions monitoring threshold parameter of SAR 60,000 means that most customer relationships may in any case stay below the radar. The quality and frequency of updating of CDD data appeared to be questionable concerning many financial institutions. Key factors supporting the statements above are: the low level of reporting, the flawed understanding of beneficial ownership, the fact that the specialized software applications are mostly unable to operate matching between KYC data and transactional records, and the reported reluctance of clients in providing information on their source of funds and other key data.

Risk

Enhanced due diligence

378. Article 4.5 of the AML IRs requires the application of enhanced due diligence measures for high-risk categories of customers, business relationships, or transactions.

379. In addition, for the banking sector and licensed money exchange businesses, Article 4.3.1 (3) of the AML/CFT Rules requires the application of "increased levels of due diligence" with respect to customers that are determined to be "high-risk". This Article lists key factors to consider when making the

determination, such as the customer's business activity, the ownership structure, anticipated or actual volume or types of transactions, correspondent banking relationships and PEPs. Pursuant to the provision, every customer relationship should undergo a risk assessment in accordance with Article 4.5 of the RBME, which sets out different measures to be applied to different categories of clients, including amongst others PEPs, private banking clients, charities, trustees, agents and intermediaries accounts.

380. In cases where a customer, account or transaction is considered high-risk, a greater scrutiny is required (Article 4.3.4). The approval of senior bank management is required to open or retain certain accounts for certain clients, including PEPs and private banking customers. For private banking customers, Article 4.5.5 further requires the application of enhanced due diligence. SAMA approval is required for the opening of accounts for social, charitable or donation purposes. In addition to the specific provisions outlined above, the CDD Rules provide under "ongoing monitoring of accounts and transactions" that accounts and transactions must be classified according to the risk level so that no high risk accounts will be opened except after obtaining the bank senior management approval.

381. For the capital market sector, Article 9 (2) of the AML/CFT Rules requires enhanced due diligence measures for higher risk types of clients, business relationships or transactions, depending on the client's background, transaction types and other specific circumstances. Article 9 (6) provides a list of additional measures to be performed by authorized persons as enhanced due diligence on higher risk clients.

382. For the insurance sector, Articles 60 and 61 of the RIC list categories of high-risk clients and require the development of policies, procedures and internal restrictions for obligatory care measures towards any high-risks customer. One of the listed measures "to be taken into consideration" stipulates the recruitment of employees at the service of high-risk clients and apply due diligence procedures and continuously monitor them in order to guarantee the disclosure of any suspicious or unusual activity at the right time.

383. For the financing sector, Article 3 (para. 2.3) of the AML/CFT Instructions provides that for all high-risk business relationships and transactions, additional due diligence measures shall be applied. Key factors determining whether a client is high-risk or not are: the geographical location of transactions, the beneficiary and the place of business operation; the nature of the transactions and services requested by the customer; and any information indicating that the client is a PEP or a customer in a country that does not or insufficiently applies the FATF Recommendations.

384. Some financial institutions appeared to have a limited perception of who could be a high-risk customer. The assessment team found that some insurance companies do not perform a classification of customers according to their respective AML/CFT risk. Applied due diligence measures (senior management approval, retaining copies of official documents, periodic review of relationship, and inquiry about source of wealth/funds, etc.) by some financial institutions were not satisfactory. These observations and factors suggest that the implementation of enhanced diligence in some sectors is also not satisfactory.

Reduced due diligence

385. For banks and money exchange businesses, Article 4.3.1 of the RBME provides that a standard level of due diligence should be applied to all customers. This level is reduced in recognized lower risk scenarios (such as publicly listed companies, other financial institutions, individuals whose main source of

funds is derived from salary, pension or social benefits, transactions involving small amounts or particular types of transactions). Article 4.5.1 provides detailed rules to be used as minimum standards when opening accounts for individuals "who are employed/on payroll, on pension or with a regular fixed income and whose main source of income is derived from salary, pension, social benefits and the like, from an identified and appropriate source and whose transactions commensurate with the funds". The Article stipulates that simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply.

386. For the capital market sector, Article 9 of the AML/CFT Rules provides that reduced CDD measures may be performed on a client that is a company listed on the stock exchange of a country that sufficiently implement the FATF Recommendations, or is a subsidiary of such a listed company. In such a case, some requirements (identification of beneficial ownership / control) do not need be carried out. However, where such a listed company is closely held *i.e.* subject to the beneficial ownership/control of an individual or a small group of individuals, an Authorized Person shall carefully review the AML/CFT risks and consider whether it is necessary to verify the identity of such individual(s).

387. There have been no indications pertaining to the implementation of reduced CDD measures on resident customers. As for customers resident in another country, the simplified or reduced CDD measures have not been tailored to address any country limitations to the applicability of these measures. Although these customers' accounts are to be classified as high risk, the shortcomings listed in section 3.6 indicate that the differentiation between these customers and the resident customers is virtually and effectively not enforced with respect to the applicability of provisions related to simplified CDD measures.

Timing of verification

General rule for timing of verification

388. The AMLS (Article 4) requires that the identity of the clients shall be verified against official documents "at the outset of dealing with these clients or when concluding commercial deals" whether directly or on their behalf.

389. Concerning banks and money exchange businesses, Article 4.3.2 of the RBME stipulates that identity verification of the client must occur at the start of dealing with such client or upon concluding commercial transactions therewith, in person or in proxy. Under 4.3.2 (2), it is required to establish the identification of the customer based on acceptable official documentation and verify the identification at the outset of the relationship or before opening an account. Under 4.3.2 (11), it is explicitly required to close accounts if identity verification cannot be satisfactorily conducted through the provision of individual and commercial IDs. Under Article 4.5.2, it is prohibited to accept any transactions for walk-in customers unless any of the exceptions listed in the provision applies. In cases where the client relationship has already been initiated, the bank account has to be frozen pursuant to Articles 3-1-1 to 3-1-3 of the CDD Rules if in the course of the relationship the identification document on file expires.

390. For the capital market sector, Article 12 of the AML/CFT Rules requires that the identity of the client, beneficial owner or potential client is verified before or during the course of establishing a business relationship.

391. For the financing sector, Article 3 (Para. 1) of the AML/CFT Instructions requires that the identity and legal status of the customer and the beneficial owner are obtained and verified at the beginning of the transactions. Article 6.6 also states that in cases where a company is unable to comply with CDD measures, including when failing to obtain or verify the client identity or obtain information about the purpose of the client relationship, any dealings should be terminated.

392. At some financial institutions, it seemed that some customer files do not contain key documents pertaining to the identification process: It is not clear whether this situation reflects a failure in performing timely identification.

Delayed verification

393. The AMLS requires that the identity of the clients shall be verified at the outset of dealing with these clients or when concluding commercial deals. No provisions establish the possibility to deal with any client based on delayed implementation of identity verification.

394. As indicated earlier in relation to the capital market sector, Article 12 of the AML/CFT Rules requires that the identity of the client, beneficial owner or potential client to be verified before and during the course of establishing a business relationship.

Failure to satisfactorily complete CDD

Before commencing the business relationship

395. For banks and money exchange businesses, Article 4.3.2 (11) of the RBME provides that no new accounts, business relationships or transactions may be accepted and any existing accounts, business relationships or transactions should be closed/terminated if the identity of the customer cannot be verified, the beneficial owner is not known or information on the purpose or intended nature of the business relationship cannot be obtained. In case banks or money exchange businesses identify any of the above cases, they should immediately report them to the SAFIU with a copy to SAMA. Article 6-6 of the CDD Rules states that in such cases, the bank is not allowed opening of the account, starting the relationship or executing any transactions and that SAFIU must be advised about the suspicions.

396. For the financing sector, Article 6.6 of the AML/CFT Instructions states that in cases where a company is unable to comply with CDD measures, including when failing to obtain or verify the client identity or obtain information about the purpose of the client relationship, any dealings should be terminated and the company should consider filing an STR with the SAFIU.

397. For the insurance sector, Article 25 of the RIC provides that the company must inquire about the identity of the customer, the possible customer, and the actual beneficiary before and during the working relation. Companies which are unable to make the maximum possible effort to inquire about the customers must not perform the required operations by the customer at the beginning of the relation. In such case, the company must study the need to notify SAFIU. The company must not start dealing with any customers before completing all determination measures and inquiring about the customer.

398. For the capital market sector, Article 8.6 of the AML/CFT Rules provides that if there is doubt or difficulty in determining whether the document obtained to verify the identity is genuine, authorized persons must not open the account and shall consider making an STR to the SAFIU.

399. With money exchange businesses, it appeared possible to conduct business transactions simply against submitting a copy of identity. At some financial institutions, it seemed that many customer files do not contain key documents pertaining to the identification process: It is not clear whether this situation reflects a failure in satisfying the requirement to refuse relationship and report accordingly.

After commencing the business relationship

400. The provisions of the RBME and the AML/CFT Instructions for the financing sector relating to situation before commencing the business relationship apply equally to situations after commencing a business relationship.

401. For the capital market sector, Article 12.2 of the AML/CFT Rules provides that when the Authorized Person is unable to perform the CDD process satisfactorily at the account opening stage, it must terminate the business relationship and not perform any transaction, and must consider whether a Suspicious Transaction Report (STR) must be made.

402. Insurance companies are not explicitly required to terminate the business relationship and consider making a suspicious transaction report in case required CDD measures could not be applied to existing customers and to cases whereby the institution has doubts about the veracity or adequacy of previously obtained customer identification data. At some financial institutions, it seemed that many customer files do not contain key documents pertaining to the identification process: It is not clear whether this situation reflects a failure in satisfying the requirement to terminate relationship and report accordingly.

Existing customers

403. No legal or regulatory provisions deal explicitly with the concept of existing customers as defined by the Recommendation 5 of the FATF Standards[70]. The mentioning of existing customers refers broadly to institutions' actual, *i.e.* old as opposed to new, customers (regardless of whether they are so before or after the date the national requirements are brought into force). This, in turn, renders any requirements applicable vis-à-vis "existing customers" part of the usual ongoing CDD. No reference is made to applying CDD requirements on the basis of materiality or risk in the current set of requirements.

404. Therefore, certain actions are required in relation to applying CDD on existing customers at appropriate times. Concerning banks and money exchange businesses, Article 4.3.2 (11) of the RBME stipulates that any existing account, business relationship or transaction should be frozen, where the identity of the customer cannot be verified or the identity of the beneficial owner is not known or there is a failure to obtain information on the purpose and intended nature of the business relationship. The Article also requires the updating of beneficial ownership for existing accounts whenever there is a suspicion that the account, relationship or transaction is being used for a different or illegal purpose, thus requiring more

[70] Existing customers as at the date that the national requirements are brought into force.

information from the customer; or during the mandatory periodic updating of customer information, as per SAMA Account Opening Rules (CDD Rules).

405. Article 4.5.4 stipulates that policies and appropriate risk management systems should be in place to identify and categorize PEPs and related individuals for closer scrutiny. Identification of PEPs should include the existing and new customers as well as the beneficial owners. In addition, if an account completes six months without any movement whatsoever, the account will be considered "inactive" and any transaction or withdrawal from the account has to be approved by two employees as well as one member of senior management of the bank.

406. Under Para. 3.2, CDD Rules stipulate that banks have the right to freeze the account upon the expiration of the customer's ID or when the account holder does not update his personal data and information, addresses, income sources and signature, etc. Article 4.11 states that if there is any suspicion of money laundering or terrorist financing in any time, customer and authorized persons information must be updated.

407. In addition, SAMA issued circulars in 2003 and 2004 requiring banks to finalize the updating of existing accounts and setting deadlines for it. The circulars tackle the account freezing process for the purpose of conducting the updating plans and provide suggestions to banks in this regard. Moreover, SAMA conducts a yearly follow-up on the updating process at banks, requiring the latter to provide detailed figures on the implementation progress.

408. For the capital market sector, Article 18 of the RAP requires to obtain updated information on existing client accounts in certain situations.

409. For the financing sector, Article 3 (Para. 4) of the IFC provides that client information and data obtained through the CDD process shall be updated periodically for all clients, including customers existing at the time of the implementation of the Instructions. Updating is further required if, at any stage of the dealings with the beneficial owner or client, any doubts about the accuracy or efficiency of the information obtained surface or whenever there is a suspicion of ML or FT.

410. As indicated above, banks, money exchange businesses, insurance companies and authorized persons are not explicitly required to apply CDD requirements to existing customers on the basis of materiality and risk. On the other hand, financial institutions are required to conduct due diligence on such existing relationships at appropriate times. It appeared that financial institutions focus mainly on updating copies of official documents when updating accounts; therefore, the assessment team is of the view that the quality of updating was not proper at some financial institutions, or that the process has not been completed. It seemed that CDD information for existing business relationships at many non-bank financial institutions is not up-to-date.

CDD for existing anonymous accounts

411. As discussed above, anonymous accounts and accounts in fictitious names are not permitted in KSA. Numbered accounts, despite not being prohibited in non-banking sectors, seem also to not exist in KSA. Consequently, applying CDD measures on existing customers in relation to those types of accounts is not applicable. On a practical level, the authorities stated that when the CDD Rules were issued in 2001,

the requirement to continue relationships with clients based on valid identification caused the freezing of a wide number of bank accounts, some of which are still frozen today.

Politically exposed persons (Recommendation 6)

Determining a PEP

412. For the banking sector and licensed money exchange businesses, Article 4.5.4 of the RBME define PEPs as "individuals who are or have been entrusted with prominent public functions, for example heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state owner corporations and important political party officials." It adds that business relationships with family members or close associates of PEPs involve a reputational risk similar with those of PEPs themselves. In addition, the Article states the requirement to put in place appropriate risk management systems to determine whether a potential customer, existing customer or the beneficial owner is a politically exposed person.

413. As to the insurance sector, Article 1 AML/CFT of the RIC defined "political personality" as "any person who occupies or had recently occupied, or is aiming at or is a candidate to occupy a high civil position at the government, or military position or any position at a state company, etc." The definition extends to all direct members of the person's family and anyone working as a consultant or agent for that person. "Recently" is not defined, nor does it cover persons in a non-public position. Article 61 classifies political persons as high-risk customers. Article 64 states that companies should develop risks management systems to identify PEPs.

414. Regarding the capital market sector, Article 2 of the AML/CFT Rules defines PEP as "any individual who occupies, has recently occupied, is actively seeking or is being considered for, a senior civil position in a government of a country, state or municipality of any department including the military, any agency, or government owned company." "Recently" is not defined, nor does it cover persons in a non-public position. The definition also extends to related individuals and close associates of a PEP. Article 10 provides that risk management systems should be in place to identify whether a client or potential client, or a beneficial owner, is a PEP.

415. With respect to the financing sector, Article 6 of the AML/CFT Instructions requires that companies establish measures to identify high-risk customers. Article 3 Section 2.3 (c) lists Politically Exposed Persons as high-risk customers.

416. Financing companies are not explicitly required, in addition to performing the CDD measures, to put in place appropriate risk management systems to determine whether a potential customer, a customer or the beneficial owner is a politically exposed person.

417. In general, banks appeared to have proper definitions and risk management systems to determine whether a client is a PEP or not, especially that many seem to rely on commercial database services for this purpose. However, the other types of financial institutions (notably some insurance companies and money exchange businesses) did not seem to be able to detect all possible PEPs among their customers or had incomplete definition on which categories of clients could be designated as PEPs.

Business relations approval

418. Regulatory provisions for financial institutions require senior management approval at the beginning of a business relationship with a PEP (Article 4.5.4 of the RBME, Article 64 (b) of the RIC, Article 10 of the RAP, Article 3 Section 2.3 of the IFC).

419. Article 4.5.4 (5) of the RBME explicitly provides that where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a PEP, senior management approval to continue the business relationship is to be obtained.

420. Concerning the capital market sector, Article 10 (2) of the RAP requires senior management approval for the opening or continued operation of an account for a PEP Article 64 (c) of the RIC requires approval of the company's higher management where an existing company customer becomes a PEP. Article 2 Section 6 of the IFC requires obtaining the approval of higher management when establishing or continuing business relations with high risk customers (including PEPs as per section 3-2 of article 3 (c)). However, for RAP, RIC & IFC, senior management approval has not been required to continue the business relationship with a customer whereas the beneficial owner is subsequently found to be, or subsequently becomes a PEP.

421. There was a positive impression on the involvement of senior management for approving the establishment of such business relationships generally, however, it appeared that some PEP customers in some financial institutions (some banks for instance) are conducting business while their relationship with the institution had not been validated by senior management at any stage. Moreover, for already existing customers that have been found to be PEPs at a later stage, the assessment team established that senior management involvement was not systematically there. The authorities indicated that supervisory follow-up action has been taken to address those situations.

Establishing the source of wealth and source of funds

422. Concerning banks and money exchange businesses, Article 4.5.4 (2) of the RBME states that the identification of PEPs should include the existing and new customers as well as beneficial owners. Article 4.5.4 (4) requires the determination of "the source of funds, source of wealth and beneficial owners for all PEPs".

423. Concerning insurance companies, Article 64 (d) of the RIC requires taking "logical measures to determine the source of income as well as the source of funds". The term "logical" may not be indicative enough of the extent of efforts expected from an insurance company while seeking such information. Article 20 (h) provides that the funds source and the income of the customer (therefore includes PEPs) are components of the risk document. These texts do not cover the inquiry on source of wealth, neither stipulates that such measures should be applicable to cases whereas beneficial owners of a business relationship are identified as PEPs.

424. Concerning the capital market sector, Article 10 (3) of the RAP expresses adequately the requirements mentioned above.

425. As for the financing sector, Section (Second) Paragraph 6 (8) of the AML/CFT instructions requires to put in place basic indicators to contribute to identify high-risk persons and operations according to the customer's country of origin, sources of revenue and the quality of operations (etc).

426. Insurance companies are not required to determine the source of wealth and source of funds for beneficial owners identified as PEPs, as well as source of wealth for customers identified as PEPs. Financing companies are not explicitly required to determine source of wealth and source of funds for clients or beneficial owners identified as PEPs. Some financial institutions expressed difficulties about dealing with customers when it comes to obtaining info/justifications on the source of funds and even more about source of wealth. The assessment team established that many financial institutions could/did not take reasonable measures to establish the source of wealth (and sometimes the source of funds or even copy of identification documents) for a client or a beneficial owner identified as PEP.

Enhanced ongoing monitoring

427. Concerning banks and money exchange businesses, insurance companies and authorized persons, Article 4.5.4 (7) of the AML/CFT Rules, Article 64 (e) of the RIC and Article 10 (1) of the RAP respectively express the requirement to conduct enhanced ongoing monitoring for PEP accounts.

428. For the financing sector, Article 6.8 of the IFC requires conducting enhanced monitoring on all high-risk customer relationships, while Article 3 Section 2.3 (c) provides that PEPs are considered high-risk customers.

429. It appeared that the annual review of PEP accounts to approve continuation of relationship as outlined by the AML/CFT policy is not being conducted at some financial institutions. It is difficult to imagine a proper enhanced monitoring when information about the source of wealth and source of funds are not available.

Additional elements

430. The definition of PEPs applies to both domestic and foreign PEPs and all the rules outlined above therefore also extend to domestic PEPs. The Merida Convention has been signed by Saudi Arabia and the ratification process is underway.

Correspondent banking (Recommendation 7)

Identification of respondent institutions

431. Article 4.5.10 of the AML/CFT Rules defines "correspondent banking relationship" and requires taking strict measures to prevent the use of correspondent accounts for money laundering and terrorist financing. Prior to opening any correspondent account, banks are required to fully understand and document full details of the respondent bank's management and nature of business. Banks should also determine from publicly available information (*e.g.*, internet) whether the correspondent bank has been subject to any ML or TF investigations or regulatory action. In addition, banks should obtain, for all correspondent relationships, a certification that the bank is under jurisdiction of a central bank or a similar monitory authority. Such certification should contain other information on the location, major business activities, and management as well as other AML/CTF compliance data.

432. Article 300.2.5 of the CDD Rules requires that banks should ensure through publicly available information and research (the media and others) that the correspondent banks planned to deal with, or to continue to deal with has never been subject to investigation on money laundering or terrorist financing cases, or raising issues in this regard or subject to regulatory investigation.

433. In practice, it appeared that most banks set proper policies and procedures in order to address the identification process of banks requesting new correspondent relationships. The implementation of these measures seems adequate. However, some financial institutions seemed to have not yet applied such measures with respect to already established correspondent relationships.

Assess respondent's AML/CFT controls

434. Article 4.5.10 of the RBME provides that banks should ensure that their correspondents are governed by and committed to AML/CTF and KYC policies and procedures. Banks should also ensure the existence of procedures in place for reporting suspicious transactions and any other pertinent information that can reassure the bank that sufficient focus is being directed to combating money laundering and terrorist financing.

435. Article 300.2.5 of the CDD Rules requires local banks to obtain from correspondent banks a questionnaire of anti-money laundering and terrorism finance prevention measures, ML and TF prevention measures in relation to new banks relationships and existing relationships, and access the correspondent bank internal AML/CFT controls and ensure they are sufficient and effective.

436. Authorities reported that in April 2004, all the banks were asked to freeze their correspondent and respondent relationships which were not in compliance with the requirements of the AML/CFT and CDD rules. This was reviewed by SAMA inspection teams with follow-up where necessary to ensure compliance. Further, written approval from SAMA to establish or continue a correspondent relationship must be obtained in which SAMA assures compliance with applicable rules.

437. However, the assessment team found that practice is varied among existing banks: as some seemed to conduct outstanding due diligence towards potential respondent banks (KYB, regulatory framework, internal policies, detailed assessment questionnaire, supporting documents, oversight of supervision), others seemed to maintain very poor respondent banks' files, suggesting that existing relationships have not been subject to adequate review for implementing required due diligence.

Senior management approval

438. According to CDD Rules and AML/CFT Rules, senior management approval is required for the opening of correspondent bank accounts and after completing and satisfying customer due diligence on all correspondent bank accounts.

439. There were no grounds to perceive that correspondent relationships could be established without involvement of senior management notably in the approval phase.

Respective AML/CFT responsibilities

440. Banks are not required to ensure that AML/CFT responsibilities falling on each institution are documented. However, it appears that many financial institutions seek or reach understandings (in writing)

with their counterparts in correspondent banking relationships on the respective AML/CFT measures to be implemented and procedures/sanctions to be taking place whenever the respondent fails to comply with such agreements.

Payable through accounts

441. Both Article 4.5.10 of the RBME and Article 300.2.5 of the CDD Rules prohibit payable-through accounts. Article 4.5.10 of the RBME stipulates that third parties are prohibited from operating correspondent bank accounts and that correspondent accounts for shell banks may not be opened. Pursuant to Article 300-2-5 of the CDD Rules, banks are required to ensure that respondent bank accounts are used only for correspondent transactions and are not used or treated as current accounts. Correspondent accounts may not be used by third parties to conduct activities for their own account.

442. The assessment team has not come across a case where financial institutions maintain PTA accounts through their correspondent relationships.

443. No reference has been made for the evaluation team to any types of institutions other than banks in SA that may engage in correspondent relationships or other similar relationships[71]. No reference has been made either to provisions prohibiting such types of arrangements. However, the authorities have indicated that non-bank financial institutions in Saudi Arabia do not engage in correspondent banking.

444. It is worth noting that the Saudi regulatory provisions do not distinguish between the concepts of "correspondent institutions" (offering correspondent services) and "respondent institutions" (requesting/receiving such services). All provisions broadly set forth rules for dealing with "correspondent" institutions (instead of "respondent" institutions). This means that institutions operating in KSA (mostly respondent) are required to apply measures based on FATF Recommendation 7 that are expected from and executed by correspondent institutions (only) against their respondents. The authorities may wish to detail the correspondent relationships obligations to explain which of them should be carried out by which institutions (party in a correspondent relationship).

New technologies and NFTF business relationships (Recommendation 8)

Managing risks of new technologies

445. Article 6.2 (a) of the AML IRs provides that covered entities have to put in place internal controls and procedures to prevent the misuse of technological developments in money laundering and terrorism financing schemes.

446. Furthermore, Article 5.1.5 of the RBME prohibits banks and money exchange businesses from offering banking products and services through electronic payment methods if a customer does not maintain a bank account and thus has been subject to the full range of CDD measures. This includes online banking, banking payment, phone banking, automated teller machines, or any other new electronic payment method.

[71] For example, those established for securities transactions or funds transfers, whether for the cross-border financial institution as principal or for its customers.

447. For the capital market sector, Article 16 of the RAP requires that authorized persons consider ML/FT threats arising from the misuse of new or developing technologies, and formulate its policies, procedures and controls to prevent such threats.

448. For the financing sector, Article 6 of the AML/CFT Instructions provides that companies shall establish policies and take necessary measures to prevent the misuse of modern communication technologies and technical means for ML/FT purposes.

449. There is no bank-independent electronic banking system in Saudi Arabia. Each bank offers its own proprietary system in both the retail and corporate sectors. Internet banking is also becoming increasingly commonplace among retail users and smaller companies. Electronic banking guidelines issued by SAMA in 2001 do not address AML/CFT risks. Authorities stated that financial institutions use systems to track the operations conducted through electronic channels and to identify and analyze unusual transactions. Every bank also has defined its own set of policies and procedures that govern the electronic channels and prevent their misuse. Supervisory authorities examine these electronic channels in the course of their examinations.

450. Besides the user protection procedures (password, private number, transaction limits), there was no information pertaining to the extent/validity/effectiveness of measures undertaken by financial institutions to prevent the misuse of new technologies for ML and TF purposes; however, the quality of due diligence applied to customers granted online banking / electronic transfer services for instance does not seem, at most of the financial institutions, to be enhanced when compared to diligence applied with respect to other customers. On the other hand, quality and frequency of banking supervision do not appear to guarantee an adequate implementation of these measures. It is believed that sanctions are missing as well in this respect, which reinforces the belief that the effectiveness is questionable.

Managing risks of NFTF business relationships

451. Article 6.2 (a) of the AML IRs requires covered entities to put in place written and effective controls to manage the risks associated with non-face to face transactions.

452. In addition, for the banking sector and licensed money exchange businesses, Article 4.3.2 (2) of the AML/CFT Rules provides that accounts or relationships with customers may not be established without a face-to-face meeting and without subjecting all accounts to interview and identity verification procedures. In addition, for the banking sector, Article 100.8 of the CDD Rules provides that no account should be opened for new customers without interview*ing them, including mail, internet, and telepho*ne applicants, payroll accounts of government, private sectors and other sectors' employees, except in cases of legal powers of attorney authorizing the opening of bank accounts and containing the personal data of both parties. Phone and online banking may only be provided to existing customers. Where the customer is unable to visit the bank, the bank may delegate two or more of its staff to meet the customer on site and obtain relevant information and documents as required in these rules. Furthermore, as banks are required to apply the CDD measures and identify the client whenever a transaction is carried out, the risk posed by non-face-to-face transactions is adequately addressed for the banking sector.

453. For the insurance sector, Article 26 of the RIC states that companies should assure that transactions of protection and savings insurance are conducted face to face. SAMA does not grant authorization, according to the RIC, for online sale of protection and savings insurance policies.

454. For the capital market sector, Article 7 (4) of the AML/CFT Rules requires that no client may be accepted or account opened for a client without a face-to-face meeting with the client.

455. For the financing sector, Article 3 (Para. 2.4) of the AML/CFT Instructions prohibits companies from dealing with new customers unless a face to face meeting with the client has been held. The provision allows for a few exceptions from the general prohibition, in which case Article 3 (Para 2.5) requires the application of policies, measures and internal controls to deal with the risk associated with such customers and transactions. The provision extends to applications through mail, internet, and phone. Article 3 (Para. 2.4) further provides that services may not be provided through technical means, such as the internet, unless a business relationship has been established based on authenticated documents and the identity of the client has been obtained in verified through a face to face meeting.

456. There was no additional information pertaining to the extent/ validity/ effectiveness of measures undertaken by financial institutions to prevent the misuse of non face-to-face business relationships for ML and TF purposes. The authorities noted that users of online banking services are originally normal customers of the bank. It is not possible for customers to establish a business relationship directly through online channels, but instead establishing the business relationship must take place in a face to face meeting. Therefore, customers must meet the CDD requirements in order to receive electronic services. However the quality of due diligence applied to customers benefiting from such services does not seem, at most of the financial institutions, to be enhanced (during the establishment of the relationship and afterwards in the monitoring phase) when compared to diligence applied with respect to other customers. On the other hand, quality and frequency of banking supervision does not appear to guarantee an adequate implementation of these measures. It is believed that sanctions are missing as well in this respect, which reinforces the belief that the effectiveness is questionable.

3.2.2 Recommendations and Comments

Customer due diligence including enhanced and reduced measures (Recommendation 5)

- CDD requirements for insurance companies and authorized persons were recently circulated (at the time of the Onsite visit) which suggests that the effectiveness could not be properly addressed.

- There should be a guarantee in a primary or secondary legislation that in case numbered accounts are opened, financial institutions are required to maintain them in such a way that full compliance with the FATF Recommendations can be achieved.

- Ongoing due diligence requirement should be provided for explicitly by primary or secondary legislation.

- Insurance companies should be explicitly required to terminate the business relationship and consider making a suspicious transaction report when required CDD measures cannot be applied to existing customers and in cases when the institution has doubts about the veracity or adequacy of previously obtained customer identification data.

- Banks, money exchange businesses, insurance companies and authorized persons should be explicitly required to apply CDD requirements to existing customers on the basis of materiality and risk.

- Performing CDD measures based on doubts about the veracity of previously obtained information is possibly not being implemented at most financial institutions.

- The identification and verification process is insufficiently implemented at some financial institutions. With money exchange businesses, it appeared possible to conduct business transactions simply against submitting a copy of identity.

- Many financial institutions do not obtain information concerning the directors of legal entities. There was evidence that proofs of incorporation of these entities have not been retained in several instances.

- Financial institutions demonstrated a flawed understanding of the requirement to obtain and verify beneficial ownership. Some institutions did not seem to inquire the client about it. When some financial institution proved to be verifying ownership, it stated to perform it "up to the third level", and in other instances "up to first level"; as for understanding the control structure of legal entities, it seemed that institutions knew little about it. It was frequently noted that adopted KYC forms do not contain fields by which such information can be retained; institutions appeared to be satisfied with reliance on received copies of official documents (mainly commercial registration and Articles of Association) to collect the information required above (which does not makes it possible for shareholders of bearer shares companies).

- The scrutiny of transactions for consistency with due diligence data is likely not being conducted by non-bank financial institutions. The reported reliance of many banks on specialized transactions monitoring software for such scrutiny does not include matching with KYC data.

- For banks and money exchangers, the transactions monitoring threshold parameter of SAR 60,000 means that most customer relationships may stay below the radar, which would exclude the requirement to undertake CDD measures when there is a suspicion of money laundering or terrorist financing below this threshold. The quality and frequency of updating of CDD data appeared to be questionable concerning many financial institutions.

- Due diligence measures are not satisfactorily applied by many financial institutions (limited perception of who could be a high-risk customer, no classification of customers according to risk). Enhanced diligence is not satisfactorily applied in some sectors.

- At some financial institutions, some customer files do not contain key documents pertaining to the identification process: It is not clear whether this situation reflects a failure in performing timely identification and/or a failure in satisfying the requirement to refuse or terminate relationship and report accordingly

- The extent (mainly for official documents) and quality of updating was not proper at some financial institutions. The updating process has often not been completed. CDD information for existing business relationships at many non-bank financial institutions is not up-to-date.

Politically exposed persons (Recommendation 6)

- Definition of PEPs only covers current and recent PEPs, with no definition of "recent".

- Financing companies should be explicitly required, in addition to performing the CDD measures, to put in place appropriate risk management systems to determine whether a potential customer, a customer or the beneficial owner is a politically exposed person.

- Insurance companies, Authorized persons and Financing companies should be explicitly required to seek senior management approval for continuing the relationship in cases where a beneficial owner is subsequently found to be, or subsequently becomes a PEP.

- Insurance companies should be required to determine the source of wealth and source of funds for beneficial owners identified as PEPs, as well as source of wealth for customers identified as PEPs.

- Financing companies should be explicitly required to determine source of wealth and source of funds for clients or beneficial owners identified as PEPs.

Correspondent banking (Recommendation 7)

- Banks should be required to ensure that AML/CFT responsibilities falling on each institution are documented.

- Banks should apply adequate due diligence towards correspondent relationships, notably the ones already established.

New technologies and NFTF business relationships (Recommendation 8)

- Authorities should make sure that adequate attention is paid by financial institutions regarding AML/CFT-related risks that may be posed by new technologies.

3.2.3 Compliance with Recommendations 5 to 8

	Rating	Summary of factors underlying rating
R.5	**PC**	• CDD requirements for insurance companies and authorized persons were recently circulated (at the time of the Onsite visit) which suggests that the effectiveness could not be properly addressed. • No primary or secondary legislation guaranteeing numbered accounts are maintained in such a way that full compliance with the FATF Recommendations can be fully achieved. • Ongoing due diligence requirement was not provided explicitly by primary or secondary legislation. • Insurance companies are not explicitly required to terminate the business relationship and consider making a suspicious transaction report in case required CDD measures could not be applied to existing customers and to cases whereby the institution has doubts about the veracity or adequacy of previously obtained customer identification data. • Banks, money exchange businesses, insurance companies and authorized persons are not explicitly required to apply CDD requirements to existing customers on the basis of materiality and risk. *Effectiveness* • Performing CDD measures based on doubts about the veracity of previously obtained information is possibly not being implemented at most financial institutions. • The identification and verification process is insufficiently implemented at some financial institutions. With money exchange businesses, it appeared possible to conduct business transactions simply against submitting a copy of identity. • Many financial institutions do not obtain information concerning the directors of legal entities. There was evidence that proofs of incorporation of these entities have not

	Rating	Summary of factors underlying rating
		been retained in several instances. Financial institutions demonstrated a flawed understanding of the requirement to obtain and verify beneficial ownership. Some institutions did not seem to inquire the client about it. When some financial institution proved to be verifying ownership, it stated to perform it "up to the third level", and in other instances "up to first level"; as for understanding the control structure of legal entities, it seemed that institutions knew little about it. It was frequently noted that adopted KYC forms do not contain fields by which such information can be retained; institutions appeared to be satisfied with reliance on received copies of official documents (mainly commercial registration and Articles of Association) to collect the information required above (which does not makes it possible for shareholders of bearer shares companies). • The scrutiny of transactions for consistency with due diligence data is likely not being conducted by non-bank financial institutions. The reported reliance of many banks on specialized transactions monitoring software for such scrutiny does not include matching with KYC data. • For banks and money exchangers, the transactions monitoring threshold parameter of SAR 60,000 means that most customer relationships may stay below the radar, which would exclude the requirement to undertake CDD measures when there is a suspicion of money laundering or terrorist financing below this threshold. The quality and frequency of updating of CDD data appeared to be questionable concerning many financial institutions. • Due diligence measures are not satisfactorily applied by many financial institutions (limited perception of who could be a high-risk customer, no classification of customers according to risk). Enhanced diligence is not satisfactorily applied in some sectors. • At some financial institutions, some customer files do not contain key documents pertaining to the identification process: It is not clear whether this situation reflects a failure in performing timely identification and/or a failure in satisfying the requirement to refuse or terminate relationship and report accordingly. • The extent (mainly for official documents) and quality of updating was not proper at some financial institutions. The updating process has often not been completed. CDD information for existing business relationships at many non-bank financial institutions is not up-to-date.
R.6	**PC**	• Definition of PEPs only covers current and recent PEPs, with no definition of "recent". • Financing companies are not explicitly required, in addition to performing the CDD measures, to put in place appropriate risk management systems to determine whether a potential customer, a customer or the beneficial owner is a politically exposed person. • Insurance companies, authorized persons and financing companies are not explicitly required to seek senior management approval for continuing the relationship in cases where a beneficial owner is subsequently found to be, or subsequently becomes a PEP. • Insurance companies are not required to determine the source of wealth and source of funds for beneficial owners identified as PEPs, as well as source of wealth for customers identified as PEPs. • Financing companies are not explicitly required to determine source of wealth and source of funds for clients or beneficial owners identified as PEPs. • Inadequate implementation of several components of the due diligence requirements towards PEPs, notably with respect to the risk management systems in place to spot PEPs at insurance companies and money exchange businesses, senior management approval for continuation of business relationship, verification of source of wealth and enhanced ongoing monitoring.
R.7	**LC**	• Some banks did not seem to be implementing adequate due diligence towards correspondent relationships, notably the ones already established.
R.8	**LC**	• Measures undertaken by financial institutions to prevent the misuse of new

	Rating	Summary of factors underlying rating
		technologies and non face-to-face business relationships for ML and TF purposes are not effectively implemented.

3.3 Third parties and introduced business (R.9)

3.3.1 Description and Analysis

Obtaining data on essential CDD elements

457. Concerning banks, Article 4.5.9 of the RBME states that "it is customary for banks to rely on procedures undertaken by other banks or introducers… In doing so, banks risk placing excessive reliance on the due diligence procedures that they expect the introducers to have performed". Under subparagraph 1.3, the Article stipulates that for introduced business, banks "should obtain and carefully review all relevant identification data and other documentation pertaining to the customer and the introducer". On the other hand, Article 2.4 of the Rules on outsourcing issued by SAMA in July 2008 stipulates that ''banks are not allowed outsourcing any functions relating to the transmission, processing and or retention of Customer Data to a Service Provider, with the exception of functions such as credit card processing and remittances utilizing international payment systems where banks are required to seek SAMA's prior no objection".

458. For the insurance sector, Article 29 (e) of the RIC provides that companies relying on third parties to perform CDD measures must receive copies of documents and information relevant to customer due diligence measures of the third party.

459. For the capital market sector, Article 14 of the AML/CFT Rules provides that only commercial banks or financial institutions engaged in securities activities may act as introducers for authorized persons. In any case, authorized persons must obtain copies of the CDD documentation and information in line with Article 8 of the Rules.

460. The Rules do not bind financial institutions by a timeframe in order to obtain immediately necessary CDD information from third parties. While Article 29 of RIC and 14 (5b) of AML/CFT rules for the capital market sector stipulate that the company must ensure that third party will ''make all documents and data available once asked without any delay'', criterion 9.1 expects the company to immediately obtain (or ask) these documents or information. Some financial institutions (mainly some insurance companies) did not seem to obtain necessary CDD information from the brokers they deal with since "some of them do not know what is needed in terms of AML/CFT". However, these institutions stated that they conduct anew their own identification measures.

Responsiveness of the Third Party

461. Concerning banks, Article 4.5.9 of the RBME provides that an agreement must be established with the introducer that it will be permitted to verify due diligence undertaken by the introducer at any stage. Banks should not rely on introducers that are unwilling to share copies of due diligence documentation.

462. For the insurance sector, Article 28 (e) of the RIC provides that insurance businesses have to take measures to ensure that documents and data relating to customer CDD are made available by the third party when requested and without any delay.

463. For the capital market sector, Article 14 of the AML/CFT Rules provides that the authorized person must take steps to satisfy itself that copies of relevant documents relating to CDD requirements will be made available from the third party without delay, such as establishing their respective responsibilities in writing, including reaching agreement with the third party that copies of other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay and the authorized person will be able to verify the CDD undertaken by the third party at any stage.

464. Some financial institutions (mainly some insurance companies) seemed to be aware that some/most of their brokers do not conduct required CDD. In addition, third parties dealing with some insurance companies did not seem to be keeping necessary/all documentation and information pertaining to CDD requirements.

Supervision of Third Party & Ability to Conduct CDD

465. Concerning banks, Article 4.5.9 of the RBME provide that there should not be reliance on introducers with weaker standards than those governing the banks' own CDD procedures. The banks must further satisfy themselves that the CDD measures applied by the third party are reliable.

466. For the capital market sector, Article 14 of the RAP provides that the reliance on a third party should be coupled with ensuring that this third party is regulated and supervised by a competent authority, and has measures in place to comply with CDD and record keeping requirements in line with these rules and the FATF Recommendations. Prior to reliance, authorized persons must satisfy themselves that the CDD measures of the third party are as rigorous as those that would have been applied by the authorized person itself. Furthermore, the authorized person must establish clear procedures to determine whether the third party possesses an acceptable level of reliability.

467. For the insurance sector, Article 29 (e) of the RIC requires that the insurance company to ensure that the third party is licensed, supervised and applying CDD procedures as well as record keeping procedures in line with the FATF Recommendations.

468. Banks are not required to satisfy themselves that the third parties are regulated and supervised. The sample of insurance companies met showed that their satisfaction with respect to dealing with third parties comes from the knowledge that this third party is supervised. The sample of authorized persons showed that this satisfaction seemed to be reached with the knowledge that the third party is supervised and regulated (this knowledge is provided through a questionnaire to be filled out by the third party).

Country of Third Party

469. According to Article 4.5.9 of the RBME, an introducer can be another bank or a person or an entity or a professional intermediary. On the other hand, a referred business means a relationship referred by one branch to another, within one bank or externally from other banks inside or outside the country. On the other hand, non resident customers can have access to banking services in the KSA according to a detailed set of provisions listed within sections 200, 300 and 400 of the CDD Rules. Articles 300.2.1.2 (in

a, b, &c) allows non-resident GCC legal persons to open accounts for trading in securities of companies listed in the KSA through an intermediary or an introducer. Many other Articles (400.1 (2) for instance) exclude this possibility since they require that necessary documents be presented through a correspondent bank or even face-to-face. Whereas the Articles do not forbid the reliance on intermediaries to perform some of the elements of the CDD process or to introduce business, and despite that other validation conditions may be required (such as SAMA approval, authentication by a Saudi embassy…), banks are not prohibited from relying on a third party based in a country which is not adequately applying the FATF Recommendations. However, as indicated above, the opportunity for non-resident legal persons to have financial services in the KSA is limited to GCC countries, which limits the potential ML/TF risks to a much smaller group of countries.

470. Article 29 (c) of the RIC provides that companies may count on third parties to perform the CDD process only if the third party's headquarters are located in any GCC country or in another country which applied appropriately the FATF Recommendations and if the customer is a foreign resident and has a clear reason for the insurance relation in SA. Furthermore, pursuant to Article 28 (g), it is not allowed to rely on third parties in a high-risk country, such as countries which have no or insufficient AML/CFT finance regulations. Article 66 (b) requires insurance companies to attach special attention to reports evaluating the level of commitment of the concerned country to FATF's Recommendations, developed by FATF, FSRBs, IMF, and World Bank when evaluating a country's application of FATF's AML & CFT standards.

471. For the capital market sector, Article 14 of the AML/CFT Rules provides that authorized persons may not rely on third parties based in countries considered as high risk, such as countries that have no or inadequate AML/CFT systems.

472. Whereas the introduced/referred business does not involve a correspondent bank, banks are allowed in limited circumstances to rely on a third party (from GCC countries), which limits the potential ML/TF risks to a much smaller group of countries. . It seemed that financial institutions mostly deal with third parties based in GCC countries when it comes to cross-border introduced business.

Ultimate responsibility for CDD

473. Article 4.5.9 of the RBME, Article 29 (b) of the RIC and Article 14 of the RAP expressly state that the ultimate responsibility for customer identification and verification remains at all times with the financial institution relying on the third party.

3.3.2 Recommendations and Comments

- The rules should bind financial institutions to obtain immediately necessary CDD information from third parties when relying on them to perform some of the elements of the CDD process or to introduce business.
- Banks should be required to satisfy themselves that the third parties are regulated and supervised.

3.3.3 Compliance with Recommendation 9

	Rating	Summary of factors underlying rating
R.9	**LC**	*Regulatory* • The rules do not bind financial institutions by a time frame in order to obtain

	Rating	Summary of factors underlying rating
		immediately necessary CDD information from third parties. • Banks are not required to satisfy themselves that the third parties are regulated and supervised. *Effectiveness:* • Non-bank financial institutions (mainly insurance companies) did not seem to apply adequate diligence towards relied on third parties.

3.4 Financial institution secrecy or confidentiality (R.4)

3.4.1 Description and Analysis

474. Article 8 of the AMLS provides that as an exception to confidentiality provisions that normally apply (under Article 19 of the BCL, Articles 17 and 45(c) of the CML, Article 29 of the APR, and Article 12 of the Insurance Law), financial and non-financial institutions must provide the judicial or competent authority with documents, records, and information where requested. It is explicitly stated that entities may not use the principle of confidentiality of accounts, identity of clients, or other recorded information pursuant to any other law as a pretext for withholding information. The law specifies that requests for information by the FIU or other judicial or competent authorities must be requested through the Anti-Money Laundering Unit in the relevant supervisory body (SAMA, MOCI, CMA or MOJ). Article 13 also states that competent authorities must observe the confidentiality of such shared information except as necessary in the use of investigations and legal proceedings related to a violation of the AMLS.

475. Supervisory authorities are also granted sufficient access to information in the fulfillment of their supervisory duties. SAMA (Article 11 of the Insurance Law, Article 17 of the Banking Control Law, and Article 9 of the Decision on Money Exchange Businesses) and the CMA (Article 18 of the CML) are explicitly authorized to access all information required to perform their supervisory functions.

476. Regarding the sharing of information with foreign competent authorities (described as the FIU or its functional equivalent), Article 22 of the AMLS allows for this provided that the authorities are in countries with which Saudi Arabia is a party to a legal agreement or convention, or on the basis of reciprocity. It also states that this can be done only "provided that this shall not prejudice the provisions and practices related to the confidentiality of financial and non-financial institutions." The assessment team found no reasons to believe that such provision has hindered information sharing in practice.

477. While the AMLS sufficiently provides exceptions to confidentiality provisions to facilitate access to information by competent authorities, both foreign and domestic, it does not address the sharing of information between entities or institutions. Article 2.6 of the RBME supports cooperation among banks and money exchange businesses in the context of fulfillment of their AML/CFT obligations, specifying that exchange of information must be conducted through SAMA in order to "maintain controlled flow of confidential information." Institutions are further instructed that in such exchange they "must strictly follow the legal and regulatory procedures that aim to protect customer confidentiality and banking secrecy" (Article 2.6.2).

478. In the case where a bank or money exchange business receives a request for the sharing of information from a foreign institution, Article 2.6.3 requires the domestic institution to obtain approval

from SAMA before sharing information (except for commercial enquiries)[72]. The authorities also provided statistics to show that there have been several such requests received and approved by SAMA. The assessment team could however not establish that provision is not an impediment to the implementation of this recommendation.

3.4.2 Recommendations and Comments

479. The evaluation team found no evidence to suggest that access to information in the context of application of the FATF Recommendation is inhibited by confidentiality laws. Nevertheless, it is recommended that a legal basis regarding exceptions to confidentiality provisions in the sharing of information between institutions, domestic and foreign, be explicitly established.

3.4.3 Compliance with Recommendation 4

	Rating	Summary of factors underlying rating
R.4	**LC**	• Limitations on the sharing of information between domestic and foreign banks in the implementation of R.7 and SR.VII • Exceptions to confidentiality provisions in the sharing of information between entities and institutions, foreign and domestic, not explicit

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

3.5.1 Description and Analysis

Record keeping (Recommendation 10)

Maintaining records of transactions

480. Article 5 of the AMLS requires covered entities to keep, for a period of not less than ten years from the date of the completion of a transaction or the closing of an account, all records and documents that show the financial dealings, commercial and cash transactions, whether domestic or foreign and, to retain account files, business correspondence and copies of personal identification documents.

481. Article 5.2 of the AML IRs provides that records shall contain all transaction details necessary for the competent authorities to trace and reconstruct each transaction and for the covered entities to answer all the competent authorities' inquiries. Article 5.3 further provides that in cases where covered entities are requested by authorities to maintain any records or documents, including transaction records, for longer than the regular retention period of 10 years, it must extend the retention period until the end of the period specified in the request.

482. In addition, for the banking sector and money exchange businesses, Article 4.10 of the RBME requires that all records kept have to be adequate enough to enable for the reconstruction of transactions and offer a complete audit trail of all financial transactions, in particular cash transactions and funds transfers.

[72] SAMA circular M A T/97 of 13/4/1424.

483. For the capital market sector, Article 19 of the AML/CFT Rules requires that records of all client identification data and other documents and information obtained as part of the CDD process, account files and business correspondence as well as transaction records must be kept. Authorized persons are expressly required to maintain sufficient records to permit the reconstruction of individual transactions, including the amounts and types of currencies involved so as to provide, if necessary, evidence for prosecution of criminal activity.

484. As to the insurance sector, Article 59 of the RIC provides that companies should keep sufficient records allowing the restructuring of any insurance transaction, so as to provide evidence for the prosecution of criminal activity if necessary.

485. For the financing sector, Article 4.2 of the AML/CFT Instructions provides that companies shall keep records that enable stakeholders to follow up and reconstitute operations.

Maintaining records of identification data

486. Article 5 of the AMLS requires that covered entities keep for at least ten years from the date of closing an account all account files, business correspondence and personal identification documents of the client.

487. Article 5.1 of the AML Regulation clarifies that the record keeping requirement extends to copies of the personal identification documents of the clients and of any document pertaining to transactions conducted. Article 5.3 further provides that in cases where covered entities are requested by the authorities to maintain any records or documents for longer than the regular retention period of 10 years, it must extend the retention period until the end of the period specified in the request.

Responsiveness to competent authorities

488. Article 8-2 of the AML IRs requires that all documents, records, and information be submitted to the competent authorities promptly upon request. No clear timeframe is given in this regard. It is noteworthy that requests for information by the judicial authorities, BIP, or FIU have to be channeled through supervisory authorities (SAMA, MOCI, CMA, and MOJ). Interviewed authorities stated that pursuant to an agreement between the FIU and SAMA (circulated to all banks), any request coming from SAMA has to be answered by the banks within 10 days. However, the team was not able to access such an agreement.

489. The following table illustrates the number of requests received by SAMA from some related authorities, in addition to the percentage of what have been executed of these requests as follows:

Number of inquiry requests received by SAMA from FIU during the period 01.01.2006 - 30.09.2008.		
Year	**Number of Requests**	**Executed Requests**
2006	390	100%
2007	514	100%
2008	402	100%

Number of inquiry requests received by SAMA from the Bureau of Investigation and Public Prosecution during the period 01.01.2006 - 30.09.2008		
Year	**Number of Requests**	**Executed Requests**
2006	54	100%
2007	69	100%
2008	44	100%

Number of inquiry requests received by SAMA from the General Department of Criminal Investigations (Ministry of Interior) during the period 01.01.2006 - 30.09.2008.		
Year	**Number of Requests**	**Executed Requests**
2006	567	100%
2007	1990	100%
2008	1998	100%

Wire transfers (Special Recommendation VII)

490. Domestic or cross-border transfer services may only be carried out through a bank account or a transfer membership (with bank remittance centers or a category A money exchange business). Under Article 5.1.2, AML/CFT RBME, wire transfers are defined as "any transaction carried out on behalf of an originator (both natural and legal) through a bank or money exchange business by electronic means for the purpose of making an amount of money available to a beneficiary at another bank or money exchange business. The originator and the beneficiary may be the same person/ entity. The following transfers are excluded from the scope of KSA system (in line with the requirements of FATF Special Recommendation VII):

- Transfers carried out using a credit or debit card provided that a unique identifier accompanies the transfer.
- Where both the payer and the payee are payment service providers acting on their own behalf.

491. In addition to the above Article of the RBME, the authorities referred to the CDD Rules and Circular 866 issued by SAMA. Authorities provided as well circular No. 3291//73 issued 16.02.1409 AH (September 1988), stipulating detailed requirements to be applied by banks and money exchange businesses with respect to outgoing/incoming transfers as well as other provisions ruling relations with counterparts. It was observed that the latter circular, in one instance (*i.e.* requirement to register the purpose of the transfer), stipulates tougher requirements than what the other Rules do.

492. Article 1.2.2 of the RBME stipulates that the Account Opening Rules, in addition to consolidating all previous SAMA circulars on the subject, were improved with new requirements to facilitate implementation and conform to the best international banking practices in line with the Basel principles. It is also noteworthy that Circular (No. 5082/ BCI /55) dated 14.05.2002 issuing the CDD Rules states: "these Rules shall be enforced as from this date and are to replace all previous circulars in respect of

opening accounts. These take precedence over all current internal controls and procedures applied by the banks".

Full originator information

493. Article 5 of the AMLS requires covered entities to keep, for a period of not less than ten years from the date of completion of the transaction or closing of the account, all records and documents to show the financial dealings, commercial and cash transactions, whether domestic or foreign and, to retain account files, business correspondence and copies of personal identification documents.

494. Article 5.1.2 of the RBME (on wire transfers) stipulates that conducting KYC/due diligence vis-à-vis the remitter/originator is the responsibility of the remitting bank or money exchange business, whether foreign or local. "Banks and money exchange businesses should always have adequate information about the originator/ remitter". And "to enhance the transparency of wire transfers for effective AML/CTF programs", the following measures should be adopted:

1. For all outgoing cross-border transfers, ensure to include full and accurate originator information (name, address and account number) on the funds transfers and related messages that are sent.
2. For domestic transfers (within Saudi Arabia), ensure the remitter's name and account number is included, which should be recorded and retained in the system of remitting bank or money exchange business for prompt retrieval if requested by competent authorities.

495. Article 5.1.2 (3) further provides that for domestic transfers, the remitter's name and account number has to be included and retained in the bank/ME's system.

496. Article 3 of Circular 866 issued for money exchange businesses requires them to ensure that all the necessary data for the exchange and transfer forms that are used are submitted, and that all the necessary data are completed when used, that are represented in the full name as in the ID of the customer, his address, etc. Article 5 of the circular requires MEs to maintain all the documents and records especially for the bank transaction for at least 10 years.

497. It is noteworthy that requirements related to obtaining and maintaining full originator information for outgoing wire transfers are not restricted by any threshold, *i.e.* all transfers are subject to the same set of obligations regardless of the amounts.

498. It was not possible for the assessment team to confirm that the shortcomings identified in relation to the implementation of CDD obligations would have been resolved in relation to the requirements to obtain and maintain originator information.

Cross-border wire transfers

499. Article 5.1.2 (1) stipulates that full originator information should be included on all funds transfers and related messages that are sent. Such information should also remain with the transfer message in the payment chain.

500. For batched transfers, although it would be sufficient to include the originator's account number or unique identifier on each individual cross-border wire transfer, provided that the batch file contains full originator information that is fully traceable within the recipient country, , the general applicable rules

require full originator information to accompany any, including batched, transfers. Financial institutions stated that the customer address may not be included on all wire transfers.

Domestic wire transfers

501. Article 5.1.2 (3) of the RBME provides that for domestic transfers, the remitter's name and account number have to be included and retained in the system of the remitting bank or money exchange business for prompt retrieval if requested by the competent authorities.

502. There were no grounds to believe that financial institutions do not comply with information transmission rules for domestic wire transfers.

Duties of intermediary and beneficiary institutions and technical limitations

503. As stated above, Article 5.1.2 (1) stipulates that full originator information for all transfers has to accompany each transfer in the payment message at all stages. Article 5.1.2 (2) provides that for incoming transfers above SAR 5000, full originator information must be included, and if not, the transfers must be suspended and the remitting bank should be asked to provide it. If such information is not provided, this should be considered a suspicious transaction and the transfer has to be sent back to the ordering institution. See below for more information on incomplete originator information.

504. Article 5.1.2 (4) of the AML/CFT Rules states that banks and money exchange businesses should "retain all physical records and system records of all funds transfers in accordance with the prevailing record retention periods" (10 years, see section 3.5 on Recommendation 10 of this report).

505. No explicit provisions mandate any measures to be taken by intermediary institutions in case of technical limitations preventing the full originator information from being transmitted during the necessary time to adapt payment systems. However, Article 5.1.2.4 of the RBME requires retaining all physical and system records of all funds transfers in accordance with the prevailing record retention period. While there were no indications available pertaining to the compliance with the information transmitting rules by intermediary institutions, authorities stated that these applied the required measures satisfactorily and that no such technical limitations existed.

Incomplete originator information

506. Pursuant to Article 5.1.2 (2) of the RBME, incoming cross-border transfers above SAR 5000 should be put on hold and the remitting banks be contacted for the missing information in cases where complete originator information is not submitted with the transfer. Failure to obtain the missing information may be considered as a cause for suspicion and should trigger a reassessment of the relationship with the remitting bank.

507. Since wires need to be put on hold or rejected, beneficiary financial institutions are not required to adopt effective risk-based procedures for handling wire transfers that are not accompanied by complete originator information. It is the view of the team that financial institutions would be unable to put incomplete incoming transactions on hold, which would be difficult given the millions of transactions each day (no data confirming the possibility to put transactions on hold were available). These institutions do not seem to report such cases (this would have led to a higher number of STRs to SAFIU than currently is

the case). Moreover, financial institutions do not seem to restrict or terminate banking relationships based on receiving wire transfers lacking originator information from a remitting bank.

Compliance monitoring and sanctions

508. SAMA as the supervisory body for banks and money exchange businesses monitors compliance with all rules and regulations relating to cross-border and domestic wire transfer, most notably the RBME, which address SR.VII-related requirements. Information on the supervisory powers and effectiveness of SAMA is detailed in Section 3.10 of this report.

509. Authorities stated also that the sanctioning powers of SAMA are applied with respect to the obligations under SR VII as contained in Article 5.1.2 of the RBME. Information on the sanctioning powers of SAMA is outlined in Section 3.10 of this report.

510. It appeared that shortcomings identified under Recommendation 17 (sanctions) and 23 (monitoring and supervision) apply equally to the compliance of this Special Recommendation.

Additional elements

511. Article 5.1.2 (1) of the RBME stipulates that full and accurate originator information (name, address and account number) should be included on all outgoing cross-border transfers.

3.5.2 Recommendations and Comments

Wire transfers (Special Recommendation VII)

- Beneficiary financial institutions should be required to adopt effective risk-based procedures for identifying and handling wired transfers that are not accompanied by complete originator information.

3.5.3 Compliance with Recommendation 10 and Special Recommendation VII

	Rating	Summary of factors underlying rating
R.10	**C**	
SR.VII	**PC**	*Regulatory* • Beneficiary financial institutions are not required to adopt effective risk-based procedures for identifying and handling wired transfers that are not accompanied by complete originator information. *Effectiveness* • Customer address is not included on the wire transfer. • In relation to the rules that have been enacted to replace risk based procedures: Banking relationships are not likely to be terminated based on receiving wire transfers lacking originator information from a remitting bank. Reporting accordingly is not likely to be performed either. • The shortcomings identified under Recommendations 17 (sanctions) and 23 (monitoring and supervision) have a negative impact on this Special Recommendation.

Unusual and Suspicious Transactions

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

3.6.1 Description and Analysis

Special attention to complex and unusual transactions (Recommendation 11)

512. The AMLS requires that "financial and non-financial institutions shall establish precautionary and internal monitoring measures to uncover and foil any of the crimes provided for in this Law and comply with the instructions issued by the competent monitoring authorities in this field" (Article 6). Additionally, the AMLS requires financial and non-financial institutions to maintain indicators of suspicion of ML or TF in order to "pay special attention to unusual patterns of transactions that have no apparent or visible economic or lawful purpose" (Article 7.1). The AMLS however otherwise does not refer to transaction monitoring and does not clearly specify a requirement that transaction monitoring be undertaken.

513. Monitoring of transactions is addressed to varying degrees of satisfaction in the rules issued by relevant competent authorities. The RBME (Article 4.6) describes a risk-based approach to the monitoring of customer transactions. In this context, the RBME notes by way of example certain types of transactions or events that indicate "suspicious activities", including unusual patterns that do not have apparent visible economic or lawful purpose. While the RBME does not make explicit the requirement to monitor transactions, this obligation can be implied. The evaluation team found that in practice, institutions consistently accept monitoring of transactions as set out by the RBME to be required.

514. The RBME states that the risk-based monitoring process should apply to all customer transactions. However, it also stipulates a SAR 60,000 (USD 16,000) transaction monitoring threshold parameter for either a single transaction or aggregated transactions over a one month period. Banks and money exchangers, depending on satisfactory customer profiling, can however apply product-related threshold limits that are consistent with the profile of the concerned customer. While one of several parameters banks must consider in monitoring transactions, the presentation of a threshold parameter is problematic in that banks have a tendency to place an emphasis on threshold monitoring as an acceptable approach to meeting their monitoring obligation. Furthermore, this indirect promotion of a threshold approach to monitoring can have the adverse consequence of effectively deterring monitoring for complex transactions.

515. Article 8 of the RIC, issued in January 2009, requires that insurance companies pay added attention to and investigate further complex and unusual transactions or patterns of transactions that have no apparent or visible economic or lawful purpose. Companies are additionally required to investigate further any transactions above a minimum value not to exceed SAR 10,000 (USD 2,660). The assessment team noted that as these rules were very recently established and implemented, and supervision in insurance is nascent, effectiveness in the sector could not be assessed. Such businesses did not exhibit adequate awareness of relevant AML/CFT requirements and have not had systems in place to systematically and adequately monitor and evaluate unusual transactions.

516. For the securities sector, Article 17.2 of the RAP requires that special attention be paid to all complex, large transactions and unusual pattern of transactions without apparent economic or visible

lawful purpose. Article 5.1 of the IFC requires companies to conduct continuous monitoring, giving particular care to all complicated, large and unusual transactions that do not have a clear economic or visible legal purpose.

Examination and record keeping of complex and unusual transactions

517. The AMLS includes a general record-keeping provision (Article 5) requiring that all financial and non-financial institutions retain records of documents and details relating to all transactions for a period of not less than ten years. The requirement refers to the need to retain all information necessary to ensure implementation of the AMLS.

518. Article 4.6.1 of the RBME requires that investigations into the background and purpose of unusual or suspicious transactions must be documented in writing. Further, per Article 4.10, all documentation relating to these investigations into unusual transactions must be retained in original and/or electronic form for no less than ten years. Article 5.1 of the IFC requires the authentication in writing of monitoring and analysis undertaken to identify unusual activity. All documentation including that related to operations undertaken by the company must be retained for at least ten years (Article 4). Article 8 of the RIC requires companies to transcribe the results of any inquiry into complex or unusual transactions in writing, and to retain these findings for a period of at least five years.

519. Article 17.4 of the RAP requires securities companies to retain a record of findings and material associated with investigations into unusual transactions for a period of at least 10 years. This information must be made available to the authorities, internal and external auditors upon request.

Effectiveness (Recommendation 11)

520. While implementing regulations issued by supervisory authorities generally more clearly distinguish between monitoring and STR identification, the AMLS presents detection of crime as the purpose of monitoring measures, thereby having the adverse effect of promoting transactions monitoring systems designed strictly to generate STRs. This problem is exacerbated by the description of the STR filing requirement set out in Article 7 of the AMLS, which states that "Upon availability of sufficient indications and evidence showing that a complex, an unusual, immense, or unusual deal or transaction has been made" an STR must be filed. This lack of a clear distinction between monitoring and STR identification adversely impacts effectiveness.

521. The assessment team noted that Article 4.6 of the RBME, while providing detailed explanation of the elements of the monitoring process, lacks clarity regarding institutions' specific obligations. This renders it difficult for banks and money exchange businesses to implement.

522. The assessment team found that no financial institutions with which they met were able to confirm that findings related to the investigation of complex or unusual transactions are retained in accordance with record-keeping requirements. In practice, and as suggested by the RBME, many financial institutions use automated monitoring systems that will incorporate and retain information and findings related to investigations into complex or unusual transactions. Accessibility and appropriateness (*i.e.*, inclusion of information such as reason for initial selection and for determination of whether or not to file or report) of these recordings could not be determined although authorities noted that they have not faced difficulties with institutions providing the results of the investigations performed on transactions. The

assessment team also noted that some institutions may not be adequately staffed to sufficiently and effectively review all cases of unusual activity generated by such automated systems.

523. While at the aggregate level the monitoring of activity in the banking system has improved over recent years, this progression has not been consistent across institutions. A review of examination reports revealed problems among some institutions in the implementation of policies and procedures related to transaction monitoring, providing verification of the assessment team's observations obtained in the context of meetings with private sector individuals during the onsite visit. Inspections turned up evidence of institutions improperly carrying out internal investigations of unusual activity whereby, for example, questions critical to the inquiry were left consistently unanswered and information provided was often irrelevant.

524. Transaction monitoring is effective only to the extent that those responsible for conducting the monitoring have a clear understanding of what constitutes unusual activity. While the banks tend to be more savvy and knowledgeable in this regard, other types of financial institutions lack a strong understanding of what they are monitoring for and to what end. Non-bank financial institutions exhibit limited understanding of potential ML/FT abuse of their sector, and as such cannot be expected to undertake effective monitoring. While finance, insurance and securities businesses comprise a relatively small portion of the financial sector, it is important that the foundations for strong implementation of AML/CFT be established now in anticipation of their future growth.

525. As the RIC were only recently issued by SAMA in January 2009, implementation and the effectiveness thereof is difficult to assess. SAMA has understandably to date been largely focused on the issuing of licenses rather than supervisory functions. That said, SAMA's supervisory activities with respect to the insurance companies has begun and a number of supervisory visits and examinations on unlicensed companies has been performed. Similarly, the CMA issued the RAP in December 2008 and supervision of AML/CFT procedures has been limited to date.

Recommendation 21 (Countries that apply the FATF Recommendations insufficiently)

Description and analysis

Special attention to countries

526. The RBME (Articles 4.6 and 5.2) draw attention to geographic and country-specific risks that must be taken into consideration in banks and money exchange businesses. Entities should pay special attention to all business relationships and transactions conducted with persons and entities located in countries that do not sufficiently apply the FATF Recommendations. A description of indicators of AML/CFT regime weaknesses is provided in an appendix describing "red flag indicators" where it is also stated that "the classification of an account as high-risk based on the geography of where the customer conducts its business activities depends on whether or not the country is on the FATF list of Non-Cooperative Countries and Territories (NCCT)" and refers to the FATF website. To assist these financial institutions, SAMA distributes FATF statements through banking circulars. SAMA additionally acts to ensure the banking community's awareness of the FATF statements through meetings of the Self Supervisory Committee (SSC), at which SAMA is an observer participant.

527. Article 54 of the RIC requires companies to pay particular attention to their relationships and activities with companies and individuals (including beneficiaries) that work in or operate through countries that do not or do not sufficiently apply the FATF Recommendations. To assist companies in the identification of countries that do not sufficiently apply the FATF Recommendations, Article 67 refers to reports issued by FATF, FSRBs, the International Monetary Fund (IMF) and the World Bank. SAMA has also disseminated FATF statements to insurance businesses.

528. For the financing sector, Article 3.2 of the IFC instructs that additional customer due diligence and ongoing monitoring must be applied to all high risk business relationships and operations, including those involving customers in countries that do not or insufficiently apply the FATF Recommendations. From this, an obligation to pay special attention can be inferred, although no further instructions or guidance to assist in the identification of such countries is provided.

529. For the securities sector, as described in the RAP (Article 17), there is a requirement to consider the level of implementation of the FATF Standards as part of the risk-based CDD requirements, to enable businesses to apply enhanced CDD measures. Article 9 also requires that entities must carry out assessments of standards of AML/CFT, pay attention to assessments of compliance with FATF Recommendations such as those undertaken by FATF, FSRBs, the IMF and the World Bank.

Examination of transactions

530. Article 4.6.1 of the RBME, in describing the characteristics of transactions that should be further examined , notes business relationships or transactions with entities and individuals from or in countries that do not sufficiently apply the FATF Recommendations. While there is no specific rule for the examination of such transactions in particular when they do not have any apparent economic or viable purpose, the RBME also states that all "unusual patterns of transactions that do not have apparent or visible economic, lawful or commercial purpose" must be examined.

531. The supervisory authority explained that based on the RBME, banks and money exchangers in KSA are required to investigate further all transactions involving a jurisdiction with weak AML/CFT and put these findings into writing. As such, institutions will automatically investigate transactions that, in addition to involving a country with weak AML/CFT regime may additionally have no economic or viable purpose. The assessment team was unable to verify institutions' implementation of this. It should furthermore be noted here that, as described above, while providing details regarding the monitoring process (in which the aforementioned guidance regarding transactions involving jurisdictions with weak AML/CFT appear) the RBME lacks clarity in addressing institutions' specific obligations with regard to transaction monitoring. This has an adverse impact on institutions ability to implement this parameter.

532. The RIC contain several provisions regarding companies' obligations to pay special attention to transactions on the basis of the involvement of a country that does not adequately apply the FATF Recommendations. Article 54 states that if SAMA informs companies of a country that does not sufficiently apply the FATF Recommendations, those companies must treat any transactions involving that country as high-risk. Separately, Article 8 specifies that companies must inquire further about any transaction to or from a country that does not sufficiently apply the FATF Recommendations and having no visible economic or lawful purpose. The results of such inquiry must be put into writing. Furthermore, Article 54 states that all transactions meeting these two criteria must be reported to SAFIU.

533. Article 5.1 of the IFC provides that measures should be taken to identify any transactions that do not have a clear economic or visible legal purpose as a general rule, but does not draw a direct link between this condition and that of involving a country that does not sufficiently apply the FATF Recommendations (once a transactions from a high risk jurisdictions is identified, financial institutions should determine if this transaction has no visible legal purpose). The RAP (Article 17.4) requires that the background and purpose of transactions with clients or institutions from countries that do not or do not sufficiently apply the FATF recommendations be examined and the results established in writing.

Counter-measures

534. Article 5.2 of the RBME gives SAMA the authority to issue counter-measures in the situation where countries continue to not sufficiently apply the FATF Recommendations. Specifically, they are authorized to issue instructions about how transactions relating to certain countries of concern should be handled.

535. SAMA regularly distributes FATF statements through circulars, although the circulars do not provide adequate additional guidance to institutions. The sample of such circulars provided to the assessment team contained instructions limited to either "review" or "review and implement".[73] SAMA provided some evidence of where they have followed up with banks to verify what additional measures and procedures have been taken by these institutions in response to SAMA circulars disseminating FATF statements. Measures undertaken by financial institutions included the review and assessment of transactions, consideration of taking cautionary measures, refusal to open correspondent accounts, and ensuring that all transactions with these countries abide by enhanced supervisory procedures. The basis for these actions (*i.e.*, whether they were directed by SAMA or undertaken voluntarily) could not be established by the assessment team. Hence, it could not be established that the authorities have exercised their ability to require financial institutions to take counter-measures, nor could the nature of such counter-measures be determined.

536. Requirements for exercising enhanced due diligence with respect to transactions involving countries that do not apply the FATF Recommendations sufficiently can be found in sector-specific AML/CFT rules and regulations. Article 5.2 of the RBME states that banks and money exchange businesses, when conducting business with persons and entities that are located in or conduct activities in countries that do not sufficiently apply the FATF Recommendations, should exercise additional due diligence. For the securities sector, the RAP require that, based on an assessment of a country's adherence to the FATF Recommendations, the higher the risk, the greater the due diligence that must be applied to business relationships. In the case where businesses are advised of such countries by CMA, they must also apply enhanced due diligence to include obtaining additional information and conducting ongoing monitoring. There is no further provision for taking action beyond enhanced CDD when transactions involve a country that does not apply the FATF Standards. Similarly, the RIC (Article 61(b)) and IFC (Article 3.2.3(c)) refer to the need for enhanced due diligence in such situations, but do not provide specifically for the application of counter-measures. The assessment team furthermore found no evidence of application of counter-measures in the non-bank financial sector.

537. Since these described enhanced due diligence measures are a common risk factor to be taken into account as part of any CDD framework (see Section 3.2 of this report), the assessment team does not

[73] None of the circulars provided corresponded to a FATF statement calling for counter-measures.

consider this to be a form of counter-measure. The assessment team is not aware of any other possible counter-measure.

Effectiveness (Recommendation 21)

538. In their efforts to satisfy the provision that special attention be paid when activities involve countries that do not sufficiently apply the FATF Recommendations, financial institutions have a tendency to focus their efforts on the set of countries noted in FATF's statements as and where provided by the authorities. While the RBME provide broader guidance for use by institutions in identifying countries with weak AML/CFT regimes, in practice there is heavy reliance on direct guidance from SAMA. While those institutions that subscribe externally to private services that provide information for use with automated systems may more adequately consider countries with weaknesses in their AML/CFT regimes, a number of institutions are falling short in their observance of the requirements in this area. Of particular note is that in the course of meetings, several private sector entities referred to incorporating into their policies and procedures the need to identify activity involving countries on the NCCT list, which was effectively terminated in early 2008. These same entities further noted that there have been no countries on the NCCT list for several years such that this parameter has not figured into their monitoring processes for some time.

3.6.2 Recommendations and Comments

Recommendation 11

539. The evaluation team found that generally there is a lack of clear understanding among government agencies and financial institutions regarding the distinction between requirements to monitor unusual transactions (as required by Recommendation 11) and to report transactions that are identified as suspicious (as required by Recommendation 13). More fundamentally, entities are often unsure of what are the appropriate parameters and considerations to apply to the monitoring of transactions (that is, what constitutes complex or unusual, and, in short, what they are monitoring for). These issues could be conquered over a reasonable amount of time through a combination of further clarification of rules and regulations, training, and supervision.

540. Regarding the monitoring obligation, it should be noted that there exists more than one official version of the AMLS. In a second version of the AMLS, a monitoring obligation is more clearly laid out, although because the reference appears in an implementing regulation (7-1) associated with the reporting of STRs, the linkage between monitoring and the detection of suspicious or criminal activity is similarly established. That multiple versions of these regulations coexist is in many ways problematic, not least in that it is not clear to which entities must adhere.

541. Clarification of the rules and regulations related to the monitoring of transactions is critical to ensure entities' understanding and ability to comply. As an absolute priority, authorities should ensure that there is one version of the AMLS, the exact wording of which is consistent in Arabic and English.[74] The AMLS and references to it in the RBME should furthermore be modified in such a way as to ensure that financial institutions' monitoring process is not prejudiced by the suggestion that the objective of the

[74] The assessment team notes that many senior management positions of banks are occupied by non-Arabic speaking individuals such that an accurate official version of the AMLS in English that is consistent with the Arabic is of critical importance.

process is to detect criminal activity. Further, the RBME should be modified to make explicit the monitoring obligation for banks and money exchangers and to clarify guidelines for monitoring procedures to enable more effective implementation. References to monitoring threshold parameters in the RBME and RIC should also be removed.

542. Improved supervision of banks' AML/CFT procedures – and the levying of sanctions in the case of violations – would result in significantly more effective systems for the monitoring and evaluation of unusual activity. This is applicable across all sectors, although given the risks associated with the banking sector and its dominance in the financial system, marginal improvements in this sector in particular are likely to reap significant returns in overall effectiveness.

Recommendation 21

543. The authorities should seek to clarify what is required of institutions with respect to identifying those countries that do not sufficiently apply the FATF Recommendations, and to the handling of transactions and business involving such countries. Additionally, counter-measures must be established for all sectors.

544. For all sectors, the competent authorities should provide better guidance to institutions to assist in the identification of countries that do not sufficiently apply the FATF Recommendations. Furthermore, where SAMA does distribute by circular FATF statements identifying countries of concern, it should more explicitly note institutions' obligations with respect to use of this information. Across all sectors, where it appears in rules and regulations governing the AML/CFT practices, reference to the NCCT list should be replaced with more comprehensive and up-to-date guidance.

3.6.3 Compliance with Recommendations 11 & 21

	Rating	Summary of factors underlying rating

R.11	**PC**	• Legal framework establishes monitoring for unusual transactions as a means for crime detection.
		• Monitoring obligation is not explicit for all sectors.
		• Effectiveness issues:
		  ○ Lack of distinction and awareness of the difference between monitoring unusual transactions and STR reporting requirements negatively impacts monitoring process.
		  ○ Deficiencies related to supervision and enforcement hinders effectiveness
		  ○ Monitoring threshold parameters for banking and insurance

R.21	**PC**	• Absence of counter-measures • Insufficient guidance regarding what is required of institutions with respect to identifying those countries that do not sufficiently apply the FATF Recommendations • Overreliance on FATF statements and uneven adherence across sectors and entities hinders effectiveness.

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

3.7.1 Description and Analysis

Recommendation 13 and Special Recommendation IV (Suspicious transaction reporting)

Requirement to make STRs (ML and FT)

545. As indicated in section 2 of this report, under the AMLS, terrorism finance is considered to be a money laundering offense under the AMLS. In this light, the following description equally applies to R.13 and SR.IV.

546. The obligation to file STRs is set out in primary legislation and applies to all financial institutions in Saudi Arabia. Article 7 of the AMLS requires that covered entities inform the FIU immediately "upon sufficient indications and evidence showing that a complex, a large or an unusual deal or transaction has been made, or that an activity of suspicious nature or purpose is underway, or is related to money laundering, terrorist acts or terrorist organizations." While the STR reporting obligation specifically includes transactions believed to involve the financing of terrorism, terrorist acts and terrorist organizations, shortcomings in the criminalisation of terrorist financing (see section 2.2) however translate into limitations in the reporting requirements as specified under Recommendation 13.

547. Upon discovery of a suspicious transaction, covered entities are required to immediately notify SAFIU using a standard STR reporting form designed by SAFIU. They are required to thereafter submit a report detailing all available data relating to the transaction or attempted transaction including information on the parties involved. For financial institutions, this report must be submitted within ten days. Financial institutions are also required to provide a copy of the STR to their supervisory body simultaneously upon filing it with SAFIU (see section 2.5).

548. The requirements for STR filing for financial institutions is reiterated and further detailed in SAMA's RBME, RIC, and IFC, and in CMA's RAP.

Attempted transactions and tax matters

549. Article 7 of the AMLS specifies that covered entities must report all suspicious transactions, including attempts to carry out such transactions. In practice, this requirement is understood and financial institutions do not limit their reporting to executed transactions. Furthermore, Article 2 of the AMLS includes tax evasion crimes among a list of criminal activities whereby dealing with the resulting proceeds is deemed a money laundering crime. Hence, suspicious transactions thought to involve tax matters must be reported.

Reporting threshold

550. The law requires reporting of STRs, regardless of the amount of the transaction. However, as previously noted, Article 4.6.3 of the RBME includes as a parameter for transaction monitoring a threshold of SAR 60,000 for a single transaction or transactions aggregated over a one month period (product- and customer-specific adjustments of the threshold and other monitoring parameters can be made based on risk

assessment). Similarly, the RIC (Article 8) specify a monitoring threshold parameter of SAR 10,000. While it cannot be excluded that transactions below the threshold are reported, this effectively may impede the reporting of transactions below the threshold and, as observed by the assessment team in meeting with private sector entities, can in practice have the effect of a reporting threshold. However, the authorities reported that many suspicious transactions under this amount are reported. The monitoring threshold also could have a negative impact on the ability of FIs to detect structuring of transactions to avoid reporting and CDD requirements below the identification threshold ("smurfing") (see section 3.2 of this report).

Effectiveness

551. Statistics provided by SAFIU indicate steady growth of STR filings on behalf of financial institutions over the past few years. This can be attributed to the provision of additional and updated implementing regulations, and increased awareness – particularly among banks – resulting from the significant efforts of authorities working with the institutions. Given the size of the Saudi economy, the size of the remittance market (globally second only to the US) and broad scope of required reporting coverage, however, one should expect more STRs to be filed. The authorities point to other factors that contribute to a low number of STR filings, including the presence of significant undocumented economy, low rate of crime, and efforts of the Saudi government and supervising authorities to combat ML and TF activities. Nevertheless, the assessment team considers the current numbers to be too low.

STRs Filed by Financial Institutions (2004-2008)					
	2004	2005	2006	2007	2008
Banks	311	418	303	546	769
Exchange companies and institutions	30	12	13	30	18
Total	341	430	316	576	787

Source: SAFIU

552. At the institutional level, several banks reported a steady increase in the number of their STR filings to SAFIU over recent years and credited this to guidance from SAMA, training and increased capacity.

553. In comparison to banks, other financial institutions exhibit a lesser understanding of their general AML/CFT obligations—in particular their responsibility to report all suspicious transactions to the FIU—and awareness of the AML/CFT threats posed to these non-bank sectors. While the non-bank financial sector is small and only relatively recently established, and risk is undoubtedly a factor (authorities note that these sectors in some cases are prohibited from dealing in cash transactions), it is noted that no STR has ever been filed on behalf of an insurance, investment or finance company.

554. Within the banking sector, while at the level of operating headquarters there exists a reasonable level of awareness of AML/CFT threats and the STR filing requirement, the assessment team found that this understanding diminishes at the lower levels of operations. Branches and subsidiaries are required to conduct transaction monitoring and report up to the AML/CFT compliance unit of the parent institution so that the determination can be made as to whether or not a STR is to be filed. Awareness at branch and subsidiary level of AML/CFT requirements, including in particular those regarding monitoring of transactions and the identification of suspicious activity, is questionable and could adversely impact both

the quantity and quality of STR reporting. The authorities additionally emphasized their efforts to continue to enhance awareness at the level of subsidiary branches through special training and inspections.

555. The authorities emphasize that the Saudi government agencies treat combating the financing of terrorism as a high priority. In their issuance of rules for AML/CFT, supervising authorities provide indicators to assist financial institutions in distinguishing between money laundering and terrorism finance-related transactions. However, in the course of discussions with private sector participants, the assessment team observed that there is often less understanding and awareness of potential abuse related to terrorism finance than to money laundering. When asked how their sector or business might be taken advantage of for the purposes of financing and facilitating terrorism, financial institution representatives consistently answered either that this simply does not happen, or that screening against the Specially Designated Nationals (SDN) and UN lists provides them with the necessary assurances that this cannot happen. A further breakdown of data on TF-related STR filings by type of entity was not available.

STRs Received by Nature of Suspicion (financial and non-financial institutions) (2004-2008)					
	2004	**2005**	**2006**	**2007**	**2008**
ML	348	444	351	649	955
TF	2	7	54	94	64
Total	350	451	405	743	1019

Source: SAFIU

Recommendation 14 (Safe harbor and tipping off)

556. According to Article 25 of the AMLS, unless the actions are determined by a competent judicial authority to be in bad faith (with the intention to harm), exemption from criminal, civil or administrative liability arising from the performance of duties under the AMLS is provided for the chairman of financial and non-financial institutions, board members, owners, temporary and permanent employees, and authorized representatives. This protection is restated in the RBME, IFC, RIC, and the RAP.

557. "Tipping off" is prohibited under Article 9 of the AMLS, which states that financial and non-financial institutions, their staff and others subject to the provisions of the AMLS may not directly or indirectly alert clients or related parties of suspicions regarding their activities. The Article additionally specifies conduct that is to be observed in order to avoid tipping off, including maintaining the confidentiality of STRs filed to SAFIU. The RBME (Article 4.7.3) further provides that banks and money exchange businesses should not inform or otherwise unintentionally tip off customers of their suspicion or of their notification to the authorities. Article 52 of the RIC, Article 14.2 of the IFC and Article 21 of the RAP also forbid the disclosure of any information related to the filing or potential filing of a STR.

558. The assessment team found no gaps in the legal provisions regarding safe harbor and tipping off as applied to financial and institutions and their staff. Indeed, heightened awareness of the prohibition of tipping off is apparent among private sector entities and their employees.

559. As described in section 2.5 of this report, the double reporting of STRs to the SAFIU and to the supervisor authority, as well as the access that accountants (themselves reporting entities) have to STRs filed by other reporting that they are supervising on behalf of the supervisor, increases the risk of tipping

off. Despite general confidentiality and no-tipping-off requirements for supervisory staff, this could lead to institutionalized tipping-off. However, it should be noted that the team is not aware of any such cases of tipping-off.

Recommendation 19 (other types of reporting)

560. The feasibility and utility of a requirement for the reporting of currency transactions above a certain threshold was considered by the PCCML, which formed a team to investigate and report on the issue. This team consulted with the FCML, a consultative group comprised of representatives from the private commercial banking community, which also undertook a study into the matter. It was the finding of the PCCML that the current reporting requirements for unusual activity monitoring and suspicious activity reporting adequately capture activities of concern. The PCCML endorsed the reported findings of the investigative team in November 2008. The assessment team received a copy of the notes of this meeting.

Recommendation 25 (Feedback related to STR)

561. Article 11 of the AMLS requires the FIU to provide feedback to reporting entities and competent authorities, although does not specify the form this feedback should take. While it seems SAFIU does consistently acknowledge to reporting entities the receipt of STRs, provision of feedback beyond that is not consistent either across or within sectors. While SAFIU receives adequate feedback from prosecution regarding the utility of reports sent on, this feedback is not consistently provided to the reporting entity. Statistics on disclosures and their results are published in SAFIU's annual report (see also section 2.5).

562. With respect to case-by-case feedback, SAFIU is most diligent in its communication with banks and money exchange businesses, although even this varies in degrees, at times depending on how proactive the entity in question is in terms of following up with SAFIU and seeking this feedback. In the second half of 2008, SAFIU provided feedback on more than 257 cases, compared to a total of 1,019 STRs received for the year. Authorities describe feedback provided to the reporting parties as clarification of the procedure and the final decision in respect of the STR. Furthermore, in the case where a filed STR revealed use of new methods, the reporting party is informed of that, and such way or method will be included in guidance issued by SAFIU after appropriate review, including by the PCCML.

563. For banks, SAMA noted that the FCML and the Self Supervisory Committee[75] (SSC are additional forums that facilitate feedback between institutions. These private sector-comprised consultative groups meet monthly to share experiences regarding compliance issues, in particular in the area of AML/CFT. It is the understanding of the assessment team that lessons learned with respect to suspicious transaction reporting is commonly discussed in the meetings of these committees in which SAMA also participates as an observer.

3.7.2 Recommendations and Comments

Recommendation 13 and Special Recommendation IV

[75] Saudi banks have established a Self-Supervisory Committee to closely monitor and fight against the threat posed by terrorism and to coordinate all efforts to freeze the assets of the identified individuals and entities. The Committee is composed of senior officers from banks responsible for Risk Control, Audit, Money-Laundering Units, Legal and Operations, and operates in the presence of SAMA officials. (Source: KSA embassy in Washington website, http://www.saudiembassy.net/archive/2001/statements/page1.aspx).

564. Saudi Arabia is to be commended for its efforts regarding suspicious transactions reporting, as evidenced by the upward trend in STR filings with SAFIU over the 2004-2008 period. As previously noted, however, the low overall number of STR filings relative to the size of the economy and characteristics of the financial sector point to a lack of effectiveness. Further improvements can be made in the quantity and quality of STR reporting by more clearly explaining the distinction between monitoring transactions for unusual activity and identifying and reporting of suspicious activity. Efforts to increase awareness – through training, provision of typologies and case studies, etc. – of the potential for money laundering and terrorist financing abuse is also recommended. Additionally, the monitoring threshold parameter for banks and insurance companies should be abolished, as the assessors believe it could have a negative impact on the effectiveness of the reporting system.

Recommendation 14

565. The sharing of STRs with supervisors (and effectively with accountants) increases the chance that a STR is tipped-off, and should be abolished. However, in the absence of any tipping-off cases, the team considers this Recommendation to be met.

Recommendation 25

566. SAFIU and relevant competent authorities should seek to implement a comprehensive system of providing feedback that is in line with the FATF Best Practice Guidelines. In particular, the FIU should endeavor to provide case-by-case feedback to all those filing STRs (including whether or not an STR resulted in an investigation and prosecution), and the development of case studies and typologies (in addition to indicators) relating the potential for ML and TF abuse across sectors. SAMA and CMA should also seek to provide further guidance in the form of typologies to assist institutions with the development of their capabilities to identify unusual and suspicious transactions. Special attention should be given in particular to the development of terrorism finance awareness.

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**	• Shortcomings in the criminalization of terrorist financing limit the reporting obligation. • *Effectiveness issues:* o Effectiveness is inconsistent across and within sectors o Lack of clear distinction between unusual and suspicious activity hinders effectiveness of STR reporting o Low reporting levels raise concerns about the effectiveness of the system o Monitoring threshold parameter for banks and insurance companies promotes a de facto reporting threshold
R.14	**C**	• This Recommendation is fully observed.
R.19	**C**	• This Recommendation is fully observed.
R.25	**PC**	• Feedback is inconsistently applied and not adequately used as a tool to further the effectiveness of AML/CFT provisions • Insufficient guidance regarding ML and TF methods and typologies

	Rating	Summary of factors underlying rating
SR.IV	**LC**	• Shortcomings in the criminalization of terrorist financing limit the reporting obligation. • *Effectiveness issues:* o Effectiveness is inconsistent across and within sectors o Lack of clear distinction between unusual and suspicious activity hinders effectiveness of STR reporting o Low reporting levels raise concerns about the effectiveness of the system o Monitoring threshold parameter for banks and insurance companies promotes a de facto reporting threshold.

Internal controls and other measures

3.8 Internal controls, compliance, audit and foreign branches (R.15 & 22)

3.8.1 Description and Analysis

Recommendation 15 (internal controls)

567. The requirement that financial institutions establish internal procedures and controls is set out in the AMLS. Article 6 describes the general requirement that financial institutions "establish precautionary and internal monitoring measures to uncover and foil any of the crimes provided for" in the AMLS. Further detail is found in Article 10, which requires that institutions have programs that include the development and implementation of internal controls and procedures, training programs for employees, internal audit and control systems, and the appointment of qualified officers "at the higher administrative level" to implement the program.

568. For banks and money exchangers, Article 4.2 of the RBME establishes the requirement that institutions develop and implement AML/CFT comprehensive compliance programs. Internal controls requirements are further detailed in Article 4.7.4 of the RBME. For the insurance sector, Article 5 of the RIC requires that all companies must develop written policies to combat money laundering and the financing of terrorism. Companies must ensure that all employees understand and implement the measures described by such strategies, to include guidance on customer due diligence reporting, records keeping, transaction monitoring and suspicious transaction reporting.

569. The IFC (Article 6) requires finance companies to establish internal control programs to combat ML/TF and to notify all employees thereof. For the securities sector, Article 23 of the RAP requires that companies have in place and implement internal policies, and procedures to help prevent ML/TF, and that they communicate these to its employees.

Designated AML/CFT Units

570. Article 10 of the AMLS requires covered entities to appoint qualified persons at the highest administrative level to implement their AML/CFT policies, plans, procedures, and internal controls and the setting up of internal audit and control systems to ensure that AML/CFT requirements are met. The director general of the covered entity (or nominee thereof) must accept responsibility for AML/CFT

compliance and an employee or department must be designated as responsible for submitting reports to SAFIU. For all sectors, equal provisions can be found in the relevant AML/CFT rules and instructions.

571. Article 4.7.4 of the RBME requires banks and money exchangers to establish an independent, dedicated function to implement AML/CFT compliance programs. For small institutions, this can be handled by a dedicated Compliance officer while larger institutions (more than five branches) must establish a money laundering control unit (MLCU) with adequate staffing as described by the RBME. In either case, the head compliance officer must be a senior management position, reporting directly to the general manager of managing director. Article 4.7.4 states that such person "should have sufficient authority, independence, accountability and resources, and he/she should be granted timely access to customer information," including CDD information, transactions records and other relevant data.

572. The RIC (Article 39) require companies to designate a compliance manager to ensure compliance with AML/CFT policies, measures and rules and regulations. Article 40 further ensures that the compliance officer has full access to all data necessary to perform these duties. Additionally, the RIC require companies to create an "internal inspection team" to carry out a range or responsibilities related to AML/CFT (Articles 33 and 34).

573. Article 6 of the IFC provides that an AML/CFT compliance officer be appointed with total independence from the other departments of the company, reporting directly to the senior management. It is further stated that the compliance officer has to have adequate and sufficient financial, technical and human resources to perform the compliance function appropriately. The RAP (Article 3) require that companies appoint a director or senior manager to oversee compliance with AML/CFT policies, procedures and requirements. This officer and his/her staff is ensured timely access to all data necessary in the fulfillment of their duties (Article 23.3).

Independent Audit Programme

574. Article 10 of the AMLS requires covered entities to set up internal audit to ensure the implementation of AML/CFT measures. Where such task is performed by an external auditor, testing compliance with established AML/CFT policies and procedures must be included in the auditing functions. For banks and money exchange businesses, Article 4.8.2 of the RBME states that an independent internal auditing department must periodically assess the effectiveness of internal controls and the adequacy of the overall AML/CFT policies. The audit report must be provided to senior management for appropriate action.

575. For financing companies, Article 6 of the IFC requires regular auditing of the AML/CFT compliance to be conducted by an internal unit, independent from compliance. External auditors must also verify compliance with AML/CFT policies in the course of their duties.

576. Article 32 of the RIC requires that as part of their internal control measures, a company must set up an internal audit unit to review compliance and effectiveness of the AML/CFT program. A review must be conducted on an annual basis, the results of which must be reported to the company's Board. For the securities sector, Article 24 of the RAP requires that an internal audit shall regularly assess the effectiveness of the internal AML/CFT policies, procedures and controls and compliance. Neither the RIC nor the RAP explicitly provide for the independence and adequate resourcing of the audit function.

Training programs

577. Article 10 of the AMLS sets out the requirement that all covered entities establish continuing training programs for employees to keep them updated on money laundering developments and help them to fulfill their AML/CFT duties. Training program must include plans and budgets for the training of staff in subjects to include AML/CFT conventions, laws, rules, and instructions, as well as new developments in money laundering and terrorism finance (typologies) and the means of recognizing and combating these threats. The training programs must also cover the potential civil and criminal liability of each employee under the pertinent laws, regulations, and instructions.

578. For banks and money exchange businesses, further detail on the required coverage of training programs is described in the RBME (Article 4.9.2). This includes the requirement to provide AML/CFT training to employees prior to allowing them to engage in provision of services to customers. The RIC (Articles 37 and 38) lay out detailed requirements for training programs to be applied to new employees and all level and category of employees on AML/CFT rules and regulations, including CDD measures, and the tracking, detecting and notifying of suspicious transactions. Companies are required also to provide training at least once a year or as deemed necessary to update staff on AML/CFT developments.

579. Article 8 of the IFC requires companies to prepare and organize regular training programs for their employees to enhance their awareness of the AML/CFT laws and regulations and their understanding of such operations, the different typologies used by money launderers and terrorist financiers and the company's internal instructions to combating them, including on CDD procedures and identifying and reporting suspicious transactions. The training programs have to be updated periodically to include the latest developments. Also all new employees, particularly those directly dealing with the public, have to obtain training on AML/CFT.

580. For the securities sector, Article 25 of the RAP requires companies to ensure that all new staff and employees receive regular training on AML/CFT, including laws, regulations, CDD measures, detecting and reporting STRs, new techniques, methods and trends used by money launderers and terrorist financers, and the company's internal controls, procedures and policies with respect to AML/CFT. Employees must also be trained on the roles and responsibilities of staff in combating money laundering and terrorist financing.

581. Training programs can and often are developed and conducted internally, but the competent authorities also help to facilitate AML/CFT training by offering courses to which companies can send employees. The following statistics were provided to the assessment team:

Number of bank institutions' employees trained in AML/CFT (January 2004 to September 2008)			
YEAR	**Number of Participants inside SA: Bank institution's employees**		**Number of participants outside SA: Bank institution's employees**
	Internal Sessions	**External Sessions**	
2004	3 868	202	15
2005	3 427	234	14
2006	4 541	1 864	36
2007	8 145	1 010	25

Number of bank institutions' employees trained in AML/CFT (January 2004 to September 2008)			
YEAR	Number of Participants inside SA: Bank institution's employees		Number of participants outside SA: Bank institution's employees
	Internal Sessions	External Sessions	
9/2008	4 215	1 414	11

Source: SAMA

582. Statistics provided on the number of non-bank trained staff are as follows:

Number of non-bank financial institutions staff who have received AML/CFT training	
Financial Sector	*Number of staff*
Securities	89
Insurance	250
Financing	75 (2 Companies)

Note: Period and comparative statistics (total number of staff) not available.

583. While it is apparent that institutions largely undertake to conduct training of employees in accordance with requirements laid out by SAMA, training often focuses primarily on familiarization with rules and regulations with less emphasis on developing a foundation for understanding actual ML and TF risks.

Screening Procedures

584. The AMLS (Article 10.1) requires the appointment of qualified senior management staff to implement AML/CFT policies and procedures. Article 4.9.2 of the RBME provides that banks and money exchange businesses should put in place adequate background screening procedures to ensure high standards when hiring employees. Screening procedures may be conducted on a risk-based approach and taking into account the function and responsibilities associated with a particular position.

585. For the insurance industry, the RIC (Article 35) specify that companies must ensure that employees are qualified and investigations into their identities and personal data are undertaken. Additionally, the rules require that special attention is given to assessing the qualifications of and exercising control over the conduct of employees in positions deemed to be vulnerable to targeting by those with seeking to conduct money laundering or terrorism finance (Article 36). Finance companies must also establish and apply to the hiring process criteria that ensure a high level of competency and integrity of employees (Article 6).

586. The assessment team was informed by banks that they are aware of their inherent attractiveness to persons seeking opportunities to conduct fraudulent activity, and that banks have, therefore, in place robust screening procedures for the hiring of staff to limit the risk of being defrauded. Recognizing that 80% of fraud is conducted internally, banks commonly screen potential employees against the "E-List". This is a list that contains the names of individuals who have been laid off by banks as a result of questionable actions or otherwise accused of wrongdoing in their employment. The

list is populated and maintained by the banking community. Identified individuals are kept on the list for a period of five years only.

Recommendation 22 (Foreign operations)

587. The provisions of the AMLS apply to financial institutions and their branches and subsidiaries operating within and outside the Kingdom (Article 3.2). Article 2.3 of the RBME reiterates this for banks and money exchange businesses, specifying that in the case where requirements of the host country differ from those imposed by Saudi Arabia, foreign branches and subsidiaries must apply the more stringent of the two regimes. SAMA is to be informed when a foreign branch or subsidiary is not able to apply AML/CFT requirements that are up to the Kingdom's standards. Entities are required to pay particular attention to branches and subsidiaries located in countries that do not adequately apply the FATF Recommendations.

588. For the financing sector, Article 2 of the IFC provides that the provisions of the AMLS, the AML/CFT regulations, and the FATF Recommendations apply not only to companies operating in Saudi Arabia, but to all branches and affiliates inside and outside the Kingdom. The companies have to implement these provisions on their branches and affiliates outside the Kingdom to the extent authorized by the laws and regulations applicable in the host country and SAMA is to be notified in the event of any conflict in home and host country requirements when the stricter provision cannot be implemented. The RIC and RAP also adequately address the criteria of the recommendation. However, as these rules were introduced very recently and comprehensive AML/CFT supervision under these standards has yet to begin, effectiveness cannot be assessed. Authorities note that there are currently no braches of insurance companies located outside the Kingdom.

589. The assessment team noted in the course of meetings that banks are aware of the existence of requirements regarding the application of AML/CFT standards to their foreign operations. Authorities indicated that SAMA conducts onsite supervisory visits to Saudi bank branches operating abroad, which cover their ability to apply Saudi AML/CFT requirements. A sample list of such visits was provided to the team, showing visits to Saudi bank branches in Bahrain, UAE, Turkey, and Pakistan. Documentation related to banks' assessments of their ability to apply AML/CFT regulations to their overseas operations was however not available.

590. As noted previously, inadequate guidance to assist in the identification of countries that are not sufficiently compliant with FATF Recommendations adversely affects effectiveness across all sectors.

3.8.2 Recommendations and Comments

591. With the exception of explicitly providing for the independence and adequate resourcing of the audit function in the insurance and securities sectors, the rules and regulations pertaining to internal controls and policies are relatively robust., The assessment team however found their application to be somewhat inconsistent among financial institutions, and smaller non-bank financial institutions in particular. In the course of meetings with representatives of some private institutions, concerns were at times noted by the assessment team with respect to, for example, reporting structures and appropriateness of dedicated staffing.

592. As regards training, competent authorities are putting significant effort into training and increasing awareness, facilitating institutions' execution of training requirements by providing training through, for example, the Banking Institute. However, more can be done to both expand training opportunities across all sectors and to broaden the scope of training. The focus of most training is on understanding the rules and regulations in place. More training to enhance an understanding of how various systems, sectors, and individual entities can be exploited for the purposes of money laundering and terrorism finance is recommended.

593. The assessment team found that in the nascent insurance industry, where comprehensive rules to address AML/CFT were very recently introduced, companies have not established robust internal policies. Also limiting the effectiveness of internal control policies and programs to adequately address AML/CFT needs in this sector is the limited institutional awareness of AML/CFT threats regarding insurance and the measures companies must take against them. Notably, however, life insurance represents a small portion of these companies' business. Furthermore, SAMA has begun supervisory visits and examinations on insurance companies, and as such improvements in this sector should ensue. The evaluation team also encourages the authorities to work with the nascent financing industry to effectively implement the robust provisions regarding internal controls and policies that are laid out in the recently issued IFC.

3.8.3 Compliance with Recommendations 15 & 22

	Rating	Summary of factors underlying rating
R.15	**LC**	• Independence and adequate resourcing of the audit function not explicitly provided for in case of insurance and securities companies. Deficiencies related to supervision and enforcement hinders effectiveness, particularly in insurance and securities sectors.
R.22	**LC**	• Deficiencies related to Recommendation 21 have a negative impact on the ability to fully comply with Recommendation 22. • Deficiencies related to supervision and enforcement hinders effectiveness, particularly in insurance and securities sectors.

3.9 Shell banks (R.18)

3.9.1 Description and Analysis

594. The assessors were informed that SAMA will not grant a license to a bank without a physical presence in the KSA. All companies operating in the KSA, banks included, must register with the MOCI. Article 3 of the Commercial Register Law requires that commercial registrations must include "the address of the company's headquarters, branches, and agencies, whether inside or outside the Kingdom."

595. Article 4 of the RBME prohibits financial institutions in the KSA from entering into or continuing correspondent banking relationships with shell banks. Furthermore, Article 4 stipulates that in the establishment and maintenance of correspondent relationships, banks must verify that several minimum conditions are met by the correspondent bank, including that the bank does not maintain correspondent accounts for or deal directly with a shell bank. Banks are also required to obtain certification of AML/CFT compliance for all correspondent relationships, which should include a confirmation that they are not

dealing with any shell banks. These provisions are further reinforced by the Rules Governing the Opening of Bank Accounts and General Operational Guidelines for banks.

Effectiveness

596. There are currently no shell banks operating in the KSA. In meetings during the onsite mission, private sector entities largely demonstrated an awareness of the prohibition on maintaining correspondent relationships with shell banks and with banks that in turn have relationships with shell banks. However, the assessment team was not able to confirm adherence to the correspondent banking requirements to an extent that it would not have a negative impact on the ability of banks to ensure that they are not entering into a correspondent relationship with a shell bank, or that they ensure that their foreign correspondent does not permit its accounts to be used by shell banks.

3.9.2 Recommendations and Comments

597. Inadequate implementation of CDD measures in relation to correspondent banking relationships as noted in the discussion of Recommendation 7 have a negative effect on the ability of banks to ensure that the respondent bank is not a shell bank, or to ensure that the respondent bank does not permit (*de facto* or *de jure*) their accounts to be used by shell banks.

3.9.3 Compliance with Recommendation 18

	Rating	Summary of factors underlying rating
R.18	**LC**	• Effectiveness deficiencies relating to Recommendation 7 have a negative impact on the ability to fully comply with Recommendation 18.

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

General Background on Supervisory Authorities

The Banking Sector (Banks & Money Exchange Businesses)

598. For financial institutions in SA, SAMA and CMA are the supervisory authorities. SAMA, the Central Bank of SA, was established in 1952. SAMA:

- Issues the national currency, the Saudi Riyal.
- Acts as a banker to the government.
- Supervises commercial banks.
- Manages the Kingdom's foreign exchange reserves.

- Conducts monetary policy for promoting price and exchange rate stability.
- Promotes the growth and ensures the soundness of the financial system.

599. SAMA is also the supervisory authority for insurance companies and financing leasing companies.

600. The Banking Control Department, which reports to the deputy governor for technical affairs, is the ultimate tool that houses the supervisory and regulatory function within SAMA through its sub departments. The first of these, the Banking Technology Department is involved in developing and maintaining electronic payment systems. The second sub-department under Banking Control is the Banking Supervision Department, which is tasked with the licensing process and off-site supervision. The department, consisting of 70 employees, is involved in the off-site monitoring of banks, money exchanges and financing companies. The third sub-department, the Banking Inspection Department, is responsible for the on-site supervision (examination) for the previously mentioned sectors and has 150 employees. The very recently established Insurance Companies Department is tasked to license and both on and off site monitoring of insurance companies. It has a staff of 55 employees.

601. For the purpose of verifying the compliance of bank institutions with the AML/CFT requirements, SAMA, being the authority in charge of the supervision and monitoring of banking, insurance, leasing and financing activities in the Kingdom, has established, within the Banking Inspection Department, a unit specialized in the field of combating financial crimes and ML and FT operations. The number of inspectors working in the unit is 35; their main duties comprise covering all aspects of AML, CFT and financial crimes restraints including preparing organizational policies and measures, disseminating such policies to the banks, following-up and verifying banks' compliance therewith, preparing training material for the banking and non-banking sectors concerned with combating such crimes, in addition to providing bank data and studies that may be requested by the competent AML/CFT authorities, such as the FIU, the Investigation and General Prosecution Authority, and the General Research Directorate.

602. One of SAMA objectives, according to Article (1) of the Charter, is to regulate commercial banks and money exchange businesses. Article (7) of the same Charter stipulates that SAMA's Board of Directors may make such rules and regulations as it may consider necessary and appropriate to the conduct of the work of the Agency in accordance with its charter.

603. Pursuant to the Banking Control Law (BCL) of 1966, no person in Saudi Arabia may carry on any banking business without a license. The law designates SAMA as the licensing agency and provides that SAMA may, based on Article 16(3) of the BCL and subject to the approval of the Minister of Finance and National Economy, issue general rules regarding "fixing the terms and conditions, which banks should take into consideration when carrying out certain types of transactions for their customers." Articles 22, 23, and 24 of the BCL define administrative and criminal sanctions for violations of one or more provisions of the BCL or any regulations issued pursuant to Article 16 (3). Ministerial Decision No. 3/2149 dated 14.10.1406 H (1985??)- issued by the Minister of Finance and National Economy - approved the Rules for Enforcing the Provisions of the Banking Control Law, thus empowering SAMA with direct powers to apply some administrative sanctions as mentioned in other parts of the report.

604. The Minister of Finance and National Economy issued the "Decision on Regulating Money Changing Business" ("Decision on Money Exchange Businesses")[76] designating SAMA as the licensing agency for money exchange business. Two types of licenses are provided for: Type A allows for both currency exchange and money remittance services to be conducted; Type B only allows for currency exchange services. The scope of the BCL does not include money exchange businesses. However, Article 10 of the regulation provides that any violation of the Decision on Money Exchange Businesses entitles SAMA to withdraw the license to conduct the money changing business and allows for the application of sanctions pursuant to Articles 22, 23, and 24 of the BCL.

The Insurance Sector

605. Pursuant to the Law on Supervision of Cooperative Insurance Companies ("CICL"), insurance companies in SA have to obtain a license pursuant to the requirements set out in the Insurance Law, whereby SAMA is the designated authority to receive and approve license applications. Article 23 of the Insurance Law provides the Minister of Finance and Economy with the power to issue implementing regulations. As in the case of the Banking Control Law, any violations of the Insurance Law or its implementing regulations allow for the application of administrative measures by SAMA pursuant to Article 19 of the Insurance Law as well as of criminal sanctions by the courts pursuant to Article 21 Insurance Law.

The Financing Sector

606. The Minister of Finance and National Economy, through Ministerial Decision No 30317/1 issued on 21/7/1420 AH (1999), and based on Article 16 of the BCL designates SAMA as the licensing agency for finance leasing companies. Article 2 of the Decision provides that SAMA shall determine the conditions and rules related to its supervisory mandate, including to set internal control guidelines, accountability measures and policies and to set risk management guidelines. Article 5 of the Decision provides that the sanctions provided for in Articles 22 and 23 of the BCL are applicable for any violations of the provisions of the Decision or any rules issued by SAMA.

The Capital Market Sector

607. CMA was established in 2004 by virtue of Article 4 of the Capital Market Law issued by Royal Decree M/30 dated 2/6/1424H (2003)(CML). According to Article 5 of this law, CMA has the following main functions:

- Regulate and develop the Capital Market, seek to develop and improve practices of parties involved in trading in securities.
- Protect investors in securities from unfair and unsound practices or practices involving fraud, deceit, cheating or manipulation, or any insider trading.
- Seek to achieve fairness, efficiency and transparency in securities transactions.
- Develop the procedures that would mitigate the risks associated with securities transactions.

[76] Decision R920/3 dated on 16/2/1402 h (1981??), based on the Council of Minister's Decision 1012 and pursuant to Royal Order 1064/8

- Regulate and monitor issuance of and trading in securities.
- Regulate and monitor the activities of parties that are under CMA regulation.
- Regulate and monitor the full disclosure of information regarding securities and issuers, the dealings of informed persons and investors, and define and make available information which the participants in the market should provide and disclose to shareholders and the public.

608. Article 6(a)(2) further provides the CMA with the power to issue the implementing regulations to the CML. As in the case of the other sectors described, violations of the CML or any implementing regulations issued by the CMA may be sanctioned through the application of administrative measures by the CMA and of criminal sanctions by the courts pursuant to Chapter 10 of the CML.).

609. CMA has six main departments: (1) Enforcement, (2) Corporate Finance, (3) Market Supervision, (4) Authorization and Inspection, (5) Research and Investor Awareness, and (6) General Administration. The Authorization and Inspection Department, through its Inspection and Compliance Section, is involved in examining the compliance of authorized persons with the regulation and circulars issued by CMA on AML/CFT. The section comprises 4 employees[77].

AML/CFT-Related Regulatory Instruments Issued by SAMA and CMA				
Instrument	**Issuing authority**	**1st date of issue**	**Date of last update**	**Scope**
AML Guidance Book	SAMA	1995		Local banks and licensed exchange institutions
AML/CFT Rules	SAMA	2003	2008	Local banks and licensed exchange institutions
Rules for opening accounts and general rules for operating them	SAMA	2001	2008	Local banks
AML/CFT Rules for insurance companies	SAMA	2009		Licensed insurance companies
Instructions for Money Exchangers	SAMA	2000 +2003 (circulars) then updated and inserted in RBME (2008)	-	Licensed exchange institutions

[77] One additional employee was hired in June 2009 as advised by the authorities following the onsite visit.

AML/CFT-Related Regulatory Instruments Issued by SAMA and CMA				
Instrument	**Issuing authority**	**1st date of issue**	**Date of last update**	**Scope**
AML/CFT Instructions for Financing Companies	SAMA	2008		Financing companies licensed by SAMA
Rules of regulatory monitoring	SAMA	2008		Local banks
Rules of review committees	SAMA	1995	-	Local banks
Guide on Financial Fraud	SAMA	1995	2008	Local banks
AML/CFT Rules for financial intermediary companies	CMA	2008		Financial Intermediary Companies
Authorized Persons Regulations	CMA	2005		Financial Intermediary Companies

Recommendation 23

610. The general supervisory powers are confirmed for purposes of the AMLS (Article 1) as "the governmental agency empowered to license, monitor or supervise financial and non-financial institutions." Pursuant to Article 6 of the AMLS, the covered entities are required to "comply with the instructions issued by the competent monitoring authority in this field". Accordingly, SAMA (for banks, money exchange businesses, insurance, and financing businesses) and the CMA (for securities business) are the relevant supervisory authorities for financial institutions, as appointed under the relevant supervisory laws and regulations (Banking Control Law, Ministerial Decision N.3/2149 dated 14/10/1406 implementing BCL, Decision on Money Exchange Businesses, Insurance Law, Decision on Financing Companies, and the Capital Market Law, respectively).

611. The AML IRs in Article 6-1 require the competent supervisory authorities to set and develop the appropriate regulatory instructions and rules to be applied against the crimes prescribed by the law, and the means and controls necessary to ensure compliance of financial and non-financial institutions with laws, rules and regulations to combat money laundering and financing of terrorism.

SAMA

612. In realizing its duties, SAMA issued AML/CFT regulations covering entities subject to its supervision. Banks and money exchange businesses are subject to the provisions of the Rules Governing Anti-Money Laundering & Combating Terrorist Financing (RBME) and the Rules Governing the Opening of Bank Accounts & General Operational Guidelines in SA (CDD Rules). The Financing and Insurance Companies AML/CFT regulations were introduced recently.

613. The previously mentioned regulations cover by large business relation acceptance conditions, customer identification process and customer due diligence procedures in addition to setting AML/CFT internal policies and compliance procedures among other things. The assessment team noticed that SAMA's approach in drafting such regulations was in a preventive and more detailed rule-based approach rather than risk-based approach.

614. In organizational terms, SAMA has established a special AML/CFT unit within its supervisory functions to address the development and interpretation of detailed AML/CFT rules for the financial sectors it supervises. The unit's 35 officers also assist in the work of the inspection department when conducting AML/CFT inspections.

615. At the time of the on-site visit, the Banking Supervision Department (Off-Site), which is involved in supervising banks, money exchange businesses and financing companies, had a staff of 70 employees. The Banking Inspection Department (On-site Supervision) is involved in the examination of banks, money exchange businesses and financing companies and had a staff of 150 employees. Of the 63 examiners, 42 of which work in a Local Banks Examination Unit, 10 in a Foreign Banks Examination Unit, 4 in a Money Exchangers Examinations Unit, and 7 in an Information System Examination Unit. The Insurance Control Department handles the licensing and examination of insurance companies with staff of more than 55 employees. After the onsite visit, the authorities confirmed to the team that SAMA is committed to hiring more staff on a regular basis and to focus on diversification of the available expertise in this regard.

616. The Insurance Control Department was established recently in 2006. SAMA is in the process of enhancing the role of this department as the insurance business is young and the expertise available in this field continues to develop. The authorities confirmed to the team that the work of this department is assisted by 2 consultants firms to enhance the expertise and the supervisory role played by this department in general and in the field of AML/CFT in particular.

CMA

617. As to the securities sector, CMA is empowered to prepare regulations and rules for the surveillance and supervision of entities subject to the provisions of Capital Market Law (CML) (Article 6.15). Also, CMA has the power to carry out inspections of the records or any other materials, whoever the holder may be, to determine whether the person concerned has violated, or is about to violate any provision of the CML, the Implementing Regulations or the rules issued by CMA.

618. For the purpose of conducting all investigations, which in the opinion of the CMA's Board are necessary for the enforcement of the provisions of the CML and other regulations and rules issued pursuant to this law, CMA employees designated by the board are empowered to summon witnesses, take evidence, and require the production of any books, papers, or other documents which the Authority deems relevant or material to its investigation (Article 5 of Capital market Law).

619. In realizing its duties, CMA issued "AML/CFT Rules for Authorized Persons" and the "Authorized Persons Regulation" covering activates subject to its supervision. These regulations cover in large business relation acceptance conditions, customer identification process and customer due diligence procedures in addition to AML/CFT internal policies and compliance procedures among other things.

620. CMA performs its AML/CFT regulatory and supervisor role through AML unit established within CMA. The team noticed that this unit was understaffed (4 employees only) with basic experience in AML/CFT. . After the onsite visit, the authorities confirmed to the team that the work of the AML unit is assisted by external consultants who are conducting the examination and surveillance role jointly. CMA is committed in enhancing the expertise available by hiring more staff on a regular basis.

621. Authorized persons and registered persons must comply with the Regulations and Rules applicable to them and must provide to the CMA without delay with any information, records or documents that the CMA may require for the purpose of administration of the Capital Market Law and its Implementing Regulations. The governing body and employees of an authorized person and a registered person must comply with any requirement issued by the CMA to appear to explain any matter or to assist in any enquiry relating to the administration of the Capital Market Law and its Implementing Regulations. (Article 3 of the authorized person's regulations).

Resources (Recommendation 30)

622. Both SAMA and the CMA have sufficient financial resources at their disposal to carry out their AML/CFT functions. As for the number of staff (human resources), SAMA has employed 35 staff at its unit dedicated to develop AML/CFT policy and procedures. It devotes considerable resources to the processing and routing of information requests from the SAFIU to the financial institutions subject to SAMA supervision. However, the small number of staff in CMA in general (23 employees) and in relation to AML/CFT in particular (4 employees) which requires CMA to increase the human recourses available to conduct examination. To address such situation, both agencies confirmed to the team their commitment to hiring more staff on a regular basis and to enhancing the expertise available to carry out the supervisory role played by them. SAMA and CMA are currently utilizing the expertise of external consultants to commence examination tasks. The legal basis of such reliance in the case of CMA, however, was not available to the assessment team.

623. SAMA has the ultimate responsibility for supervising the units subject to its supervision. According to Ministerial Decision No 3/2149 dated 14/10/1406 (1985) SAMA is empowered to conduct examination with direct access to data and information required from banks (Article 4 in implementation of Article 18 of the Banking Control Law). SAMA is able to enforce penalties and corrective actions as stipulated in Article 5 of the Ministerial Decision No. 3/2149 (in implementation of Article 22 of the Banking Control Law). Operational independence of SAMA is to some extent undermined due to the fact that in some circumstances sanctioning powers are shared with the Minister of Economy and the Council of Ministers. On the other hand, CMA's operational independence is secured (as discussed above).

624. Both SAMA and the CMA maintain high standards in relation to staff hiring qualifications. SAMA staff are required to sign an attestation/oath at the outset of their employment with SAMA, binding them to statutory confidentiality requirements and high professional standards. No information relating to the number of breaches (if any) and possible follow-up to breaches was available.

625. According to information provided by the authorities, supervisory staff has received training in AML/CFT matters at SAMA through the Institute of Banking and at the Naif University for Security Sciences. Furthermore, staffs participate in regional and international AML/CFT related programs, training sessions and conferences.

626. Since 2004, SAMA's AML/CFT unit staff has participated in AML/CFT specific training sessions. The table in Annex # shows training courses and conferences (2005-2008), related to the anti-money laundering and terrorism financing, which have been attended by SAMA's Banking Inspection Department's employees.

Number of sessions held by SAMA's Institute of Banking (IOB) on AML/CFT		
Year	**No of sessions**	**No of participants**
2004	24	351
2005	10	175
2006	6	102
2007	49	849
2008	50	864

627. On the other hand, no statistical information was available on the numbers of SAMA insurance inspectors trained in relation to AML/CFT.

628. CMA stated that one training course was planned and that they were in the process of introducing more training courses. Staff working for CMA's AML/CFT Unit received basic training as shown by the background information that was provided to the team. While the team takes into consideration that CMA was established in 2004 and acknowledges the actual performance of the assigned duties and functions in the last 2-3 years, and the fact that many AML/CFT tasks and regulations have only recently been introduced, the team also notes the increasing number of authorized persons being licensed by CMA. The number of staff and the resources available / training provided and the number of tasks and entities are at best not growing in the same pace. The low number of staff and the required expertise in this field still being at the infant stages also add to those concerns.

Recommendation 29

629. One of SAMA's objectives, according to Article (1) of its Charter, is to regulate commercial banks and money exchange businesses. Article (7) of the same Charter stipulates that SAMA's board of directors may make such rules and regulations as it may consider necessary and appropriate to the conduct of the work of the Agency in accordance with its charter.

630. Article 18 of the BCL and Article 4 of the Ministerial Decision 3/2149 empower SAMA to conduct an inspection of the books and accounts of any bank or money exchange business, either by the SAMA's own staff or by outside auditors assigned by SAMA. The examination of the bank's books and accounts should take place in the bank's premises. In such a case, the bank staff must produce all the required books and records of accounts and other documents in their custody or within their authority and must furnish any information they have relating to the bank. The MOF may exempt a bank form the provision of the law, upon approval by the Council of Ministers (Article 21 BCL).

631. The Minister of Finance and National Economy's Decision Regulating Money Changing Business of stipulates (Article 9) that SAMA may require any money exchange to provide it with any information or other data SAMA deems necessary for it to ensure the soundness of the business's

operations and implementation of the Decision. SAMA may carry out inspections of the books and accounts of any money exchange, as it deems necessary, either by SAMA's own staff or by auditors assigned by it. In such a case, it shall fall on the money exchange to furnish the books, statements and other documents and data requested.

632. The CICL gives SAMA the supervisory authority for the insurance sector. The law empowers SAMA through Article 2 to receive applications for establishing cooperative insurance and re-insurance companies and to supervise and regulate the activities of such business. Moreover, Article 8 authorizes SAMA to examine the records and accounts of any insurance or reinsurance company through its personnel or the auditors appointed by SAMA. The law gives SAMA through Article 11 the right to require the insurance and re-insurance companies to provide any information it sees necessary to realize the objectives of this law.

633. As to the CMA, being the regulator and licensing agency for investment activities providers within the Kingdom (Article 6-18 of Capital Market law), the investment activities that are licensed by CMA through the authorized persons include (AP Regulations Article 2)**:**

1. Dealing: a person deals in a security as principal or as agent, and dealing includes to sell, buy, manage the subscription or underwrite securities;
2. Arranging: a person introduces parties in relation to securities business, advises on corporate finance business or otherwise acts to bring about a deal in a security;
3. Managing: a person manages a security belonging to another person in circumstances involving the exercise of discretion;
4. Advising: a person advises a person on the merits of that person dealing in a security or exercising any right to deal conferred by a security; or
5. Custody: a person safeguards assets belonging to another person which include a security, or arranges for another person to do so, and custody includes taking the necessary administrative measures.

634. In all cases, the powers include licensing, application of fit and proper criteria, prudential reporting and ongoing monitoring (including through on-site inspections), and sanctioning. Both SAMA and the CMA are involved in the process of obtaining additional AML/CFT-related information from the supervised institutions on behalf of the FIU and law enforcement agencies.

635. The Ministerial Decision No 1/1566 dated 21/7/1420 (Article1-1) authorizes SAMA to grant licenses to leasing companies according to its rules and regulations and subject to the global surveillance requirements and the needs of the local economy. It entitles SAMA in Article 2-f to set field inspection and specialized testing procedures.

636. SAMA recently (January 2009) developed specific AML/CFT regulations for insurance companies. Regulations for leasing businesses (issued December 2008) have been developed pursuant to the Ministerial Decision that included the supervision of such companies under SAMA's jurisdiction.

637. SAMA and CMA have the power to conduct relevant on-site inspections. In relation to banks, SAMA conducts full-scope on-site inspections of banks on a three-year cycle, approximately. Inspections can be mandated to joint teams comprising staff from the ‘big four’ audit firms together with officers of SAMA, mainly from the Banking Inspection Department, which consists of 150 staff.

638. All full scope inspections include coverage of AML/CFT issues, including a review of the bank's AML/CFT policies and procedures for compliance with law and SAMA rules, and sample customer file examination and transaction testing. In addition, following the AMLS coming into force (2003 onwards), SAMA conducted a round of special purpose inspections focusing on AML/CFT issues. SAMA also conducts inspections of money exchange businesses, including coverage of AML/CFT matters. As insurance business develops in KSA, a similar program of on-site inspections is being recently applied.

639. The supervisory authorities have powers to require financial institutions to provide any information they may request and access books and related information for all units subject to SAMA's supervision. Supervisory authorities are also granted sufficient access to information in the fulfillment of their supervisory duties. SAMA (Article 11 of the Insurance Law, Article 17 of the Banking Control Law, and Article 9 of the Decision on Money Exchange Businesses) and the CMA (Article 18 of the CML) are explicitly authorized to access all information required to perform their supervisory functions. In addition, Article 6 of the AMLS (particularly Article 6-2 of the Implementing Regulations) empowers the supervisory authorities to set the means to ensure compliance with AML/CFT legal requirements. This should cover explicitly all units subject to SAMA's supervision as well as CMA's supervised units.

640. Neither SAMA nor the CMA need a court order to gain access to information in supervised financial institutions, as their respective rights to access of information are clearly set out in the relevant supervisory acts.

641. There have been no full scope examinations (or AML/CFT-related limited scope examination) carried by SAMA against the newly introduced instructions to cover the activities of money exchange businesses, insurance and leasing companies during the current examination cycle due to the novelty of such regulations. The authorities stated that such examination is planned for later this year (2009). . the authorities provided the team with more detailed tables covering the number of supervisory and inspection visits to banks, money exchange businesses and financing companies that covered different aspects of examination procedures both on full scope and targeted scope examination that cover AML/CFT in both tasks (see table below).

Table for the number of supervisory and inspectional visits by SAMA to banks and money exchange businesses licensed in the KSA from (2005 – 2009)

Type of Procedure	2005	2006	2007	2008	2009
Full-scope inspection for the banks and money exchangers licensed in the KSA, including verifying the AML/CFT requirements	6	6	21	27	18
Special inspection for the banks and money exchangers licensed in the KSA:					
a. Special test for verifying the compliance with the AML/CFT and KYC requirements	-	-	-	8	2
b. Special test for the security and safety procedures in the banks and the money exchangers	-	-	-	11	-
Inspectional visits to the licensed banks and money exchangers in the KSA	10	2	8	16	7

Table for the number of supervisory and inspectional visits by SAMA to banks and money exchange businesses licensed in the KSA from (2005 – 2009)					
Type of Procedure	**2005**	**2006**	**2007**	**2008**	**2009**
Inspectional visits to the branches of the local banks operating outside the KSA	-2	-	-	2	2
Inspectional visits to the main banks (mother company) which have licensed branches operating in the KSA.	-	-	-	3	5
Inspectional visits to the central banks supervising the main banks (mother company) which have licensed branches in the KSA.	-	-	-	2	6

Table for the number of inspectional visits paid by the SAMA from (2008 – 2009) to financing companies for verifying the compliance with the AML/CFT requirements	
2008	**2009**
0	2

Note: There are two financing companies in Saudi Arabia

642. Given that the domestic securities business is still in its infancy, though growing very quickly, the CMA is responding with modest on-site visits, focusing mainly on the relatively small number of authorized persons currently operational (106). Coverage includes the overseeing of the development of appropriate AML/CFT policies and internal controls, which is assisted by detailed AML/CFT requirements issued by the CMA. Currently, CMA's focus is still directed to the general licensing/regulation process with a plan to start a consistent supervisory process. No AML/CFT specific examinations have been conducted yet. The low number of CMA staff responsible for actual supervision and inspection would also call for more human recourses to be assigned. However, the authorities at a later stage (after the onsite visit), provided the team with the number of full scope examinations that were performed by CMA jointly with external consultants to cover the verification of compliance with AML requirements (see table below). While observing these facts, the team acknowledge the fact that CMA still needs to enhance its resources as mentioned above.

Table for the number of full-scope inspectional visits taken from (2006 – 2008) to authorized persons, paid by the CMA, covering the verification of the compliance with the AML requirements		
2006	**2007**	**2008**
49	52	68

643. Overall, based on the number of examination tasks and the fact that they do not cover all units subject to SAMA's supervision, the newly introduced regulations issued by SAMA, and the low level of corrective measures taken against noncompliant units as provided by SAMA during the onsite visit, the team was not able to ascertain the effectiveness of the supervisory role played by SAMA. However, after the onsite visit the authorities provided the team with more detailed tables covering the number of

supervisory and inspection visits to banks, money exchange businesses, and financing companies that covered different aspects of examination procedures both on full scope and targeted scope examination that covers AML/CFT in both tasks. The authorities provided the team with a list of corrective actions imposed by SAMA since 2006 that shows measures taken by SAMA before and after the onsite examinations related to a range of violations including AML/CFT related issues. As to CMA, the focus on licensing issues has affected the effectiveness of its supervision in relation to AML/CFT as noted above. While the team acknowledges the information recently provided by the authorities after the onsite visit with regards to the joint examination tasks, it still believes that CMA needs to enhance this process as noted above.

Recommendation 17

644. The AMLS and AML IRs apply to all financial sectors. Any violation of the provisions of the AMLS by financial institutions, as well as of any rules issued pursuant to the AMLS, may be sanctioned by the courts based on Article 18 of the AMLS. The said Article defines applicable criminal sanctions against financial institutions' employees.

645. Article 18 provides that without prejudice to other laws, a penalty of imprisonment of up to two years and/or a fine of up to SAR 500 000 (USD 133 000) can be imposed against a chairman or member of the board of directors of a financial and non-financial institution, its owners, managers, employees, authorized representatives, or any other person acting in such capacity in cases of violation of the obligations under Article 4 (customer due diligence), Article 5 (record keeping), Article 6 (supervisory measures), Article 7 (complex and unusually large or suspicious transactions), Article 8 (disclosure of information), Article 9 (prohibition of tipping off), and Article 10 (internal policies and controls).

646. Article 20 of the AMLS provides that with the exception of specific sanctions provided for in law, any person violating its provisions can be subject to imprisonment for a period not exceeding six months and/or a fine not exceeding SAR 100 000 (USD 27 000).

647. In addition to the sanctions pursuant to the AMLS above, violations of any regulations issued pursuant to Article 16 (3) of the Banking Control Law, including the AML/CFT Rules and the CDD Rules and the AML/CFT Rules for Financing Companies, may be sanctioned pursuant to Articles 22, 23, and 24 of the Banking Control Law.

648. Article 22 of BCL and Article 5 of Ministerial Decision No. 3/2149 provide for some administrative measures that may be applied directly by SAMA. However, some corrective measures, such as ordering the suspension or removal of any director or officer of an institution or a company (in cases other than a staff deliberately producing incorrect data or stating inaccurate information), and limiting or suspending credit granting or deposit acceptance are subject to the approval of the Minister of Finance and National Economy.

649. If SAMA is of the opinion that such proposals are not sufficient for their purpose or if the bank fails to implement an agreed or prescribed course of action within the stated period, the Minister of Finance and National Economy may, subject to the approval of the Council of Ministers, revoke the license of the said bank. The assessment team does not view having another government body in place that is ultimately responsible for deciding on harsher sanctions, *i.e.* revoking of a license, as a shortcoming. Furthermore, the assessment team believes that such penalties are fairly presented in the current regime.

650. Articles 23 and 24 define criminal sanctions that may only be imposed by a committee established pursuant to Article 25 of the Banking Control Law.

651. Administrative sanctions and actions can be applied by SAMA against insurance companies pursuant to the CICL. Article 19 include the following measures: appointing one or more consultants to provide the company with counseling in relation of the way it is conducting business; suspending any board member or employee proven to be responsible for a violation; preventing or limiting the company from admitting new underwriters, investors, or subscribers in any of its activities; and obliging the company to take any actions deemed necessary by SAMA.

652. If the company continues to breach the provision of the CICL or its IRs and does not comply with the actions taken by SAMA pursuant to this Article, in spite of the sanctions imposed thereupon, SAMA may *demand* the company to be wound up. It is noteworthy that those measures apply only if provisions of the Insurance Law or its IRs are violated (not the AMLS).

653. In addition, criminal sanctions may be applied by the courts pursuant to Article 21 Insurance Law.

654. Article 10 of Decision on Money Exchange Businesses No 3/920 dated 16/2/1402 AH and Article 5 of the Decision on Financing Companies No 1/1566 dated 21/7/1420 AH provide for sanctions listed in the BCL. In addition Decision 3/920 entitles SAMA to withdraw the license to conduct the money changing.

655. Equally, any violations of the APR or the RAP issued by the CMA may be sanctioned through administrative measures as well as criminal sanctions pursuant to Chapter 10 of the CML.

656. Chapter 10 of the CML (on Sanctions and Penalties) provides under Article 59 that if it appears to the Authority that any person has engaged, is engaging, or is about to engage in acts or practices constituting a violation of any provisions of this Law, or the regulations or rules issued by the Authority, or the regulations of the Exchange, the Authority shall have the right to bring a legal action before the Committee to seek an order for the appropriate sanction.

657. The sanctions include (1) Warning the person concerned, (2) Obliging the person concerned to cease or refrain from carrying out the act which is the subject of the suit, (3) Obliging the person concerned to take the necessary steps to avert the violation, or to take such necessary corrective steps to address the results of the violation, (4) Indemnifying the persons who have suffered damages as a consequence of a violation that has occurred, or obliging the violator to pay to the Authority's account the gains realized as a consequence of such violation, (5) Suspending the trading in the Security, (6) Barring the violating person from acting as a broker, portfolio manager or investment adviser for such period of time as is necessary for the safety of the market and the protection of investors, (7) Seizing and executing on property, (8) Travel ban, (9) Barring from working with companies whose Securities are traded on the Exchange.

658. Moreover, CMA may, in addition to taking the above-mentioned actions, request the Committee to impose a financial fine upon the persons responsible for an intentional violation of the provisions of this Law, its Implementing Regulations, and the rules of the CMA and the regulations of the Exchange. As an alternative to the foregoing, the Board may impose a financial fine upon any person responsible for the violation of this Law, its Implementing Regulations, and the rules of the CMA and the regulations of the Exchange.

659. The fine that the Committee or the Board can impose shall not be less than SAR 10 000 (USD 2 660) and shall not exceed SAR 100 000 (USD 26 600) for each violation committed by the defendant (Article 60 of CML).

660. The range of administrative sanctions in conjunction with the BCL and other related laws and the decision issued by the Minister of Finance and National Economy is broad and varies in the degree of implementation based on the 4 different types of business SAMA licenses and supervise.

661. As outlined above, Article 18 AMLS provides for adequate criminal sanctions against the chairperson or members of the board of directors of a covered entity, their owners, managers, employees, authorized representatives, or any other person acting in such capacity for violations of their institutions' respective obligations.

662. After the onsite visit, the authorities provided the team with an updated table of corrective measures imposed by SAMA on banks and money exchange businesses for different kinds of violations including in relation to AML/CFT related issues. Also, a sample of action plans to follow up with the examination reports were shared with the team. These show the follow-up procedures performed by the concerned units in correcting the violations and the follow-up process demonstrated by SAMA to verify such correction plan

Table for procedures imposed by the SAMA from (2004 – 2009) against a number of banks and money exchange businesses as a result of their non-compliance with some instructions issued by SAMA, including the AML/CFT-related instructions

Type of Procedure	2004	2005	2006	2007	2008	2009
Requesting regular reports from the banks or money exchangers on the measures they take regarding correcting the instructions obtained through the inspectional visits.	8	6	6	21	27	18
Orders to comply with special instructions, accompanied with daily financial fines for non-compliance	-	10	7	13	6	8
Financial fines as a result of committed violations	61	54	199	190	110	427
Seclusion or banning from employment within the sector	-	4	-	-	-	-
Replacing or restricting the powers of the directors or the members of the Board of Directors or the cadres	-	-	-	-	-	-
Imposing guarding	-	-	-	-	-	-
Suspending or cancelling licenses	-	2	-	-	3	-
Closing branches	-	-	1	2	-	-
Warning to withdrawing the license	-	-	6	7	-	-
Suspending or banning from transferring money	1	-	-	-	-	-

Table for procedures imposed by the SAMA from (2004 – 2009) against a number of banks and money exchange businesses as a result of their non-compliance with some instructions issued by SAMA, including the AML/CFT-related instructions						
Type of Procedure	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**
Written Warnings	-	-	-	-	6	1
Other (orders for complying with special instructions)	15	20	4	-	6	-

Table for procedures imposed by the SAMA from (2004 – 2009) against a number of banks and money exchange businesses as a result of AMLCFT related non-compliance incidents							
Type of sanction/procedure	2004	2005	2006	2007	2008	2009	Nature of noncompliance/violation
Order to banks/money exchange businesses to submit regular periodic reports regarding the corrective actions taken by them to ensure compliance of the issues highlighted in inspection reports	4	2	2	12	18	7	Weaknesses in compliance with AMLCFT instructions noticed on examination visits
Suspended or banned from employment within the sector	0	4	0	0	0	0	Fraud/falsification of transfer instruction
Warnings to withdraw the license	0	0	2	2	0	0	KYC requirements as per rules were not implemented in letter and spirit
Suspended or banned from transferring money	1	0	0	0	0	0	Non-compliance with some of AML requirements while transferring funds
Written warnings	0	0	0	0	2	0	Inadequate training and weaknesses in management of AML unit of the money exchange business
Other (orders to comply with special instructions)	3	0	0	0	0	0	Miscellaneous

663. According to CMA's officials, CMA revoked licenses in incidents that were not AML/CFT-related (see table below). While the range of sanctions available to CMA both in the AMLS and Capital Market Law is broad and complex., the team has concerns about CMA's ability to apply such sanctions.

The limited number of staff and the lack of expertise available to perform on-site and off-site examination to assess the compliance of authorized persons with related laws and regulations also has an effect on the ability to enforce sanctions. The fact that CMA performed joint examination tasks with external consultants that was provided to the team after the onsite visit still shows the need for CMA to enhance its recourses.

Table for procedures taken by the Capital Market Authority (CMA) from (2006 – 2009) against authorized persons for different violations			
Procedure	**2006**	**2007**	**2008**
Withdrawal of the License	2	2	4
Resolutions issued by the for the CMA Council's violations	27	12	19

664. The effectiveness of the corrective measures imposed by CMA is still a concern. The overall number of sanctions imposed by SAMA shows a satisfactory level of the overall effectiveness of the (prudential as opposed to AML/CFT-related) corrective measures, however, the absence of specific AML/CFT-related sanctions does not give a clear picture of such process within that specific aspect. As outlined above, there have been no incidents where criminal sanctions were imposed or proceedings related thereto were started, the team was not able to clearly assess the effectiveness of the AML/CFT-related sanctioning system applied by CMA.

Recommendation 23 – Market Entry

665. According to Article 2 of the BCL, (natural or legal) persons that are not licensed in accordance with the provisions of this Law shall not carry out any of the banking businesses. Article 3-3 adds that founders and members of the board of directors shall be persons of good reputation. Article 12 contains express conditions for the qualifications that have to be met before a person may be appointed director of a bank.

666. According to Circular No. 8733/2A-/138 (requirements for hiring senior posts in banks operating in KSA, which covers in detail the fit and proper procedures applied by SAMA on board members and directors appointed by banks. SAMA uses detailed fit and proper forms in such process. Such forms detail extensive analysis of the founders and the fit and proper checks of directors and executive officers

667. The Decision of the Minister of Finance and National Economy regulating money exchange businesses (Article 4) stipulates that the applicant to practice this business should be a Saudi national of good conduct and behavior and at least 30 years old. Neither the insurance companies nor the financing business applicants are covered by the related laws vis-à-vis this requirement Article 5-c stipulates that Money Changers shall not change the composition and the ownership of capital without prior written approval by SAMA.

668. According to the CICL (law No. 32/M) SAMA's approval is needed before the selection of the board of directors of insurance companies (article 6) and for the mergers and acquisitions of such

companies (article 9). In this regard, SAMA has fit and proper forms that detail extensive analysis of the founders and the fit and proper checks of directors and executive officers.

669. In addition to the above, the authorities indicated that most of the financial institutions in Saudi Arabia are listed companies governed by the CMA rules. These rules require that if any share holder intends to increase his holdings by more than 5%, (under Article 30(a) of rules issued by Royal Decree # M/30 dated 2/6/1424H), the company has to publicly disclose the name of the shareholder and other relevant information. In case a shareholder acquires shares holding more than 10% of the total, then it shall require CMA approval under Article 30 (f) of the same rules. The CMA allows approval for any acquisition more than 10% after completing due diligence and fit and proper test of the intended buyer. Besides, a shareholder, to become a director, chairman or to have any position in the top management, has to go through the fit and proper of the respective regulators. SAMA confirmed to the team, that any acquisitions or mergers for the financial units subject to its supervision that are publicly traded will be assessed jointly with CMA.

670. On the other hand, CMA has a complex requirement for the approval of the founders or controlling shareholders of the authorized persons as well as ongoing fit and proper procedures for the established authorized persons or applicant's employees, officers or agents. Relevant provisions can be found in Articles 6, 9 and 13 of the RAP . Such procedures include among other things assessing the skills, experience, competence and integrity of the said parties. CMA has posted on its website the forms related to licensing and registering the authorized persons.

671. The team was not able to assess the adequacy of CMA's regime on the listed financial units for any changes in the ownership as no information was shared on the number of applications turned down due to not meeting the standards of these criteria. In addition, it was not clear how CMA could crosscheck the accuracy of such information from independent sources especially for non-Saudi nationals.

672. Concerning licensing/registering MVT service providers, currency exchange and remittance services are restricted in SA to banks and licensed money exchange businesses. Under the powers delegated by the Minister for Finance and National Economy (Decision on Money Exchange Businesses assigning responsibility to SAMA), two types of licenses for money exchange businesses may be issued by SAMA: type A authorizes the provision of both currency exchange and money remittance services, while type B license holders are restricted only to currency exchange.

Ongoing Supervision and Monitoring – Recommendations 23 & 32

673. As stated above, SAMA is the supervisor for banks, money exchange businesses, insurance companies and financing companies. According to SAMA officials, the examination cycle for all supervised entities traditionally (*i.e.* before insurance and leasing companies were added to the scope of SAMA supervision) took 3 years in general. It should be taken into consideration that the inspection of insurance companies has yet to complete its first round SAMA adopts a full scope examination approach rather than a risk-based approach. In addition, according to SAMA officials they conduct annual unannounced examination visits to randomly chosen units subject to supervision that range from 1-2 weeks. These visits carry different aspects of tasks including AML/CFT issues.

674. The current examination cycle (on all units subject to SAMA's supervision) started on the fourth quarter of 2007 and covered banks (foreign bank branches included), exchange, insurance and financing

companies (see table above). The typical examination mission will range from a few weeks to 3-4 months, in which a part of the examination will cover the review of AML/CFT procedures and the adherence of the unit subject to examination with the related AMLS, its IRs and the applicable regulatory instruments issued by SAMA.

675. As mentioned above, SAMA may utilize the expertise of auditing companies to lead the examination teams. The audit firms draft a supervisory report, based on a template that differs for each audit firm; however, no information was given to the team on the role of the outsourced auditors, if any, in the process of performing the examinations. SAMA officials confirmed to the team that a number of specific examination tasks were performed on AML/CFT related matters during the current examination plan. In 2008, SAMA completed a cycle of thorough examination programs for all banks in the KSA. The audits included compliance with AML/CFT procedures and rules. In this respect, the team was advised that no major AML/CFT-related deficiencies have been reported, and accordingly no sanctions have been imposed. In addition, inspection teams in SAMA have reportedly conducted AML/CFT examinations with limited scope since 1999. In the course of these audits, banks received directions concerning the results found by inspection teams and their directives to take the necessary corrective measures.

676. During the onsite visit, the assessment team was able to evaluate a sample of full-scope inspection reports, as prepared by the audit firms. The sample was based on a selection by SAMA staff and contained reports on all kinds of inspections. In all cases, the supervisory reports indicated a low level of compliance by FIs and a low level of corrective measures taken by SAMA. No corrective measures related to AML/CFT issues were taken by SAMA during the current examination cycle based on the sample provided to the team. However, after the onsite visit, the authorities provided the team with more details on corrective measures taken by SAMA (see table above). That table covers a range of violations including AML/CFT related violations and a sample of corrective plan introduced by the violating units and the follow-up mechanism introduced by SAMA.

677. In July 2003, SAMA instructed all banks to assign their external auditors and to prepare reports about their compliance with the AML/CFT rules. SAMA received those reports in August 2003.

678. CMA conducted also a number of onsite examinations and inspections since it commenced its work. After the onsite visit, CMA provided the team with a table showing the onsite examination visits conducted since 2006 (see table above).The sanctions imposed by CMA ranged from license withdrawal to other unspecified penalties on various non compliance related matters with no specifics on AML/CFT related sanctions. CMA officials stated that so far no deficiencies had been identified in relation to AML/CFT.

679. While the team understands that the AML/CFT regulations for insurance companies (and the financing companies in the foreseeable future) were only recently established, and the novelty of the AP's sector, it believes that both SAMA and CMA have to take more steps in covering all units subject to supervision (CMA in particular) and SAMA has to cover the newly introduced regulations issued as described above.

680. Both SAMA and the CMA indicated that they maintain statistics and other records of supervisory matters, including those relevant to AML/CFT, such as number of inspections conducted, sanctions applied, and information requests processed on behalf of the SAFIU. The team found that such statistics are basically the ones contained in the inspections reports prepared upon finalizing inspections on banks

and money exchange businesses. No specific statistics are generated or kept in relation to the results of those inspections. Moreover, it was not clear to the team how the available data are utilized in spotting major common deficiencies or shortcomings that need to be addressed at sector-level by the concerned supervisory authority.

Recommendation 25

681. AML/CFT guidelines are embedded in the current set of rules that were issued by SAMA and CMA. Both provided basic background information in their AML/CFT Rules, which need to be further developed for banks and money exchange businesses, insurance companies, leasing companies and APs to include a description of ML and FT techniques and methods and additional measures that these institutions could take to ensure that their AML/CFT measures are effective.

682. Guidance provided to the capital market, insurance, and financing sectors has to date been relatively limited resulting in a low level of awareness of potential pitfalls. The evaluation team found, for example, that finance companies have an extremely limited understanding of potential AML/CFT abuse of their sector, believing themselves to be exempt from concern by virtue of the fact that they do not conduct cash-based transactions.

3.10.2 Recommendations and Comments

Recommendation 17

- The implementation level of these sanctions should be improved and corrective actions to be taken to include all types of units subject to supervision by SAMA and CMA.

Recommendation 23

- Fit and proper criteria are to be tested against real cases scenarios to check the adequacy of such criteria on existing financial units (in relation to ownership) and with regards to non-Saudi nationals.
- SAMA should apply the fit and proper requirements on financing l companies
- Empower the Insurance Control Department in SAMA with adequate manpower and expertise to carry on the assigned duties as the insurance field continues to grow.
- Provide CMA with proper enhanced training for its staff to perform the duties assigned to them.
- Empower AML unit within CMA with adequate number of examiners with AML/CFT expertise to conduct related examination tasks as the number of APs is growing.

Recommendation 25

683. The current AML/CFT guidelines should be enhanced to include more clear description of business-related methods and to cover explicitly all types of financial institutions.

Recommendation 29

- Enhance the expertise of the examiners especially in the field of AML/CFT with regards to insurance and financing companies.
- Introduce more frequent on-site AML/CFT related examination missions by SAMA to cover banks, money exchange businesses, insurance and leasing companies.
- Increase the number of AML/CFT related examination assignment has to be concluded by CMA for all licensed units. CMA should design a more frequent enhanced examination process carried by well trained CMA's AML unit staff. .

3.10.3 Compliance with Recommendations 23, 30, 29, 17 & 25

	Rating	Summary of factors relevant to s.2.10 underlying overall rating
R.17	**LC**	• Low levels of corrective measures applied by both SAMA and CMA.
R.23	**LC**	• Fit and proper procedures have not been tested against real case scenarios for existing financial institutions (in relation to ownership) and with regards to non-Saudi nationals. • Low number of human resources available for insurance and authorized persons supervision. • Lack of adequate training for CMA's AML unit staff. • Low number of AML/CFT related examination on authorized persons.
R.25	**PC**	• Guidance issued by supervisory authorities is not comprehensive and not industry specific.
R.29	**LC**	• No adequate number of staff or expertise to carry out examination within Insurance Control Unit in SAMA or CMA Low number of AML/CFT related examination tasks performed by SAMA and CMA.

3.11 Money or value transfer services (SR.VI)

3.11.1 Description and Analysis (summary)

Registration/Licensing Authorities

684. Money remittance services in the Kingdom are provided either by banks (1409 branches) or remittance centers (260 branches) as well as money exchange businesses (category A). The regulatory regime for the banks and licensed money exchange businesses has been described in previous sections of this report dealing with the financial institutions. The licensed category A money exchange businesses offering such services in the Kingdom consists of 6 companies, out of which 4 operate MVTs (as per what authorities stated). These have 13 branches in total, covering six major cities. There are seven million immigrants (27 percent) in Saudi Arabia with a population of 26 million and Saudi Arabia is the second largest remittance market in the world with $17 billion remitted in 2008, accounting for 7% of global

expatriates' remittances[78]. In addition, nearly 27% of Saudi Arabia's population is foreign-born, which amplifies the demand for money transfer services due to the growing number of Saudis studying, travelling and working outside the country. Lately, the MVT business in KSA is evolving at a fast pace, moving into a faster, simplified and convenient service: Faster because it can be done without standing in a queue, simplified because it takes one-time registration to obtain an ATM/membership cash loadable cards then operated with button push, and convenient because 24/7, no bank account needed, service through ATMs Kingdom-wide and even through phone and online[79].

685. The considerable demand for money remittance service does not look to be satisfied so far with the licensed venture of this lucrative business, which suggests the possible existence of underground transfer activities to accommodate these needs[80]. However, Saudi authorities seem to have a clear idea on the involvement of ethnic groups operating such networks as well as their Saudi counterparts. In this context, authorities have exerted commendable efforts since 1975 to dismantle illegal remittance systems and sanction its operators (see table in VI.5). Authorities seem to be also aware of how these networks operate and how they make transaction settlements, therefore, Article 5.1.3 of the RBME is envisaged to address this issue throughout banking accounts and transaction monitoring by banks and money exchange businesses, and stipulates reporting requirements to spot agents of this network.

686. The money transfer activity is considered among the bank activities that require a license from SAMA to be carried out, as the designated authority for regulation and monitoring of the bank activity in the KSA according to Article (2) of the Banking Control Law issued by virtue of the Royal Decree (No. M/5) issued on 22.02.1386 AH and Article (1) of the resolution of the Minister of Finance (No. 3/920) issued on 16.02.1402 AH about organizing the activities of the money exchange businesses.

687. Being the designated authority for organizing and monitoring of bank activities, SAMA issued instructions for banks and money exchange businesses. Additional instructions were issued by SAMA to organize the activities of the money transfer services. SAMA periodically verifies the compliance of bank institutions including money transfer companies, insurance companies, and leasing companies, with the stipulated requirements of the relevant laws, regulations, instructions, and rules including the requirements related to AML/CFT through conducting on-site and office examination. Section 3.10 (Recommendation 23) contains details concerning the analysis of this oversight.

688. The designation of SAMA is appropriate for licensing MVT services. SAMA maintains a current list of the names and addresses of licensed MVT service operators and is held responsible for ensuring compliance with licensing requirements. SAMA reported sanctioning money exchange businesses for conducting illegal operations, which suggests that these might have been operating remittances without license or dealing with businesses belonging to a non-regulated network for this purpose.

Transposition of FATF Recommendations

689. As indicated above, SAMA is responsible for the licensing (with other parties), regulation, and supervision of MVT service operators which, in the Kingdom, operate under banks and exchange houses under category A. MVT service operators are covered by and subject to the obligations imposed by the

[78] IPR Strategic Business Information Database, January 30, 2007.
[79] 2009 Al Bawaba (www.albawaba.com), July 4, 2009.
[80] http://www.saudigazette.com.sa/index.cfm?method=home.regcon&contentID=2010022164053

AMLS and IRs (Articles 4 and 6) as well as the RBME. SAMA's RBME establish the requirements for MVTs to among other things: (i) identify the customers; (ii) report suspicious transactions to the FIU; (iii) maintain records for five years; and (iv) establish policies, procedures, and internal controls to prevent money laundering. Accordingly, the level of compatibility of the instruments governing MVTs with the relevant scope of FATF Recommendations is the same as described for the banking sector.

690. As for the licensed sector, implementation of Recommendations 5, 6, 7, 9, 10, 13, 15, and 22 in the MVT sector have the same deficiencies as those that apply to banks and which are described earlier in Section 3 of this report.

Compliance monitoring

691. When transferring funds abroad, the MVTs batch the outgoing requests for transfers at the end of the day and use their bank accounts to conduct the transfers. The settlement of transactions takes place through disbursements of funds to the recipients abroad also through banking institutions as well as other MVT service providers where relationships are established. Article 5.1.3 of the AML/CFT Rules set several requirements for banks and money exchange businesses to monitor transfers and relationships for the purpose of detecting and reporting alternative remittance networks. This system consists of requirements that should theoretically help deterring ML/TF operations and be in line with some FATF Recommendations.

692. As indicated above, MVTs in SA are subject to the same obligations banking institutions are subject to (by law, regulations, and rules); therefore, the mechanisms applied for monitoring banks' activities and ensuring their compliance with the FATF Recommendations (by SAMA) are similar to those used for banks.

693. It appears that shortcomings identified under Recommendation 17 (sanctions) and 23 (monitoring and supervision) apply equally to this Special Recommendation.

List of Agents

694. Exchange houses in the Kingdom do not have agents in the sense explained in the Interpretative Note of SR.VII[81] (only branches).

Sanctions

695. Because MVTs fall within the jurisdiction and oversight of SAMA, these institutions are also subject to the same sa*nctions as* other financial institutions. SAMA had temporarily closed exchange companies conducting transactions through an unauthorized business. Corrective action in such instances included removal of the company officials. A number of sanctions were issued against individuals who provided remittance services without a license as outlined in the table below:

[81] According to the IN, an *agent* is any person who provides money or value transfer service under the direction of or by contract with a legally registered or licensed remitter (for example, licensees, franchisees, concessionaires).

Year	No.	Individual citizens	Individual residents
2004	23	7	16
2005	15	5	10
2006	31	7	24
2007	64	24	40
2008	20	3	17

696. The authorities provided a sample of decisions related to violations committed by money exchange businesses. These decisions included sanctions ranging from simple warning up to license revoking. However, these violations mostly relate to breach of accounting or branch licensing rules.

697. It appeared that authorities did not use their powers to sanction money exchange businesses not abiding by AML/CFT requirements.

Additional elements - Best Practices Paper for SR VI

698. With respect to existing Laws, Regulations and rules mentioned above, it appears that this legal framework meets some of the elements stipulated within the Best Practices Paper for SR.VI. Matching areas can be identified for Licensing/Registration (under (a), (c) and (d) in the BPP) and for AML IRs (under (a) and (c)).

3.11.2 Recommendations and Comments

699. See Recommendations 5, 6, 7, 8, 9, 11, 13, 15, 17, 21 and 23.

3.11.3 Compliance with Special Recommendation VI

	Rating	Summary of factors underlying rating
SR.VI	**LC**	• Deficiencies identified and ineffective implementation in relation to obligations required under other Recommendations (5, 6, 7, 8, 9, 11, 13, 15, 17, 21 and 23) affect the rating of compliance with SR.VI.

4. PREVENTIVE MEASURES – DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

4.1 Customer due diligence and record-keeping (R.12)

(Applying R.5, 6, and 8 to 11)

DNFBPs and authorized activities

700. Most of the businesses and professions designated by the FATF exist in SA: real estate agents, dealers in precious metals, dealers in precious stones, lawyers and legal advisers, accountants, and TCSPs.

701. It appeared that there exists a parallel sector of unregistered brokers dealing in real-estate business. Authorities stated that the TCSP activities are mainly conducted by lawyers and accountants. According to the authorized person's regulations, it is prohibited to manage client money, securities or other assets without getting a license from the CMA. However, when these professionals buy or sell real estate, manage bank, savings or securities accounts, organize contribution for the creation, operation or management of companies and create, operate or manage legal persons and buy and sell business entities, the MOCI is competent to supervise them and ensure the proper implementation of preventive measures.

702. The remaining categories of designated businesses and professions (DNFBPs) as defined by the FATF do not operate in the Kingdom:

- Casinos are prohibited;
- Notaries are civil servants who may only be employed by the MOJ and, while they do take identification details of persons appearing before them and do maintain records of that identification, they do not fall under the FATF definition of DNFBPs as they do not prepare for or engage in any financial transactions for clients.

Scope

703. The AMLS applies to "financial and non-financial institutions," which are defined under Article 1 as "any institution in the Kingdom undertaking one or more of the financial, commercial, or economic activities such as banks, money-exchange, investment and insurance companies, commercial companies, sole proprietorships, vocational activities or any other similar activity specified by the Implementing Regulation of this Law".

704. Article 1.1 of the AML IRs expounds on this definition by listing the "activities". These cover various financial transactions and include "real estate transactions; dealing in precious metals, precious stones or rare commodities like antiques; law practice; trust and company services, and accounting and auditing". The provisions of the AMLS and IRs include within their scope all the DNFBPs that operate in the Kingdom, *i.e.*, real estate agents, dealers in precious metals, dealers in precious stones, lawyers and legal advisers, accountants, and TCSPs.

705. Hereunder is a table showing the existing types of DNFBPs in SA, their supervisors, and license-issuers:

FATF Designated non Financial Businesses and Professions			
Sector	**Designated in AMLS**	**Registered**	**Supervised**
Casinos	Not applicable (casinos are illegal)		
Internet casinos	Not applicable (internet casinos are illegal)		
Real estate agents	Yes 2810 companies	Only in the company registry	MOCI (not for AML/CFT purposes)
Dealers in precious metals and stones	Yes 5407 licenses - 03.03.2009	Only in the company register	MOCI (not for AML/CFT purposes)
Lawyers	Yes	MOJ register	MOJ (not for AML/CFT

FATF Designated non Financial Businesses and Professions			
Sector	**Designated in AMLS**	**Registered**	**Supervised**
	1200 offices		purposes)
Notaries	Not applicable (a notary is a public office of the MOJ)		
Accountants	Yes 24 companies and 106 offices	MOCI register	SOCPA (SRO) (not for AML/CFT purposes)
Company Service Providers	Partially	Partially	Partially
Trust Service Providers	Partially	Partially	Partially

Regulatory obligations

706. The provisions of the AMLS IRs, and in particular those dealing with the preventive measures and the monitoring of their implementation, apply equally to financial institutions and to the DNFBPs. AML/CFT provisions, notably on CDD and reporting, are to be applied by DNFBPs to all their clients/ activities/ dealings, since measures applicability has not been restricted to:

- Transactions for a client concerning the buying and the selling of real estate for Real estate agents.
- Cash transaction with a customer equal to or above USD/EUR 15000 for Dealers in precious metals and dealers in precious stones.
- Buying or selling of real estate, managing bank, savings or securities accounts, organizing contribution for the creation, operating or management of companies and creating, operating or managing legal persons and buying and selling of business entities for lawyers and legal advisers, accountants, and TCSPs.

707. The MOCI and MOJ issued additional circulars on AML/CFT procedures (see Table below) that request the DNFBPs, regardless of their activities, to identify their clients, verify the transactions, keep records, and establish internal monitoring and training programs. These regulations mirror the requirements made in the financial sector.

708. Under the current AML/CFT framework, the CDD measures provided for under the AMLS apply to lawyers, accountants, and auditors in all circumstances, regardless of the activity carried out.

<u>General provisions:</u>

CDD and Recordkeeping for DNFBPs:

- AMLS Article 4 and IRs Articles 4.1, 4.2, 4.3, 4.4, 8

STR Reporting and internal control for DNFBPs:

- AMLS Article 7 and implementing regulation Articles 7.1 to 7.3
- AMLS Articles 25 and 10 and implementing regulation Article 10.1-10.6

Supervision/regulation for DNFBPs and establishing guidelines and providing feedback:

- Article 6 and implementing regulation Article 6.1, 6.2

Effectiveness of the existing AML/CFT regime for DNFBPs

Data compiled by SAFIU on received STRs (years 2006-2007-2008): poor reporting by DNFBPs.					
Year	**Accounting firms**	**Precious metals**	**DNFBPs Total**	**Financial institutions**	**Total STRs**
2006	1	4	5	316	405
2007	3	8	11	566	743
2008	2	6	8	787	1019

4.1.1 Description and Analysis

Applying Recommendation 5

709. As indicated above, the DNFBPs operating in SA share the general legal and regulatory framework in relation to their AML/CFT obligations with financial institutions. Detailed description and analysis of that framework is discussed in Section 3 of this report. Hereunder, description and analysis of the distinctive instruments issued for DNFBPs are outlined.

710. In addition, MOCI circular No. 1312/11 dated 15/5/1422 H emphasizes basic requirements in relation to the verification of the identity (of natural or legal persons) upon the implementation of all commercial operations (especially operations of great value). It also reinforces documentation of ID data of individuals and representatives and beneficial owners; record keeping; exclusion of anonymous clients and use of fictitious names and aliases; verification of the legal relation between the principals or their representatives/ agents acting on their behalf; verification of proxy powers; and ceasing to do business if identification procedures are incomplete.

711. In 2004, MOCI also issued "A Guide for Combating Money Laundering" for commercial entities and DNFBPs including, among others, provisions on CDD measures and record keeping. However, these provisions are not considered as mandatory requirements.

712. With respect to the regulatory framework, the following deficiencies could be noted:

- DNFBPs are not required to understand the ownership and control structure of a customer that is a legal person or legal arrangement.
- DNFBPs are not required to obtain information on the purpose and intended nature of the business relationship.
- Ongoing due diligence requirement is not provided explicitly by primary or secondary legislation.

- DNFBPs are not required to scrutiny transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the entity's knowledge of the customer, their business and risk profile, and where necessary, the source of funds.

- DNFBPs are not required to consider making a suspicious transaction report whereas required CDD measures could not be applied.

- DNFBPs are not required to terminate the business relationship and consider making a suspicious transaction report in case required CDD measures could not be applied to existing customers and to cases whereby the institution has doubts about the veracity or adequacy of previously obtained customer identification data. In such instances, it is also not required to consider making a suspicious transaction report.

- DNFBPs are not required to apply CDD requirements to existing customers on the basis of materiality and risk and to conduct due diligence on such existing relationships at appropriate times.

713. With respect to implementation and effectiveness, it appeared that for real estate agents and dealers in precious metals and dealers in precious stones, there was no adequate compliance with AML/CFT requirements (Measures are mainly limited to basic customer identification).

714. As for lawyers and legal advisers and accountants and auditors, there was no compliance with AML/CFT requirements. Concerning TCSPs, it appeared that there is no identified sector.

*715. Applying recommendations 6, 8, 9, 10 and 11*Article 7 of the AMLS requires non-financial institutions to maintain indicators of suspicion of ML or TF in order to "pay special attention to unusual patterns of transactions that have no apparent or visible economic or lawful purpose". Therefore, the law establishes monitoring for unusual transactions as a means for crime detection only (refer to analysis in Rec. 11 under Section 3.6 of this report). However, MOCI circular No. 1312/11 establishes (under thirdly (1)) the requirement to ''ascertain large-scale and complex transactions that would seem to be lacking any connection or relevance to any economic activity or licit objective''.

716. With respect to the regulatory framework, the following deficiencies could be noted:

- There are no enforceable obligations with regard to Politically Exposed Persons for DNFBPs.

- DNFBPs are not required to include specific and effective CDD procedures in their measures for managing the risks related to non-face to face customers.

- There are no enforceable obligations with regard to introduced business for DNFBPs (Business relationships between real estate companies and possible mortgage providers).

- Lawyers and TCSPs are not required to pay special attention to unusual patterns of transactions that have no apparent or visible economic or lawful purpose and to examine as far as possible the background and purpose of these. DNFBPs are not required to set forth in writing the examination of the background and purpose of complex, unusual large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose; DNFBPs are not required to keep such findings available for competent authorities and auditors for at least five years.

717. With respect to implementation and effectiveness, it appeared that some DNFBPs apply record keeping requirements only.

4.1.2 Recommendations and Comments

718. With respect to DNFBPs, it is recommended to:

- Amend the AMLS or IRs to provide the Ongoing due diligence requirement.
- Require the following, through law, regulation or other enforceable rules:
  - To understand the ownership and control structure of a customer that is a legal person or legal arrangement.
  - To obtain information on the purpose and intended nature of the business relationship.
  - To scrutiny transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the entity's knowledge of the customer, their business and risk profile, and where necessary, the source of funds.
  - To consider making a suspicious transaction report whereas required CDD measures could not be applied.
  - To terminate the business relationship and consider making a suspicious transaction report in case required CDD measures could not be applied to existing customers and to cases whereby the institution has doubts about the veracity or adequacy of previously obtained customer identification data. In such instances, it should also be required to consider making a suspicious transaction report.
  - To apply CDD requirements to existing customers on the basis of materiality and risk and to conduct due diligence on such existing relationships at appropriate times.
  - To include specific and effective CDD procedures in their measures for managing the risks related to non-face to face customers.
  - To require from Lawyers and TCSPs to pay special attention to unusual patterns of transactions that have no apparent or visible economic or lawful purpose and to examine as far as possible the background and purpose of these.
  - DNFBPs should be required to set forth in writing the examination of the background and purpose of complex, unusual large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose; DNFBPs should be also required to keep such findings available for competent authorities and auditors for at least five years.
- Issue through law, regulation or other enforceable rules:
  - Enforceable obligations with regard to Politically Exposed Persons.
  - Enforceable obligations with regard to introduced business.

- Ensure proper and efficient implementation.

4.1.3 Compliance with Recommendation 12

	Rating	Summary of factors relevant to s.4.1 underlying overall rating
R.12	**NC**	• DNFBPs are not required to understand the ownership and control structure of a customer that is a legal person or legal arrangement. • DNFBPs are not required to obtain information on the purpose and intended nature of the business relationship. • Ongoing due diligence requirement is not provided explicitly by primary or secondary legislation. • DNFBPs are not required to scrutiny transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the entity's knowledge of the customer, their business and risk profile, and where necessary, the source of funds. • DNFBPs are not required to consider making a suspicious transaction report whereas required CDD measures could not be applied. • DNFBPs are not required to terminate the business relationship and consider making a suspicious transaction report in case required CDD measures could not be applied to existing customers and to cases whereby the institution has doubts about the veracity or adequacy of previously obtained customer identification data. In such instances, it is also not required to consider making a suspicious transaction report. • DNFBPs are not required to apply CDD requirements to existing customers on the basis of materiality and risk and to conduct due diligence on such existing relationships at appropriate times. • There are no enforceable obligations with regard to Politically Exposed Persons. • DNFBPs are not required to include specific and effective CDD procedures in their measures for managing the risks related to non-face to face customers. • There are no enforceable obligations with regard to introduced business. • Lawyers and TCSPs are not required to pay special attention to unusual patterns of transactions that have no apparent or visible economic or lawful purpose and to examine as far as possible the background and purpose of these. • DNFBPs are not required to set forth in writing the examination of the background and purpose of complex, unusual large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose; DNFBPs are also not required to keep such findings available for competent authorities and auditors for at least five years. • Inadequate implementation, reporting and supervision.

4.2 Suspicious transaction reporting (R.16)

(applying R.13 to 15 & 21)

4.2.1 Description and Analysis

719. The AMLS applies to all financial and non-financial institutions. The definition of non-financial institutions encompasses any institution undertaking commercial or economic activities. Real estate agents, dealers in precious metals and stones, lawyers and legal advisers, and accountants are thereby subject to all requirements of the AMLS. As such, the requirement for DNFBPs to file STRs is established in Article 7 and that to establish internal controls is in Articles 6 and 10. Article 9 of the AMLS prohibits "tipping off"

for non-financial as well as financial institutions, and Article 25 establishes exemption from criminal, civil or administrative liability arising from the performance of duties under the AMLS for chairman of financial and non-financial institutions, board members, owners, temporary and permanent employees, and authorized representatives.

720. The MOCI is the supervisory authority responsible for real estate agents, dealers in precious metals and stones, and accountants, while the MOJ holds supervisory responsibility for lawyers and legal advisers.

Real estate agents, dealers in precious metals and stones, and accountants

721. In addition to the AMLS, a series of circulars issued by the MOCI and disseminated through chambers of commerce and self regulatory organizations (SOCPA) outline the requirements of commercial entities with respect to AML/CFT. In 2001, the MOCI issued circular No. 1312/11 outlining merchants' obligations to report any commercial or financial transaction of suspicious nature or having no evident economic purpose, and to not notify or otherwise warn customers when such transactions are reported. This also specified that those reporting such transactions in good faith are not subject to penalty. Circular No. 1312/11 also required the establishment of procedures to ensure that entities "are not misused in money laundry [sic] operations." Furthermore, employees must be qualified and trained to understand relevant regulations and to recognize money laundering risks.

722. Upon establishment of SAFIU, the MOCI issued circular No. 487/1/2/C in 2003 requiring that the reporting of suspicious transactions be directed to SAFIU. Circular No. 315/11 also issued in 2003 reiterates the requirement that all commercial entities establish programs to address AML/CFT and to educate employees to detect AML/CFT abuse, including by conducting training as needed. Additionally, circulars No. 454/FR (2007) and 1157 (2008) provide additional instructions for preventive measures including requiring all commercial establishments to develop and implement policies, procedures and internal controls to address possible ML exploitation, to assign responsibility for this to the general manager or his/her designate, to develop internal AML/CFT auditing and control systems, and to establish training programs in the area of AML/CFT. There are no specific provisions in MOCI regulations to ensure that those responsible for implementing policies, procedures and internal controls have full and timely access to data necessary to fulfill their duties, nor are there provisions that the audit function be adequately resourced and independent (not even in an industry relevant context). Companies and institutions are required to inform the AML Unit of the MOCI of measures undertaken in accordance with regulations issued by the MOCI. Screening of employees is also not explicitly provided for by MOCI regulations related to AML/CFT.

723. It is notable that the entities covered are numerous and broad in scope such that adherence in all cases questionable. The assessment team was not able to confirm comprehensive compliance. Guidelines issued by MOCI in 2004 for commercial entities and DNFBPs, include provisions for internal controls and policy, training and appointing of employees, and suspicious transaction reporting (see also Recommendation 12).

724. In reference to the application of Recommendation 21, MOCI Circular No. 1312/11 specifies that entities are required to "oversee and follow-up on transactions and deals entered with individuals, corporations or financial, non-banking businesses related to countries where money laundry [sic] measures are partially or not applied at all." Guidance to assist entities in the identification of such countries is

limited—the assessment team was informed that the MOCI distributes FATF statements through chambers of commerce although further detail regarding this practice is not known. Awareness and understanding of the requirement contained in Circular No. 1312 among DNFBPs is generally low. Additional requirements pertaining to treatment of entities and transactions related to countries that do not sufficiently apply the FATF Recommendations are not found in the MOCI regulations.

725. Real estate agents exhibit a basic level of awareness of how the sector might be used to facilitate ML/TF and the measures to be taken to mitigate this risk. Again, the evaluation team noted a tendency to associate ML/TF risk with cash-based transactions. The assessment team found that entities in this sector, while aware of the existence of a STR requirement, and despite significant issuance of guidance by the supervisory authority, otherwise exhibit relatively limited awareness of their obligations with respect to AML/CFT. The MOCI noted that they have not cited any violations for AML/CFT non-compliance in the real estate sector. No evidence was provided to indicate that a STR has ever been filed on behalf of a real estate agent. Authorities noted that the requirement of settling the value of the properties by virtue of draft cheques is considered an advanced procedure that mitigates the risks of ML/FT in the sector.

726. Relatively speaking, AML/CFT awareness among jewelers may be somewhat greater, although the evaluation team met only with industry representatives from larger, more established businesses. The majority of jewelers, and perhaps the most vulnerable, are small operations with only a few employees that nevertheless engage in significant transactions. Upon licensing, all jewelers must sign a form acknowledging their awareness of the AMLS and the obligations it defines, including specifically training. All entities seem to rely heavily on familiarity of customer base as a mitigating factor with respect to ML/TF. Jewelry representatives also pointed out that certain regulations of the industry, while not specifically designed as AML/CFT measures, effectively act as such. For example, when conducting a large purchase from a customer, this must be reported immediately to the MOI Criminal Investigation Department. It is notable also that while there is significant oversight of dealers in precious metals and stones, efforts are concentrated in areas outside of AML/CFT and on larger operations.

727. The assessment team noted that in the accounting industry, efforts are being made to provide training to professionals to increase awareness of ML/TF risks and entities' responsibilities in addressing these risks. At the time of the onsite visit, a training program for the accounting industry focusing on money laundering was soon to be launched in several cities across the Kingdom. These sessions are administered by the MOCI and provided at no cost to participants. Additionally, the Saudi Organization for Certified Public Accountants (SOCPA) are undertaking independent efforts such as publishing articles describing AML/CFT risks and the addressing thereof, to be provided to auditors and accountants upon certification.

Lawyers

728. Upon its issuance, the MOJ disseminated the AMLS by circular to all entities under its supervisory authority. Through a series of circulars addressed to lawyers, the MOJ also reinforced the obligation to report suspicious transactions to SAFIU. No regulations to apply additional AML/CFT measures have been issued by the MOJ. At the time of the onsite visit, it was noted that the MOJ was working with the Banking Institute and Chamber of Commerce and Industry to provide courses for lawyers to educate on AML/CFT risks and compliance obligations. The first such course was to be administered in March 2009. Additionally, MOJ provided the team after the onsite visit with an introductory booklet it issued to explain the concept of ML and the MOJ's efforts in fighting it. Specialized advisors at the MOJ

are entrusted with executing and following through on the implementation of the AMLS and its IRs in the sector. Nearly 200 on-site inspections of lawyers have been conducted by the supervisory unit of the MOJ, and this number increases daily. During the course of their visits with lawyers, inspectors must inquire about implementation of AML/CFT procedures. MOJ representatives noted that of the roughly 20 disciplinary orders administered to lawyers in the course of these inspections, none were related to money laundering. Inspectors of lawyer activities receive some amount of AML/CFT-specific training, although the extent and content of this training could not be confirmed by the assessment team.

729. While provision of legal services is a nascent industry in Saudi Arabia, there is potential for its rapid growth. MOJ authorities noted that at this time the legal profession in the Kingdom is largely comprised of trial lawyers. Nevertheless, the absence of adequate AML/CFT regulation and supervision, and lack of a general awareness among industry participants of the ML and TF threats posed, is of significant concern. No STRs have ever been filed on behalf of lawyers and legal advisors.

Statistics

730. The authorities provided the following statistics:

STRs Filed by Non-Financial Institutions (2004-2008)					
	2004	2005	2006	2007	2008
Accounting Firms	0	0	1	3	2
Dealers in Precious Metals and Stones	0	0	4	8	6
Companies and Institutions with Different Activities	0	0	9	21	20
TOTAL	**0**	**0**	**14**	**32**	**28**

Source: SAFIU

4.2.2 Recommendations and Comments

731. Significant ML/TF vulnerabilities exist stemming from a general low level of awareness among all DNFBPs of risks posed. Authorities must make a concerted effort to raise awareness of ML and TF risks among DNFBPs and provide regular and consistent guidance to assist in the development of systems to address these risks. Additional effort must be made to make these entities aware of their legal obligations with respect to AML/CFT beyond STR filing and the authorities must actively enforce these obligations. The MOCI indicated that they are undertaking efforts to increase awareness including through seminars and conferences organized by the Saudi Chambers of Commerce and Industry.

732. Authorities should seek to actively encourage compliance with the STR filing requirement, including through the issuance of typologies, increased training, and provision of feedback. The MOCI noted that they have never received feedback from the FIU regarding the results of any STR filed by an entity under their supervision.

733. The MOJ should issue additional regulation and guidance to legal services providers regarding AML/CFT measures. Along these lines, the Ministry is presently taking steps including the preparation of guides to be distributed to legal service providers that clarify the necessary measures to prevent any ML or TF offense. The Ministry noted also that it is increasing its efforts to heighten awareness of ML/TF risks and the means to combat them through additional training, seminars and conferences.

4.2.3 Compliance with Recommendation 16

	Rating	Summary of factors relevant to s.4.2 underlying overall rating
R.16	**NC**	*Application of R.13* • Low number of STR filing from dealers in precious metals and stones and accountants indicates low effectiveness. • Absence of STR filing from lawyers and real estate agents indicates no effectiveness. • Insufficient awareness among entities regarding ML/TF risks and identification thereof. *Application of R.15* • No specific regulations or guidance issued for lawyers and legal advisors. • Lack of supervision and enforcement renders low effectiveness. • Insufficient awareness among entities regarding ML/TF risks and identification thereof. *Application of R.21* • No requirement applying to lawyers and legal advisors. • MOCI does not provide appropriate guidance for all covered DNFBPs and requirements are not enforced.

4.3 Regulation, supervision and monitoring (R.24-25)

4.3.1 Description and Analysis

734. In relation to DNFBPs, the AMLS defines non-financial institutions as the ones that undertake commercial or economic activities such as commercial companies, sole proprietorship, professional activities or other similar activities. Such activities exist in the form of (Article 1-2 of AMLS and its implementing regulations): (a) real estate transactions and Trust service; (b) dealing in valuable metals, precious stones or rare commodities, like antiques; (c) trade in goods with high value such as luxury cars and goods offer in auction houses; (d) law practice and company service; (e) accounting and auditing.

735. The supervisory authorities responsible for the DNFBPs operating in SA are the following: the Ministry of Commerce and Industry (MOCI) for real estate agents and dealers in precious metals and gemstones; the Ministry of Justice (MOJ) for lawyers and notaries; and the Saudi Organization for Certified Public Accountants.

Ministry of Commerce and Industry (MOCI)

736. MOCI supervises and monitors the trade and manufacture of precious metals and their proceeds (Article 1 of Precious Metals and Gems Law). MOCI has the right to enter and inspect the shops and stores of precious metals and gemstones (Article 13 of Precious Metals and Gems law) and impose financial penalties with fines not exceeding SAR 200 000 when violating Precious Metals and Gems Law and its regulations (Article 17).

737. Any person who is interested in opening a real estate office should register his name in the special commercial register with MOCI (Article 1 of the rules for regulation real estate offices issued by MOCI). Failing to do so, the violator will be subject to one of the following sanctions: a fine not exceeding SAR 25 000, closure of office for a period not exceeding one year and cancelling the permit of the offices definitely.

738. As noted above, real estate agents and dealers in precious metals and gemstones, which include jewelers and jewelry shops, fall under the umbrella of MOCI. The AMLS requires MOCI being one of the competent supervisory authorities in the law to set adequate means and controls to ensure the compliance of units subject to supervision with laws, rules and regulations prescribed by AMLS and its implementing regulations (Article 6-1).

739. In realizing such role the MOCI established an Anti-Money Laundering Unit through Resolution No. 1833, dated 24/2/1425 H. The unit has the following duties among other things: to oversee implementation of the AMLS and its implementing regulations; to organize awareness campaigns inside and outside the ministry; and to take the necessary measures to foil any attempt to use trade organizations and companies in such illegal activities.

740. The MOCI through its Anti-Fraud Department engages in licensing, monitoring and imposing sanctions on (natural and legal) persons violating the related regulations issued by MOCI. The Department, which includes the AML unit, consists of 220 employees that are involved in the 3 functions specified above. Officials confirmed to the team that examiners perform onsite examinations of persons subject to MOCI supervision, which include *inter alia* monitoring compliance with AML/CFT, in addition to their regular checks on licensing and fraud issues, etc.

741. Circular No. 454/(w.d.) was also issued on 19/12/1428 AH stating the necessity to take precautionary measures so that companies and institutions are not used in passing ML or FT operations. Paragraph 1 stipulated that every company and institution should communicate with local banks they are dealing with to tell them not to accept any monetary deposit or internal transfer to the company or institution's accounts from their clients outside KSA. In case any amount or transfer not complying with these conditions was received, the bank from which they were sent will be forced to return them and assume full responsibility.

742. The authorities provided the team with documents related to the process, including an attestation form signed by the supervised persons stipulating that they are aware of AMLS and its implementing regulations. In addition, the authorities shared with the team blank report forms used by examiners to report their findings. Moreover, MOCI issued a very basic advisory guidebook to help both estate agents and dealers in precious metals and gemstones to understand and fight ML/FT. The said guidebook covers the following areas: KYC principle, internal political supervision, commercial accounts and keeping records, external auditing, appointing and training employees, reporting and cooperating with the FIU, and the legal liability and the chambers' role in AML/CFT.

743. The team met with representatives of both sectors who demonstrated their efforts in following MOCI regulations. It was noted that both sectors lack the basic knowledge of AML/CFT techniques, especially in the real estate sector. The team believes that while MOCI is taking adequate measures to supervise and regulate the activities of precious metals/stones and jewelry dealers, the techniques used by MOCI examiners are not adequate to monitor the compliance of the said sector with AMLS and its

implementing regulations. The reports used by examiners to report their findings focus primarily on licensing issues rather than AML/CFT issues, which might indicate the lack of expertise in such filed by examiners.

744. As for the real estate sector, the team noticed the lack of awareness both at authorities and brokers' levels of how such sector might be used for ML/FT. No evidence of effective monitoring was provided by the authorities to the team during the visit and no indicators were given by the industry on any preventive measures used to fight ML/FT. There was a general confidence by the authorities and brokers that, since checks were used as a form of payment, transactions in this sector are legitimate and AML/CFT risk-free.

745. However, as mentioned above, requirements on supervised persons were not monitored thoroughly by the authorities due to the lack of expertise in this field, nor the industry had the knowledge or awareness to implement such requirements in the business.

Ministry of Justice (MOJ)

746. Any person practicing law in the SA has to be licensed and registered with MOJ (Article 2 of the implementing regulations of the Code of Law Practice).The notaries are associated administratively to MOJ (Article 7 of the implementing regulations of Notaries Public).

747. Like MOCI, MOJ is subject to the same requirement as stipulated by Article 6 of AMLS and its implementing regulations. It is worth mentioning that the practice of law and resorting to lawyers are new concepts to the public, as any person can defend himself before a court. Such right is still valid in the Kingdom. Notaries in SA are government employees not practicing the activities under R.12 and are therefore not subject to this evaluation. However, it is noteworthy that the Minster of Justice issued a circular (13/c/3560 dated 29/1/1430 (2009)) requesting all courts and notaries t report any suspicious transactions related to AML/CFT to SAFIU.

748. MOJ issued Circular No. 26/93631, dated 16/11/1426H (2005), to appoint as member of the Permanent Committee the deputy Ministry of Justice to serve as a liaison, coordination, and follow-up officer with the bodies concerned in the fight against money laundering. Furthermore, the MOJ issued the circular number 9361/26 dated 16/11/1426 AH, which specifies a communication officer who shall coordinate with the FIU to accelerate the execution of requests issued by the FIU. No regulations or supervisory framework to perform supervisory duties or to monitor lawyers' compliance by the authorities were issued.

749. The team visited a law firm who confirmed on-site visits by MOJ; the team did not witness such role while visiting the authorities. No typologies or indicators were issued by MOJ to lawyers and no other forms of communications were found in demonstrating MOJ duties provided for by Article 6 of AMLS and its implementing regulations as specified above.

750. According to lawyers and authorities, practicing law is a new function introduced to the system and there is a huge potential for accelerating demand by the public to utilize the services of lawyers and law firms in the Kingdom. The supervisory mechanism and providers of this service are not adequately aware of the risk of ML/FT their profession is exposed to. The mission believes that such sector suffer from lack of knowledge and expertise in this filed.

Saudi Organization for Certified Public Accountants (SOCPA)

751. The Saudi Organization for Certified Public Accountants (SOCPA) is a professional organization established under Royal Decree No. M12 dated 1.05.1412H corresponding to 19.11.1991G. It operates under the supervision of MOCI in order to promote the accounting and auditing profession and all matters that might lead to the development of the profession and upgrading its status. A thirteen members Board manages SOCPA affairs, and practices the powers required for realizing its objectives which include:

- Review, develop and approve accounting and auditing standards.
- Monitoring the performance of certified public accountants to ensure their compliance with accounting and auditing standards and with the provisions of CPA Regulations and its by-laws.
- Establish SOCPA fellowship examination rules and organize CPE courses.
- Conduct researches and studies; publish periodicals, books and bulletins covering accounting and auditing subjects; and participating in local and international committees and symposiums relating to the profession of accounting and auditing.

752. No person, natural or legal, shall be entitled to practice the audit profession unless his name is listed in the register of certified public accountants with Ministry of Commerce (Article 1 of the Certified Public Accountants Regulations). Providing auditing services without a license or violating the regulation will be subject to penalties ranging from warning to imprisonment for not more than one year (Article 28 of certified public accountants regulations). SOCPA confirmed to the team that no role for external auditors or audit firms in performing financial or non-financial transactions or activities on behalf of their clients.

753. MOCI officials indicated that the supervision of accountants and auditor, including from AML/CFT purposes, is the responsibility of SOCPA. According to SOCPA officials, SOCPA is the body in charge of training and educating its members in all aspects of the profession, including AML/CFT. SOCPA performs routine examination of its members to asses the quality of their audits and monitor any violation against the Certified Public Accountants Regulations. However, no statutory provisions explicitly gives SOCPA the right to assume supervisory powers in relation to AML/CFT, which was confirmed by SOCPA officials.

754. Accordingly, no specific examination was performed by SOCPA to monitor the members' compliance with AMLS and its Implementing Regulations. Moreover, SOCPA did not issue any typologies or indicators for the industry.

755. While the team understands the current role of the profession providers, it acknowledges the Kingdom's massive economics reforms especially through encouraging foreign investments and believe that such services have a potential growth in the future and shall benefit from enhanced supervisory monitoring in AML/CFT filed.

4.3.2 Recommendations and Comments

- Enhance the expertise and supervisory framework for DNFBs.

- Enhance the knowledge and expertise in the filed of AML/CFT for DNFBs as the need for services of such sector is growing.

- Produce typologies and best practice monitoring techniques based on past experience and the local market condition.

- Enhance the feedback from and to both DNFBs and SAFU.

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	**NC**	• No effective system in place to supervise and examine the compliance of DNFBs with AMLS and its implementing regulations. • Lack of expertise of ML/FT risks within competent authorities and DNFBs.
R.25	**PC**	• No specific guidelines have been issued to assist all DNFBs • No feedback has been provided by SAFIU

4.4 Other non-financial businesses and professions and modern secure transaction techniques (R.20)

4.4.1 Description and Analysis

Other non-financial businesses and professions

756. According to authorities, there is a developed market for dealers in high-value luxury goods such as new cars and auction houses in the Kingdom. These activities are within the scope of the AMLS and as such are licensed by the MOCI and subject to all provisions of the AMLS and AML Regulation. This is sufficient proof that the authorities have considered applying the FATF Recommendations to other non-financial businesses and professions. [It should be noted that there is no sign of implementation of these provisions, but that is not required by Recommendation 20].

Modern secure transaction techniques

757. Cash is still heavily used in KSA. The authorities therefore support the increasing use of modern means of conducting financial services such as credit and debit cards (automated teller machine (ATM) cards). The Banking Technology Department (BTD) in SAMA has developed a series of initiatives that significantly contributed to the development of the financial sector and to the use of modern and more secure techniques for conducting financial transactions. These initiatives include:

- The establishment of the Saudi Arabian Riyal Inter-bank Express (SARIE) system in May 2004. SARIE is a high-speed and risk-contained single and bulk gross settlement system of payment of transactions. It involves all banks operating in the Kingdom and operates in real time.

- The establishment of the Saudi Payments Network (SPAN), which is an automated payment systems network. It connects all ATMs and points of sale (POS) terminals throughout the country to a central payment switch (*i.e.*, the compensation system) which in turn re-routes the financial

transactions to the card issuer (*i.e.*, a local bank, VISA, AMEX or MasterCard). In 2000, there were 2,234 ATMs operating in the Kingdom. In 2007, the number of ATMs reached 7,468. During the same period, the number of POS went jumped from 18 537 to 61 557.

- The establishment of the SADAD, a national Electronic Bill Presentment and Payment (EBPP) service provider for the Kingdom. The core mandate for SADAD is to facilitate and streamline bulk payment transactions of end consumers through all channels of the Kingdom's banks. It was launched officially in October 2007.

758. The team welcomes the authorities' initiative in this regard and encourage the wide spread of such non-cash gateways as alternative cash payment tools in the Kingdom, especially with the vast and growing number of tourists arriving to the Kingdom all year long, who can benefit of such services without the need of carrying cash to settle their expenses.

4.4.2 Recommendations and Comments

- The authorities should consider legally banning cash transactions above a certain threshold, in support of their policy to reduce the reliance on cash and encourage the use of modern secure payment techniques.

4.4.3 Compliance with Recommendation 20

	Rating	Summary of factors underlying rating
R.20	**C**	This recommendation if 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

759. Corporations are regulated by way of the Law of Professional Companies ("the Companies Law") and the Commercial Register Law ("CRL"). A company register is maintained by the Ministry of Commerce and Industry ("MOCI"), whereby all company forms are required to register. Saudi Law allows for the following forms of companies to be established: general partnerships; limited partnerships; joint ventures; joint stock companies; partnership limited by shares; limited liability companies; companies with variable capital; and cooperatives.

760. Article 1 of the CRL provides that the MOCI shall maintain a register containing the names of Saudi merchants and companies. Article 3 CRL further provides that it is up to the company management to submit an application for registration within 30 days from the notarization of the company formation contract.

761. The registry does not fulfill any notarization function and companies may, therefore, obtain legal personality upon signing of the company formation contract. However, legal status may not be invoked against third parties prior to completion of the registration process. Applications for registrations are received, studied, and granted or denied by MOCI's "Companies Department." All granted applications are

forwarded to the "Registration Department" for inclusion in the registry. The Registration Department has about 40 branches in all regions (emirates) of KSA, and all branches are all linked through a centralized electronic database.

762. Pursuant to Article 228 of the Companies Law, foreign companies generally may not establish branches, agencies, or offices in SA, nor may they issue securities or offer them for subscription or sale unless permission of the Minister of Commerce has been obtained. In cases where such permission is granted, the company must go through the regular application and registration process pursuant to Article 3 CRL. The same procedures apply to companies from GCC member states.

763. Applications pursuant to Article 3 CRL must include a copy of the Articles of agreement including information on the type and name of the company, the nature of the intended business, the company capital, and the date of commencement and termination of the company as well as names, date of birth, nationality and address of the partners, managers, and other persons authorized to sign on behalf of the company. Pursuant to Article 4 of the CRL, any modifications or changes to information previously recorded must be updated within 30 days from when the change occurred.

764. Article 8 of the CRL requires the MOCI to verify the conditions and information required for the registration and to request from the applicant any additional documentation. A copy of the articles of agreements, of the identification documents of the owners/partners, as well as the managers and board members is used for verification purpose.

765. Pursuant to Article 15 CRL, any violation of the provisions of the CRL may be sanctioned with a fine not exceeding 50,000 Riyals.

766. Article 11 CRL provides that anybody, including the competent authorities, may obtain a copy of the information held at the commercial register with respect to registered entities. With the exception of judgments or bankruptcy notifications in cases where reparation has been adjudicated and judgments concerning interdictions or attachments that have been lifted, all information held at the register as outlined above is freely accessible. In the absence of a registration record, a certificate evidencing such absence can be issued.

767. In addition, for joint stock companies and partnerships limited by shares, the MOCI publishes the company formation contract and the company by-laws in the Official Gazette. Information and documentation held at the registry is maintained indefinitely.

768. Of the eight company types listed above, only joint stock companies, partnerships limited by shares, and limited liability companies are allowed to issue shares.

769. Pursuant to Article 102 of the Companies Law, shares issued to registered holders is transferred by means of an entry in the shareholder register that is kept by the company. The register contains the shareholder names, nationalities, residence addresses and occupations, the number of shares held by each shareholder, and the amounts paid up on such shares. A transfer of title to any registered share is only considered effective from the date of its entry into the shareholder register.

770. Pursuant to Article 27 CML, ownerships of securities traded on the stock exchange shall be registered with the Securities Depositary Centre, which is the sole entity to register all property rights in securities traded on the stock exchange. Information obtained by the Depositary Centre includes a copy of

the investor's ID as well as the portfolio number, which in turn is linked to information obtained in the course of the investor's application to trade on the stock exchange, such as the nationality, date of birth, bank account number, and a copy of the passport as well as the address. In addition, persons trading on the Stock Exchange must have a valid bank account in SA and, therefore, the due diligence procedures outlined under Recommendation 5 apply.

5.1.2 Recommendations and Comments

- It appears that anyone in the Kingdom is entitled access to the information on control and beneficial ownership of legal persons, through the powers granted by CRL law. Ownership details must be submitted and verified against identity documents at the time of registration, and CRL requires any modifications or changes to the information previously recorded have to be updated within 30 days from occurrence.

- In principle, Commercial Register information is available to all competent authorities, as well as the public, however accessing such information might require time as this information is only available within the 40 branches of Commercial Register Office. The team encourages the authorities to introduce direct and spontaneous access to the information by the competent authorities.

5.1.3 Compliance with Recommendations 33

	Rating	Summary of factors underlying rating
R.33	**LC**	• Lack of direct and spontaneous access to the Commercial register information by competent authorities.

5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34)

5.2.1 Description and Analysis

771. KSA has legal arrangements that are very similar, but not identical, to the common law express trust.

772. The Saudi legal arrangement is known as *waqf*. A *waqf* can have two forms. It can either be established as a charity (see section 5.3 of this report), in which case the *waqf* operates like a legal entity (similar to the civil law foundation), or as a legal arrangement, which operates like a common law express trust.

773. Every *waqf* is required to have a *waqif* (founder), *mutawilli* (trustee), *qadi* (judge of a court) and beneficiaries. Under a *waqf*, property is reserved, and its usufruct appropriated, for the benefit of specific individuals, or for a general charitable purpose; the corpus becomes inalienable; estates for life in favor of successive beneficiaries can be created and without regard to the law of inheritance or the rights of the heirs; and continuity is secured by the successive appointment of trustees or *mutawillis*.

774. The main difference with a common law express trust is the existence of the qadi (judge), who registers the trust deed (*waqfiyya*) and supervises the *waqf* to ensure that the trustee operates within his

mandate. The qadi also has to register changes to the trust deed. The *qadi* has the power of veto, also if changes would change the nature of the *waqf* and / or be contrary to any provision of Shari'ah (Law of the Judiciary[82], Section 14). The qadi also ensures that all *waqfs* are registered with a public notary (a registry of the Ministry of Justice) and are publicly available.

775. The authorities have stated that the trust deed has to contain information on the control and beneficial ownership, although the assessment team was not able to verify this. Since the concept of beneficial ownership (as opposed to the concept of beneficiaries) is generally unknown in Saudi law, it is unlikely that the trust deed would contain information on the beneficial owner.

5.2.2 Recommendations and Comments

776. Overall, the KSA has created a system for controlling legal arrangements that outperforms system in other countries. One issue could not be resolved, which is the lack of a requirement to disclose information on beneficial ownership (in addition to the beneficiary) on the trust deed.

5.2.3 Compliance with Recommendations 34

	Rating	Summary of factors underlying rating
R.34	**LC**	• The assessment team was unable to confirm that beneficial ownership is available

5.3 Non-profit organisations (SR.VIII)

5.3.1 Description and Analysis

General framework

777. The current legal framework for regulating and licensing charities was established before Special Recommendation VIII was endorsed. The Charities Regulation[83] dates from 1990 and the Charities Executive Rule[84] dates from 1991.

778. Saudi Arabia reports that it is in the process of establishing a High Commission on Charities that will examine the regulation and supervision of all charities. However, this plan dates from at least 2003[85] and has still not been implemented.

779. Royal Decree No.2/1 dated 6/1/1425 AH (Article 6) prohibits Saudi charities to donate or collect money from abroad or operate abroad. Also government entities are prohibited (Article 4) from making

[82] Royal Decree No. M/64, 14 Rajab 1395H.

[83] Regulations of the Charitable Associations and Institutions (Charities Regulations) issued by the Council of Ministers' Resolution No. 107, dated 25/6/1410H (January 23, 1990)

[84] Executive Rules for the Charitable Associations (Executive Rules for Charities) issued by the Minister of Social Affairs' (MOSA) Resolution No. 760, dated 30/1/1412H (August 11, 1991)

[85] United Nations Security Council Letter S/2003/583 dated 29 May 2003 from the Chairman of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism, addressed to the President of the Security Council.

donations abroad. The authorities stated that donating for relieve and support abroad is a royal prerogative. This ban applies to Saudi charities and to individuals donating funds of others'; it does not apply to individuals when donations originate from their own funds[86] (individuals and states are, however, excluded from the remit of Special Recommendation VIII). However, charities, governmental entities and individuals can give support abroad with the approval of the Domestic Saudi Commission for Rescue and Charity Abroad. This commission came into being on basis of the royal decree. It is presided by MOI and members are MOFA, MOF, MOSA and MOIA. It did not become clear to the assessment team whether this commission is active or not. Article 75 of the Charities Regulation provides that charities may only operate within the borders of the Kingdom.

780. Charities are licensed either by the Ministry of Labor and Social Affairs (MOSA) or by the Ministry for Islamic Affairs (MOIA). The MOSA licenses regular charities and the MOIA licenses educational charities (*Qur'an* schools and mission charities) and *waqfs* (trusts). All types of charities are legal persons, except the *waqfs*, which are legal arrangements.

Regular charities

781. The MOSA is the authority in charge of regular charities: It licenses and registers charities and appoints the boards. Appointments can only be done on the basis of a non-objection statement from MOI concerning each member. The MOSA is responsible for supervision of the sector. This is done through 20 supervisory branches in the large cities and one in each province. A branch supervises all charities in its city or province and contracts for this purpose external accountants who make regular and unannounced visits. The external accountants prepare quarterly reports which are submitted to MOSA and the concerned charity's board. Annual reports have to be submitted by each charity to the branch under which it resorts. In case a supervisory branch or MOSA have doubts about (financial) issues an external accountant will be appointed. MOIA has a similar approach for supervising its charities.

782. To strengthen its control on the sector, MOSA has set up an impressive electronic database with extensive and comprehensive information holdings, including: *(i)* name and address of each charity and its purpose and aim, *(ii)* names and addresses of each board member as well of the manager and accountant of the charity, *(iii)* MOI and MOSA approval data, *(iv)* names and addresses of donors and of recipients of donations in money or kind, *(v)* all financial data concerning deposits and by whom and their addresses and concerning outlays of money to recipients and their names and addresses, *(vi)* plan and budget of each charity, *(vii)* the financial position of a charity and its bank balance *(viii)* quarterly follow-up on remarks by the (external) accountants. Each charity can access the database in order to update its own data (which is thereafter verified), primarily financial data and follow-up on remarks by the accountants.

783. The Charity Regulations, which make a distinction between charity societies and special charity institutions, stipulate that these are only allowed to provide social and educational services (in cash or in any other form) or cultural and health services on a humanitarian basis (*i.e.*, Diabetes Association, Down Syndrome Association). Charities are strictly not-for-profit. The Charities Executive Rules further limit the

[86] The authorities indicated that individuals are also prohibited to donate their own funds abroad. The assessment team was unable to confirm this in the law. The team would also question the ability of the authorities to enforce such a measure (given the large number of wire transfers and money transfers, and the legal ability for citizens to take cash out of the country and finance charity from abroad). Nevertheless, given the fact that Special Recommendation VIII is not intended to cover individuals or states, the assessment team decided not to have a final view on whether individuals are or are not allowed to donate abroad from their own funds.

activities by providing that the charity work may only be provided in Saudi Arabia (Article 75). Charities are subject to the supervision and control by MOSA (Article 2 of the Charities Executive Rules). Additionally, the members of the boards of charities have to be approved by MOSA or MOIA. There are currently 446 charity societies and 50 special charity institutions licensed. The former is of a public nature and collects from the public, while the latter is of a private nature. It is the initiative of a private person or a family; it is not allowed to collect from the public but can accept donations and wills.

784. Since November 2003, regular charities are required to report ML/TF related SARs[87]. However, these have to be reported to MOSA, and not to SAFIU and fall outside the STR framework as defined in the AMLS. The team is not aware of any such SARs ever reported by any charity or by MOSA to SAFIU. In a circular (No.41735 dated 23/9/1424 AH) MOSA staff is also required to report these SARs when they see fit to do so during their supervisory work. No SARs had to be reported so far (NPO to MOSA, or MOSA to SAFIU).

Educational charities

785. The Ministry of Islamic Affairs is in charge of educational charities. These can be distinguished between charities that are in charge of running *Qur'an* schools, geared to educate young people in the teachings of Islam, and charities with the aim to enlighten foreign residents and visitors of the Islamic rules and customs that need to be respected. MOIA licenses and registers and appoints the boards of NPOs using MOI for non-objection statements. Supervision is through 13 supervisory branches, one in each province, and is done in similar fashion as MOSA exercises its supervision. An exception is that the chairman of a supervisory branch is a member of the board of each charity in his province. MOIA does not make use of the electronic database of MOSA, it operates its own database. There are 13 educational charities in charge of teaching the *Qur'an* and 200 offices for communities' awareness.

786. The sector of educational charities is supervised by the Supreme Council for Charities and its Secretary, representatives of the religious university, MOI, MOE and the chairmen of the 13 supervisory branches. This company sets rules for *(i)* strategy and planning, *(ii)* approval of new charities *(iii)* nominations. It also approves the funding of MOIA for onward allocation to the charities. Since 1 January 2003[88], educational charities and *waqfs* have the duty to report ML/FT transactions. Other than is the case with regular charities, STRs will go to SAFIU directly without the requirement of MOIA to receive a copy. The team became not aware of any reports having been submitted to SAFIU.

787. The MOIA is also responsible for registering and supervising *waqfs*. Waqfs are labeled as charities in the Kingdom, but they are, in fact, legal arrangements (trusts). See for more information on *waqfs* also section 5.2 of this report.

788. There are two sorts of *waqfs*: private/individual and public. *Waqfs* are trusts in which funds were left behind by a deceased of a certain family. In the private trust (a) certain member(s) of the family can make use of the funds left behind. The public *waqf* has the purpose to use the funds in a certain way as indicated by its charter. MOIA is only in charge of public *waqfs*. It registers and supervises. Private *waqfs* are supervised by the judge of the court which registered the deed indicating the purpose of the *waqf* and its beneficiaries. There are an unknown number of public *waqfs*.

[87] Ministry of Social Affairs' Circular No. 41735, dated 22/9/1424H
[88] Circular on ML/FT reporting no 4/9/188, date 15/8/1426H

789. The sector of *waqfs* of both sorts is overlooked by the Supreme Council of *Waqfs*, the MOIA deputy minister of *Waqf* Affairs, the MOIA legal adviser for *Shari'ah* affairs, MOF (the head of the Heredity Affairs), MOE, a.o. experts. Rules are set by this council; for *(i)* registration, *(ii)* development and strategy *(iii)* budgeting, finance and expenditure, *(iv)* renting of real estate *(v)* approval of projects, *(vi)* annual reporting.

Review of the NPO sector

790. The authorities have not conducted a review of the laws and regulations that relate to the NPO sector in the Kingdom, have not undertaken a domestic review of or have the capacity to obtain timely information on the activities, size and other relevant features of their non-profit sectors for the purpose of identifying the features and types of non-profit organisations (NPOs) that are at risk of being misused for TF by virtue of their activities or characteristics, nor are they conducting periodic (partial) reassessments. The authorities stated that such reviews are not deemed necessary, due to the fact that MOSA has the permanent authority to review and amend laws. For MOIA, there is a policy that its laws are reviewed every four years. Despite this, it is the view of the assessment team that Special Recommendation VIII requires an overall NPO review, especially for the purpose of assessing whether or not the legal and policy framework is sufficient.

Outreach

791. All NPOs in Saudi Arabia are subject to licensing, registration and supervision requirements as described in this section of the report. These supervisory control mechanisms include legal standards for transparency, accountability and integrity administration and management of all NPOs. This goes beyond the outreach as envisaged by Special Recommendation VIII (which only requires promotion of these virtues). In addition, in relation to abuse of NPOs, including abuse for TF purposes, awareness is raised through outreach through the mass media, articles in specialized magazines for NPOs, with the distribution of CDs and through the mosques.

Available information

792. All NPOs have to maintain information on: *(i)* the purpose and objectives of their stated activities and *(ii)* the identity of person(s) who direct and control their activities, including senior officers (manager and accountant), board members and trustees. This information is available to MOSA and MOIA, as well as to the external accountants. This information is updated in real time.

Sanctions

793. The authorities indicated that if a charity would be involved in ML/FT, this would be considered an aggravating factor and the possible sanction would be raised (as described in Section 2.1 of this report). Authorities indicated that MOSA and MOIA will use civil or administrative sanctions if the case at hand merits it. Administrative sanctions include termination of the charity, dismissal of board members or members of the management, freezing of bank accounts. Such sanctions have been applied in the past (unknown number of sanctions), albeit not specifically for anything related to ML/FT. There is no mentioning of civil action against an official of a charity in the charity law and executive rules, but action may be undertaken depending on severity of the case. No legal references were available.

Licensing and registration

794. All charities in the Kingdom must be licensed and registered by MOSA or MOIA (see above).

Record keeping

795. All NPOs have to retain all records of all transactions, whether about incoming or outgoing funds, whether in cash, by check, wire or in kind (it is unknown for how many years and what the legal basis is for this requirement). SAMA restricts the opening of bank accounts for charities to those that have properly been licensed. A charity is not allowed to have more than one account. Regular charities will accept incoming payments by cheque, transfers, electronic payment means or cash deposit whether at a bank or at the charity's office. Normally outgoing payments will not be made in cash but by way of banking transfer. Educational charities also receive their funding from MOIA.

Information gathering and sharing, and domestic cooperation to target abuse

796. Charities are subject to regular supervision by MOSA and MOIA, either directly or through their supervisory branches. Also external accountants, at the request of MOSA or MOIA or their branches, may be checking on certain charities, in addition to the regular government appointed in-house accountants. Charities must submit annual reports to their respective supervisors for approval. The maintenance of bank accounts and the flows of funds of a charity are restricted to the manners as described in the previous paragraph. Charities as well as their supervisors have the duty to report SARs. All the information on NPOs (see above for the information that is contained in the databases) is at all times and immediately available to the government, without need for opening of an investigation (this goes beyond the requirements of Special Recommendation VIII). In addition, there are no legal barriers for exchange of information contained in the databases among government agencies, although sharing of information is upon request or MOU only.

International cooperation

797. The authorities indicated that any foreign request would be dealt with as an MLA request, and should be processed through the MOFA. See for an overview of international cooperation section 6 of this report.

Effectiveness

798. The NPO sector appears to be encapsulated in a comprehensive regulatory and supervisory system that outclasses many other systems of other jurisdictions and that appears to be rather effective. As the assessment team is not aware of any reporting of SARs, a review and reconfirmation of the SAR obligation would extend the effectiveness of the system.

5.3.2 Recommendations and Comments

799. With many charities and *waqfs* with a multiple of transactions it is essential that MOSA and MOIA review the NPO system as a whole and identify elements of the system and types of NPOs that are at risk. It is unclear what the requirement and the legal basis are for the record keeping requirements.

5.3.3 Compliance with Special Recommendation VIII

	Rating	Summary of factors underlying rating
SR.VIII	**LC**	• No review of the adequacy of domestic laws and regulations that relate to NPOs, no domestic reviews for the purpose of identifying the elements and types of NPOs that are at risk of being misused for TF by virtue of their activities or characteristics; and no periodic reassessments by reviewing new information on the sector's potential vulnerabilities to terrorist activities • Record keeping requirements unclear (terms and legal basis).

6. NATIONAL AND INTERNATIONAL COOPERATION

6.1 National cooperation and coordination (R.31)

6.1.1 Description and Analysis

Domestic cooperation mechanisms (Recommendation 31)

800. The Saudi government has established three inter agency cooperation bodies: *(i)* the Permanent Committee on Combating Money Laundering (PCCML); *(ii)* the Permanent Committee on Combating Terrorism (PCCT); and *(iii)* the Permanent Committee on Mutual Legal Assistance (PCMLA). In addition to these committees, two private sector committees organize coordination within the banking sector: *(i)* the Self-Supervisory Committee (SSC), responsible for coordinating and searching of terrorist lists; and *(ii)* the Financial Crimes and Money Laundering Committee (FCML) that examines issues in relation to financial crimes.

The Permanent Committee on Combating Money Laundering

801. The PCCML was established by Cabinet's Resolution[89] in May 1999. It is based at SAMA headquarters in Riyadh and is chaired and supervised by H.E. the Governor of SAMA. The PCCML is responsible for all AML/CFT related policy coordination, including ensuring implementation of the FATF Standards. The Committee heads the Saudi delegation to FATF, MENFATF and other international bodies. It has six members from the MOI (one for each law enforcement branch, including the FIU) and one member each from MOFA, MOJ, MOCI, MOF, Customs, the Prosecution Authority (PA), CMA and SAMA. The Committee employs a vice president and secretarial staff. The Committee meets on a monthly basis and deals with a wide range of issues related to AML. The Committee reviews and comments on proposed AML legislation or regulations. The Committee has established sub-committees to address specific issues.

[89] Cabinet resolution No. (5) on 17/1/1420 H

The Permanent Committee on Combating Terrorism

802. The PCCT was formed in December 2001[90] and has an oversight and coordination role for efforts in Saudi Arabia to combat TF. The four permanent members of the Committee are from MOI, GID, MOFA and MOF (SAMA). The non-permanent members may participate as appropriate. These are from MOF (Diwan), MOJ, MOCI, MOIA, MOSA, *Diwan Al-Mathalem* (the citizens complaints court), CMA, Customs and other party that the PCCT deems necessary to resort to. The Committee is chaired by the General Director of Intelligence of the MOI. The PCCT receives, examines and replies to requests from other countries and international organizations in relation to the fight against terrorism.

The Permanent Committee on Mutual Legal Assistance

803. The Permanent Committee on Mutual Legal Assistance (PCMLA) is chaired by the MOI. Its membership consists of representatives from the MOJ, the BIP, MOF, MOFA, SAMA, *Diwan Al-Mathalem* (the citizens complaints court) and Customs. Its role is to process requests from foreign states for international cooperation or mutual legal assistance. SAMA is the gateway through which law enforcement agencies are able to obtain information from FIs.

Review of the effectiveness of AML/CFT systems (Recommendation 32)

804. The PCCML is mandated to review the Kingdom's AML/CFT systems, and it has done so permanently on an ad-hoc manner. There has not been a complete review of the entire system by PCCML or other bodies (*i.e.*, ministries or government accountability offices).

Effectiveness

805. Despite the fact that there are at least three policy bodies that coordinate the Kingdom's AML/CFT laws and policies, overall, the Kingdom should improve the coordination between those who play a key role in international cooperation and the fight against ML/TF. Although the mandates of the three committees are defined in their charters, some of the mandates of the three committees overlap. This could have been solved in practice, however, the assessment team received different views on the mandates from the different bodies, based on different interpretations of different legal documents (charters of the respective groups vs. the AMLS) (see Section 6.3 of this Report). This is despite the fact that some representatives serve in more than one body (which in itself is supported by the assessment team).

806. Another concern is the quality of the coordination; see for example the initial failure of the authorities to draft a cash reporting form that is in line with the AMLS (see section 2.7 of this report). During the on-site meetings it appeared often that stakeholders that are responsible for implementing the FATF Recommendations were not fully aware of the actual requirements set by the FATF Standards. Operational coordination among law enforcement bodies (including the FIU), and coordination between the FIU and supervisory bodies appeared to be sound.

6.1.2 Recommendations and Comments

807. While operational coordination is sound, on the policy level the Kingdom has set up a framework for policy coordination that is not as effective as it should be. The authorities should better coordinate and

[90] Royal Decree S/20167, dated 10/10/1422 AH (25 December 2001).

streamline the mandates and work of the main coordinating bodies. The authorities should also ensure that there is sufficient information flowing to ensure a proper understanding and implementation of the FATF Standards.

6.1.3 Compliance with Recommendation 31

	Rating	Summary of factors underlying rating
R.31	**LC**	• Coordination on the policy level is insufficiently effective.

6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)

6.2.1 Description and Analysis

Recommendation 35 and Special Recommendation I

808. The Kingdom has ratified the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988 (the Vienna Convention) on 9 January 1992. The Kingdom issued implementing rules[91] on 30 November 1998. These rules contain all the elements necessary for implementation of the Vienna Convention.

809. The Kingdom has signed (12 December 2000) and ratified (18 January 2005) the United Nations Convention against Transnational Organized Crime (the Palermo Convention). The Kingdom has not issued implementing rules for the Palermo Convention, but provided the assessment team with an overview of the *de facto* general coverage of the Palermo Convention[92]. This overview highlights the efforts made by KSA in relation to Palermo implementation; however, on the basis of this overview it was not possible for the assessment team to confirm the full implementation of this Convention. Thus, although there does not appear to be any implementing legal provisions in issues such as those relating to the definition of organized crime or the protection of witnesses or victims, the criminalization of laundering of proceeds of crime and the adoption of measures to combat money laundering (Article 6 and 7 Palermo Convention) are covered through the AMLS.

810. In addition to this, the criminalization of corruption and the adoption of measures against corruption (Articles 8 and 9 of Palermo Convention) are implemented at domestic level through the Anti Bribery Regime and Jurisdiction (Article 15 Palermo Convention) is also implemented through the CPC. With regard to the TF Convention, the Kingdom has signed (29 November 2001) and ratified (23 August 2007) this Convention. Although some elements of the TF Convention appear to be covered in the AMLS, this is not the case for the majority of the requirements of the Convention that should be implemented[93]. As with all FATF assessments, the statement that an international instrument is implemented automatically because it becomes part of the national law through ratification is not considered to equal (effective) implementation.

[91] Resolution No. 168 of 11/8/1419 AH.

[92] Recommendation 35 requires Articles 5-7, 10-16, 18-20, 24-27, 29-31 and 34 to be implemented.

[93] Recommendation 35 and Special Recommendation I require Articles 2-18 of the TF Convention to be implemented.

811. The Kingdom has ratified 13 out of 13 terrorism related UN Conventions, however the authorities could not establish that the conventions have been implemented, especially with respect to the criminalisation of the criminal conduct. As with all FATF assessments, the statement that an International instrument becomes part of the national law through ratification is not considered to equal (effective) implementation.

812. Saudi Arabia has not implemented the full range of measures relating to the freezing of TF funds under the United Nations Security Council Resolutions 1267 and 1373 and successor resolutions (to various degrees). See section 2.4 of this report for a full overview of the implementation of UNSCR 1267 and 1373 and successor resolutions.

Additional elements

813. The Kingdom joined *(i)* the GCC Convention for Combating Terrorism[94]; *(ii)* the 1999 Islamic Conference Organization Convention for Combating Terrorism[95]; *(iii)* the GCC Code of Conduct Rules for Combating International Terrorism[96]; and *(iv)* the Arab Convention for Combating Terrorism[97].

6.2.2 Recommendations and Comments

814. It is difficult to assess compliance with the Recommendations in the absence of information that would prove that Saudi Arabian law meets the requirements set out in the Palermo and TF Conventions. As regards the Vienna Convention, the implementing rules contained in Resolution No. 168 of 11/8/1419 AH can be considered to meet the requirements of that convention. As regards the TF Convention, AMLS Article 2 only punishes the financing of terrorism. This does not mean that the whole convention has been implemented. Neither does the fact that bilateral agreements exist to combat TF mean that the TF Convention has been implemented. As regards the Palermo Convention, it has to be noted that although there does not appear to be any implementing legal provisions, parts of the Convention provisions are included in the domestic legal framework.

815. It is recommended that Saudi Arabia fully implements the Palermo and TF Conventions, as well as UNSCR 1267 and 1373 (where applicable, see section 2.4 of this report), to correct the deficiencies noted in relation to the implementation of the relevant international conventions and UNSCR as soon as possible.

6.2.3 Compliance with Recommendation 35 and Special Recommendation I

	Rating	Summary of factors underlying rating
R.35	**PC**	• Palermo Convention not fully implemented. • TF Convention not implemented
SR.I	**NC**	• TF Convention not implemented • The failings related to UNSCRs 1267, 1373 and successor resolutions have a negative impact on this Special Recommendation.

[94] Royal Decree No. (M/52) dated October 5, 2005 (2/9/1426 H)
[95] Royal Decree No. (M/31) dated November 3, 2000 (5/8/1421 H)
[96] Council of Ministers Resolution No. (129) dated March 29, 1994 (16/10/1414 H)
[97] Royal Decree No. (M/16) dated October 2, 1998 (10/6/1419 H)

6.3 Mutual Legal Assistance (R.36-38, SR.V)

6.3.1 Description and Analysis

Recommendation 36

General description

816. Saudi Arabia has a framework for MLA, based on provisions of the Vienna Convention that have been implemented (Criminal Procedure Code), and for AML/CFT cases as provided in the AMLS (Articles 23 and 24).

817. To coordinate MLA issues and requests, the Kingdom has set up the PCMLA (see also Section 1). This Committee can handle all cases. According to the AMLS, the PCMLA is the competent authority to handle ML/TF cases (Article 23.1). According to the PCMLA, TF cases fall within the jurisdiction of the PCCT. The PCCT indicated that TF cases should be received from abroad through the PCMLA (see also Section 6.1 of this report).

818. The PCMLA's founding charter stipulates the following tasks: *(i)* receiving requests from other countries whether through diplomatic channels or through INTERPOL Riyadh; *(ii)* classifying requests in terms of their dates of receiving, their importance, their subject, the name of the country requesting assistance, and whether the country requesting assistance is connected with the Kingdom by international, regional or bilateral agreements; *(iii)* studying requests in terms of form, ensuring their completion of conditions, data and documents provided for in agreements, and indicating discrepancies, if any, or any inquiries, clarifications, or data with the aim of facilitating the implementation of the request; *(iv)* coordinating with the competent authority or authorities to study the request in terms of subject and the extent of the possibility of its implementation; and *(v)* following up assistance requests referred to the competent authority or authorities. In order to handle these requests, the PCMLA meets twice a month (but it could meet more often if necessary to deal with urgent requests. It was not clear whether the regular frequency of these meetings is sufficient to process the request expeditiously, however, the authorities explained that the frequency is sufficient considering the limited number of requests received and that additional meetings can be held if necessary (also on an urgent basis).

819. In practice, the Prosecution Authority is the authority that handles most MLA and extradition requests directly, as it seems outside the PCMLA framework, but according to the authorities also as a follow-up to forwarded PCMLA requests. The Prosecution was the only authority that was able to provide the team with practical background information on handling MLA requests. The Prosecution, as the leading law enforcement agency, is able to cooperate with foreign parties, and does so as part of its daily business.

820. However, it seems that the overall implementation of MLA requests in Saudi Arabia suffers from a low level of coordination given the involvement of multiple actors and the lack of a clear follow up procedure, which considerably slows down the procedure to implement those requests.

Range of mutual legal assistance

821. As noted in the previous FATF evaluation (2004), the KSA has a range of conventions, treaties multilateral and bilateral agreements that provide for general international cooperation particularly within the Middle East and GCC regions. The Kingdom also concluded additional bilateral agreements in the field of judicial and security cooperation after the conclusion of the last evaluation with a number of jurisdictions (Chad, India, Italy, Morocco, Senegal, Sudan, Syria, Turkey, United Kingdom and Yemen). The Kingdom can also provide MLA outside the framework of a treaty, on the basis of reciprocity[98].

822. Generally speaking, the Saudi authorities indicated that they are flexible as regards most types of mutual legal assistance *i.e.* taking of evidence or statements from persons, providing originals or copies of relevant documents or the identification, freezing, confiscation or seizure of assets. The AMLS only makes provision in relation to the implementation of requests for the identification, freezing, confiscation and seizure of assets related to ML (AMLS, Articles 23 and 24), however, other such examples can be found in article 14 of the Riyadh Arab Agreement for Judicial Cooperation، in article 9 of the Arab Convention on the Suppression of Terrorism، in the GCC Counter-Terrorism Agreement (article 27-14)، article 14 of the Agreement for Security Cooperation between the Kingdom of Saudi Arabia and the Great Socialist People's Libyan Arab Jamahiriya، article 2 of the Agreement for Security Cooperation between the Kingdom of Saudi Arabia and the Republic of Senegal، Article (2) and finally in the Cooperation Agreement for Fighting Crime between the Kingdom of Saudi Arabia and the Republic of Italy.

Timeliness of mutual legal assistance

823. There are no provisions in the law for the timeliness of MLA requests. According to the foundation chapter of the PCMLA, it stipulates that this institution is responsible for the follow up on assistance requests which are referred to the competent authority or authorities for implementation. Requests under AMLS Article 23 must pass through PCMLA and are referred to the Prosecution Authority.

824. The PCMLA is a large committee of 16 members. At first sight, this may be cumbersome and time consuming. One of the concerns raised in the previous FATF evaluation was that the requirement for all mutual legal assistance requests to pass through a single body (at that time, SAMA) could delay or impede the fulfillment of foreign requests. It was suggested that SA should take steps to ensure that this did not occur and should also enter into bilateral agreements for the exchange of AML/CFT information between regulatory authorities. However, it is not clear whether the creation of the PCMLA has sufficiently improved the situation.

825. In addition, one of the main difficulties in the implementation of MLA requests (AMLS, Article 24) is the level of coordination and clear definition of functions between different policy committees and institutions such as the Board of Grievances or the Prosecution Authority.

Conditions for mutual legal assistance

826. The PCMLA has issued Rules on how to handle MLA/CFT requests, which do not set out any grounds for refusal of MLA/CFT requests, which is acceptable. The authorities stated that in practice, the

[98] Royal order no (4/b/1194) and dated 23/1/1418H and article 23 and 24 AMLS

circumstances listed in Article 7(15) of the Vienna Convention would constitute grounds to refuse a request. Also, requests are always refused if they contradicted *Shari'ah*, threaten the security of Saudi Arabia, or if responding to a specific request would contradict one of the basic principles of Saudi Arabia.

827. Non-compliance with MLA requirements as set in AMLS Article 23.4 would be sufficient to reject a request. However, the PCMLA would request the foreign country to provide the missing information by attaching a list of the formal requirements included in the AMLS. These requirements do not seem to be an obstacle to implement foreign mutual legal assistance requests.

Process for mutual legal assistance

828. The Saudi authorities indicate that, by establishing the PCMLA and defining its tasks in its founding charter, the KSA has a clear and efficient process for the execution of MLA requests. However, the PCMLA founding charter only sets out the tasks of the Committee; it does not prescribe the process that needs to be followed. As described earlier, even among competent authorities in the Kingdom there are different views about which Committee has which role in MLA.

Fiscal matters

829. MLA requests (on ML or TF) are not refused solely on the basis that the predicate is also considered to involve tax matters. For background purposes only, it should be noted that there are only a few and very limited taxes in the Kingdom (the tax revenue as percentage of GDP is only around 5%) and that the punishment for evasion of the taxes that exists is limited. However, the FATF Standard does not require a state to collect taxes, nor does it require a country to criminalize tax evasion, nor does it require a country to designate tax evasion as a predicate offence for ML.

Confidentiality requirements

830. The AMLS provides that information disclosed by FIs and DNFBPs, can only be shared if this does not prejudice existing confidentiality provisions and practices. Besides, information can only be exchanged through the FIU, not through other law enforcement agencies and the PCMLA. It should be noted (see Section 2 of this report) that the FIU can only get information from FIs and DNFBPs through other supervisors and law enforcement entities. Finally, the information exchanged on this basis can only be used for the purpose it is requested for and only be disclosed to a third party (which, in practice, could be a judge) upon explicit approval of the FIU (AMLS, Article 22). In this regard, see AMLS Articles 8 and 22 which provide an exemption from the requirements of banking secrecy and specifically allows for the sharing of information disclosed by (non-)FIs.

Conflict of jurisdiction

831. The Court Law and the Criminal Procedure Law contain extensive provisions on how to deal in cases when conflict of jurisdiction arises. Most of the explanations provided by the Saudi authorities related to how criminal jurisdiction is determined in Saudi Arabia (location of offence, nationality of accused etc.) rather than what happens in cases of conflict of jurisdiction. Brief mention is made of special provisions under bilateral agreements with other states but these appeal to be general in nature dealing with *e.g.* how to prevent conflict in investigations. The PCMLA, however, seems unaware of the potential problem conflict of jurisdiction may cause. In their view, a crime is always committed somewhere, which

automatically defines the place of jurisdiction. In addition, it also seems that KSA would not be keen to waive jurisdiction in favor of other countries; instead, Saudi Arabia appears to retain jurisdiction over all investigations, except in cases where real estate located outside the Kingdom is involved.

Recommendation 37

Dual criminality

832. Dual criminality is only a requirement in relation to extradition but not for any other forms of MLA. Articles 23 and 24 do not require dual criminality to assist countries in tracing, freezing, seizing or confiscating proceeds or instrumentalities of crime. This view was also confirmed by the Saudi authorities, which indicated that there is no need for dual criminality in relation to the execution of requests for mutual legal assistance.

Dual criminality in case of extradition

833. In case of extradition, dual criminality is required; however, the Saudi authorities would focus on the conduct underlying the offence, not on the strict language of the criminalisation The Saudi authorities illustrate this point by reference to Article 22 of the GCC Convention, and a whole range of other agreements[99] (see also section 6.4 of this report).

Statistics (Recommendation 36 and Recommendation 37)

834. The team received two sets of statistics. In the written answers before the on-site, the authorities reported that since PCMLA was established in 2004, fifteen requests for MLA were received, of which three related to terrorism offences, eight related to ML and two were unrelated to ML or terrorism financing. Out of the eight requests relating to ML, seven were granted and implemented and one was still pending. No requests had been rejected by PCMLA and PCMLA had not received any request to implement a foreign confiscation order. However, during the on-site, PCMLA insisted that since 2004 it had only ever received one foreign MLA request. That request related to ML and was granted. In the follow up to the on-site, the authorities again updated the number of cases. Out of thirteen MLA cases, 8 were related to ML, 3 to TF and 2 MLA requests were unrelated to AML/CFT. The final statistics are closer to the original statistics. However, the confusion remained and was enforced by the fact that, apparently, the Kingdom has only received around 13 MLA requests since 2004 of which 11 (85%) are related to AML/CFT.

[99] Examples are: Article (38) of Riyadh Arab Agreement for Judicial Cooperation stated on extradition "Each contracting party hereby undertakes to extradite persons found on its territory charged with having committed a crime by the competent authority or convicted of having done so by a judicial body of any other contracting parties, subject to the rules and conditions laid down in this Part". Article (5) of The Arab Convention on the Suppression of Terrorism stated "Each of the states parties shall undertake to extradite the accused or the persons convicted with the terrorist crimes, who are requested to be extradited by any of these countries according to the rules and conditions provided for in this convention". Article (6) of the Arab Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances states "each member state without any delay notify the other state if a national of the later committed a crime provided in article (2) paragraph (1) of this convention and notify the general assembly". The GCC Counter-Terrorism Agreement stated on extradition "Each of the states parties shall undertake to extradite the accused or the persons convicted with the terrorist crimes, who are requested to be extradited by any of these countries according to the rules and conditions provided for in this agreement".

835. The following eleven AML/CFT requests have been received by the PCMLA: 2 request through MOFA (from Turkey); six requests through Interpol (from Iraq, Lebanon, Syria and the UK); one through law enforcement (from France), one through the SCIPP (from Australia); and one through MOI (from Switzerland). See the Annex for a table with more information on these MLA cases.

Effectiveness (Recommendation 36 and Recommendation 37)

836. There are several factors that reduce the effectiveness of MLA in the country. Although there is a legal framework for MLA in place, several issues should be improved, mainly, coordination between different institutions involved in the implementation of mutual legal assistance requests. For instance, the rules implementing the Vienna Convention contain provisions that are important for international cooperation (*cf* rule 12 on jurisdiction and rules 14 *et seq.* on international assistance), but their application and interpretation are unclear. There is no system to allow for the monitoring of the execution of mutual legal assistance requests (no deadlines by which the request must be met, for instance). Although in theory, AMLS Articles 23 and 24 confer the task of executing mutual legal assistance requests on the PCMLA, following the on-site visits, it is not clear how the different institutions coordinate the execution of the requests. It is also not possible to confirm the effectiveness of the system, due to a lack of a single set of comprehensive statistics.

837. In view of the statistics provided to the evaluation team and the above-mentioned key issues, it is difficult to ascertain the type of requests received in relation to ML and TF, as well as the time needed for their execution.

Recommendation 38

General framework

838. As is described in section 2.3 of this report (Recommendation 3), Saudi Arabia has two frameworks for confiscation, freezing and seizing of proceeds of crime. The first framework is based on provision of *Shari'ah* and applies to all proceeds of crime. The second framework is based on the AMLS and the CPL and, targets the proceeds of ML (as a part of the sanction provisions for ML).

839. AMLS Article 23 is a specific mutual legal assistance provision for the offence of ML/CFT, defined by reference to "property, proceeds and instrumentalities" in Article 16. However, this targets only funds related to ML crimes, not to funds related to other crimes (predicate offences), as these are governed by their own laws and regulations that target it such as anti drugs and psychotropic substances, anti bribe, forgery, currency counterfeiting and anti cyber crimes.

840. In case of the need to provide an effective and timely response to MLA request by other countries related to the identification, freezing, seizure or confiscation of any funds related to predicate offences, the regular MLA channels through the MOFA need to be used. Such measures may be also taken based on provisions in other laws (*i.e.* article 9 Anti-Drugs Law, article 29 Procedure Before Shari'ah Court Law) or based on the provisions of signed conventions[100].

[100] There are arrangements to coordinate the seizure and confiscating procedures with other states as stated in the bilateral agreements. Examples are: articles 1 and 2/8 of the cooperation agreement with the Republic of Sudan; articles 1 and 2/5 of the cooperation agreement with the Republic of Senegal; articles 1 and 2/8 of the cooperation

Corresponding value (ML cases only)

841. There is no specific provision regarding the confiscation or seizure of property of corresponding value and international cooperation. However it is arguable that AMLS Article 16 could apply in these circumstances. Nevertheless, the wording of this Article would seem to suggest that rather than applying to international cooperation, it exclusively relates to confiscation in domestic cases. In addition to AMLS Article 24, this would only cover "final judicial judgments", which in the view of the assessment team relates to confiscation, but excludes identification, freezing and seizure.

Coordinating actions with other countries (ML cases only)

842. Despite the fact that there is a specific provision (AMLS, Articles 23 and 24) for the implementation of foreign request to trace, identify and seize property and for the making of a confiscation order, it seems that the authorities have set up arrangements for coordinating seizure and confiscation actions with other countries. They, however, rely on coordination on a case by case basis through communication between the relevant authorities and by bilateral agreements (see above for these agreements).

Asset forfeiture fund (ML cases only)

843. The Kingdom has considered establishing an asset forfeiture fund. The AMLS provides that the competent authority may dispose of the proceeds "according to the law or share them with other countries". As a result, the AMLS directs that in ML cases related to drugs cases confiscated funds should be transferred to an independent SAMA account and used to cover the needs of the Anti-Drugs Directorate (ADD). In all other cases, confiscated funds or items are to be deposited with the State Treasury (AMLS, Article 15-5.c).

Sharing confiscated assets (ML cases only)

844. The AMLS contains a provision that directs competent authorities to share confiscated assets with other countries. There is a need for an agreement or a treaty, which are in place (see above). A request for confiscation of funds, proceeds or means must be specified in the prosecution's indictment and in the judicial decision rendered by a Court (AMLS, Article 15.3).

Statistics and effectiveness (Recommendation 38 only)

845. The authorities could not provide any statistics to prove the effectiveness of the system, but according to the authorities, this is because the Kingdom did not receive any request.

6.3.2 Recommendations and Comments

846. There is a clear need to establish effective procedures for the implementation of requests for legal assistance which allow, in particular, for the follow-up of the execution and response to the request by the local authorities involved. In this connection, there should be a central body with responsibility for the

agreement with the Republic of Italy; and finally articles 1/1 and 7/3/c of the cooperation agreement with the United Kingdom.

coordination of follow-up of such requests. The PCMLA would seem to fit this role, regardless of the subject matter of the request, even though it should improve the coordination role and ensure the monitoring procedure in the implementation of requests by the competent authorities (as set out in its founding charter) and be fully aware of its functions under Articles 23 and 24 of the AML.

847. Due to a lack of a single set of comprehensive statistics, it was not possible to confirm effectiveness. Nevertheless, the statistics that are available do not confirm the presence of an effective system for MLA either.

848. The shortcomings related to Special Recommendation II (criminalisation of TF, as described in section 2.2 of this report), may have a negative effect of the implementation of this recommendation.

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**	• The PCMLA should improve its coordination role in order to ensure the effective follow up of the implementation of foreign MLA requests. • No legal framework or effective mechanism for dealing with conflicts of jurisdiction which causes uncertainty about the willingness to retain jurisdiction over every investigation in these conflicts of jurisdiction cases. • The deficiencies in the TF criminalization may impact on the ability to provide MLA
R.37	**LC**	• Not established that that there are no practical impediments for dealing with dual criminality in extradition cases
R.38	**PC**	• There is no specific provision regarding the confiscation or seizure of property of corresponding value and international cooperation • Effectiveness cannot be assessed as a result of lack of implementation. • No legal framework for dealing with non-ML MLA confiscation cases. • The deficiencies in the TF criminalization may impact on the ability to provide MLA
SR.V	**PC**	• The deficiencies related to Recommendations 36 to 40 have a negative effect on the rating of this Recommendation.

6.4 Extradition (R.37, 39, SR.V)

6.4.1 Description and Analysis

Recommendation 39

ML and TF as extraditable offences and extradition of Saudi nationals

849. Both ML and TF are extraditable offences. The terms of extradition are set out in the multilateral, regional and bilateral agreements concluded by the KSA, as well as in law. ML is an extraditable offence under Saudi law. Extradition requests may be granted pursuant to a multilateral, regional, or bilateral agreement or on the basis of reciprocity. Article (42) of the basic law states "Laws and International Conventions determine basis and measures of extradition' constitute the basis for extradition by Saudi

Arabia". The Agreement on Criminal Extradition between Egypt, Jordan and Saudi Arabia[101], the Arab Riyadh Agreement on Judicial Cooperation[102], the Arab Agreement on Terrorism Combating[103], and the GCC Security Agreement[104] constitute a basis for extradition by Saudi Arabia. In addition, Saudi Arabia has concluded a bilateral extradition agreement with Kuwait, Oman, Pakistan, Qatar, UAE, and Yemen. No information was available as to the full list of countries that KSA has bilateral of multilateral extradition treaties with. The assessment team would suspect that many countries (for example EU members states) would not be prepared to extradite with KSA on the basis of reciprocity given that KSA's legal system allows the death penalty and corporal punishments, especially for those crimes where these punishments are mandatory (see Section 1 of this report). This situation could be overcome by concluding more extradition agreements, which is currently missing.

850. Saudi Arabia does not extradite its nationals. However, as an exception, it is nevertheless permissible to extradite a Saudi citizen under the terms of bilateral agreements made with Bahrain and UAE, Qatar and Oman (as KSA pointed out) and under the GCC Security Arrangement if the crime for which the accused is sought is a *Hadd* crime (see Section 1) under *Shari'ah* law (Article 28) with a punishment for not less than 6 months.

851. The Arab Agreement on Criminal Extradition, to which the Kingdom acceded, stipulates the duality of incrimination in the laws of both countries – requesting extradition and requested to extradite – but if there is no punishment for the action in the laws of the requested country, or the prescribed punishment for the crime is in the requesting country, extradition is not mandatory unless the wanted person is the national of the requesting country or of another country that prescribe the same punishment. The Arab Riyadh Agreement on Judiciary Cooperation provides that each signatory party can refrain from extraditing its nationals.

852. As a general rule, extradition of Saudi nationals can only be granted based on dual criminality. However, if the person is a national of the requesting country, the request may be granted even in the absence of dual criminality. Equally, if the person to whom the request pertains is a national of a country in which the offence is criminalized, the request may be granted even if the conduct in question is not criminalized under Saudi law. In cases where dual criminality is required, the Saudi authorities would focus on the conduct underlying the offence, not on the strict language of the criminalisation (see above on Recommendation 37, and article 22 of the GCC Convention)

853. Where extradition of a Saudi national is requested and denied, Saudi Arabia prosecutes the person according to International Agreements (see for example Articles 7 of the Agreement on Criminal Extradition between Egypt, Jordan and Saudi Arabia and 39 of the Arab Riyadh Agreement on Judiciary Cooperation). However, no domestic provision has implemented these agreements and the legal basis for the prosecution of those cases, in which extradition has been rejected remains unclear. While on-site, the authorities could not give any practical examples or statistics of this kind of cases, however, at a later stage the authorities indicated that in 133 cases Saudi Arabia had prosecuted its own nationals. It remains unclear how many of these cases relate to ML/TF cases, what the timeframe for these 133 cases was and if the

[101] The official name is the Arab League Extradition Agreement (1954)
[102] Royal Decree No. (M/14) dated 12/8/1420H
[103] Royal Decree No. (M/16) dated 10/6/1419H
[104] Royal Decree No. (M/3) dated 26/10/1415H

Kingdom cooperated with the other country, in particular on procedural and evidentiary aspects, to ensure the efficiency of the prosecution.

854. Requests for extradition are processed by the MOFA, in normal circumstances, and by the Interpol office in Riyadh, in urgent cases. The requests are then referred to the Ministry of the Interior. The Prosecution Authority issues the arrest warrants and deals with the substantive and procedural aspects of the extradition. Extradition requests must include information on the date and place of the conduct for which extradition is sought, a description of the act and copy or description of any legal and statutory provisions that apply. A copy of any relevant witness statements or other evidence has to be included as well.

Statistics

855. From 2004 to 2009, the Saudi authorities recorded 322 cases of extradition requests from a variety of countries, none of them regarding ML. In 189 cases, the request was granted, in 133 cases the request related to a Saudi national. No other requests were refused. Considering the lack of regular MLA, the assessment team wondered if this relative high number of extradition cases would also include unilateral expulsion or deportation from the Kingdom. The assessment team unsuccessfully requested an overview of the jurisdictions that had requested extradition for each year.

Effectiveness

856. The overall system for extradition seems to be effective and there is no reason to believe that extradition in ML cases would be less effective. It is somewhat confusing that the effectiveness of the systems for regular MLA (Section 6.3 of this report) differs so much from the system for extradition MLA (with respect to effectiveness). There is a concern related to the limited number of extradition treaties/agreements and the requirement of reciprocity in cases where an agreement is absent.

6.4.2 Recommendations and Comments

857. There is a need to implement International Agreements at domestic level in order to establish a clear basis that permits the prosecution of those citizens whose extradition has been refused. In addition to this, these provisions should also establish a framework of cooperation with foreign authorities, in particular at the level of the collection and admissibility of evidence, for the effective prosecution of those individuals. Additionally the Kingdom should conclude extradition agreements with more countries and do not narrow the scope of extradition requests in view of the reciprocity principle. The nature of the statistics could not be fully understood or analyzed, which makes that effectiveness, although likely, could not fully be confirmed.

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**	• Unclear if and how KSA authorities submit the case to its competent authorities for the prosecution of the offences where extradition has been refused • Extradition on the basis of reciprocity not effective • Overall effectiveness of the system could not fully be confirmed

R.37	**LC**	• Not established that that there are no practical impediments for dealing with dual criminality in extradition cases
SR.V	**PC**	• The deficiencies related to Recommendations 36 to 40 have a negative effect on the rating of this Recommendation.

6.5 Other Forms of International Cooperation (R.40 & SR.V)

6.5.1 Description and Analysis

858. The legal framework for international cooperation for any authority in Saudi Arabia is based on the agreements and treaties as described in Sections 6.2 to 6.4 above:

859. International cooperation is based on the Basic Law (article 70), the Council of Ministers Law (article 20) and the *Shurah* Council Law (article 18) which stipulate that international conventions, agreements and privileges can be issued and amended by virtue of Royal decrees after being studied by the Council of Minister, or the *Shurah* Council respectively.

FIU to FIU exchange of information

860. SAFIU has the ability to exchange information with its foreign counterparts on the basis of a valid agreement, convention, or on the basis of reciprocity. SAFIU, as a law enforcement agency, can also cooperate with foreign FIUs through the Interpol (AML, articles 11 and 22). The following number of requests have been received and made. It should be noted that the numbers are not high, but that SAFIU joined the Egmont Group of FIUs only recently in June 2009. The joining of the Egmont Group should have a positive future effect (as is shown in the table below).

Number of incoming and outgoing request 2005 – 2009 (responded requests shown in brackets)						
	2005	**2006**	**2007**	**2008**	**2009[105]**	**Total**
Incoming	0	4 (4)	6 (6)	15 (15)	37 (35)	62 (60)
Outgoing	0	1	0	1	14	16

861. SAFIU has also organized a number of meetings with other FIUs (Australia, United States) and visits to more FIUs are planned. SAFIU also received visitors from other FIUs (Canada, Germany, Japan, Korea, Senegal, United Kingdom, and the United States).

862. MOUs concluded with Egmont Group members is the practical gateway or mechanism for SAFIU to facilitate and allow for prompt exchange of information. This is not only a requirement or policy for SAFIU, according to the authorities, the non-membership of SAFIU if the Egmont Group at the time of the on-site visit, caused foreign FIUs to decline cooperation[106]. Accordingly, at the time of the on-site visit,

[105] As the on-site visit took place in March 2009, the normal two months rule for including information into an assessment would exclude any statistics from after 11 May 2009. However, all statistics for 2009 are included for information to show the latest trend.

[106] After SAFUI was granted Egmont membership (outside the time period for this assessment), SAFIU sent letters to 60 foreign FIUs with a request for an MOU.

no such MOU had been concluded. Pending Egmont Group membership, SAFIU had exchanged information with FIUs from Bahrain, Egypt, the UAE and Senegal. As SAFIU is a police FIU, information can be exchanged with other FIUs through INTERPOL. This has been done with Belgium, France, Germany and Switzerland.

863. Information can be shared upon request, for ML and predicates. It is not known if information can be shared by SAFIU with foreign counter parts spontaneously, but the authorities indicate that articles 11.3.d and 22 AMLS provide the basis for such exchange (no statistics were available).

864. SAFIU can search its own database upon request of foreign counterparts, it is not known if SAFIU can conduct inquiries within KSA (*i.e.* search other databases) on behalf of foreign counterparts, but the authorities indicate that articles 11.3.d and 22 AMLS provide the basis for such exchange (no statistics were available).

865. SAFIU is permitted to investigate STRs, but domestic law does not authorize SAFIU to conduct other investigations. This means that it can also not conduct other investigations on behalf of foreign counterparts (which would only be required by the FATF Recommendations if SAFIU were permitted to do undertake such investigations).

866. The AMLS does not provide that SAFIU has to adhere to disproportionate or unduly restrictive conditions to be able to exchange information, but makes a general provision that information exchange should be based on established legal procedures and not prejudice financial (institutions) confidentiality. The assessment team is not aware of any such law posing any unduly restrictions to SAFIU to exchange information. The fact that a case would involve fiscal matters should not be a problem for SAFIU (AMLS article 22).

867. The AMLS clearly provides that information exchange by SAFIU should only be used for the purpose it is requested for and shall not be disclosed to a third party, except with the approval of SAFIU or of the foreign FIU. These safeguards bind SAFIU, as well as the foreign FIU (AMLS, article 22.3.a and b).

Law enforcement to law enforcement exchange of information

General framework

868. See also Sections 6.2 – 6.4 for treaty based law enforcement cooperation, which also provides for part of the overall law enforcement to law enforcement cooperation. In addition, the KSA has provided the authorities with statistics regarding information exchange related to the implementation of UNSCR 1267. These detailed statistics are not repeated in this report, but are acknowledged by the assessment team (and are, to a certain extent, the basis on which Special Recommendation is considered to be partially complied with. See also section 2.4 of this report on Special Recommendation III.

869. It is not known if law enforcement bodies can conduct investigations on behalf of foreign counterparts and what the legal basis for this is. No statistics were available.

870. It is not known what the practical gateways or mechanisms are for law enforcement entities (see below) to facilitate and allow for prompt exchange of information, but the INTERPOL channel seems to be the most used (see below). It is unknown what the legal basis is for this information exchange, but considering the number of reports, the assessment team considers that there is a legal basis.

871. Law enforcement bodies can share information upon request, for ML and predicates. It is not known if information can be shared by law enforcement bodies with foreign counter parts spontaneously and what the legal basis for this is. No statistics are available.

872. Law enforcement bodies can search their own databases upon request of foreign counterparts (the legal basis is unknown), it is not known if law enforcement can conduct inquiries with other bodies within KSA (*i.e.* search other databases) on behalf of foreign counterparts. The legal basis for this is not known, and there are no specific statistics.

873. The law does not provide that law enforcement bodies have to adhere to disproportionate or unduly restrictive conditions to be able to exchange information. If law enforcement bodies exchange information through SAFIU, article 22 of the AMLS applies (see above for FIU cooperation). The fact that a case would involve fiscal matters should not be a problem for law enforcement.

874. It is not known what the legal controls and safeguards are for law enforcement to ensure that information received is only used in an authorize manner, other than the provisions of the CPC. If law enforcement bodies exchange information through SAFIU, article 22 of the AMLS applies (see above for FIU cooperation).

General Directorate of Investigations (GDI)

875. The GDI exchanges information with other similar security authorities in many countries, and financial and security information was provided by KSA to other jurisdictions as shown below

Number of cases (information provided by KSA) 2004 – 2009		
Year	**Total number of cases**	***Specific figures on selected countries***
2004	**102**	*-*
2005	**76**	*Yemen 27*
		Pakistan 2
		Algeria 6
2006	**103**	*Yemen 47*
		Pakistan 2
		Algeria 34
		Libya 6
2007	**40**	*Yemen 25*
		Pakistan 1
		Libya 2
		Syria 12
2008	**40**	*Yemen 17*
		Pakistan 1
		Algeria 5

Number of cases (information provided by KSA) 2004 – 2009		
Year	**Total number of cases**	***Specific figures on selected countries***
		Libya 15
		Syria 2
2009[107]	**18**	*Yemen 6*
		Pakistan 6
		Libya 4
		Syria 2
Total	**379**	

INTERPOL based law enforcement cooperation

876. The authorities indicated that INTERPOL KSA cooperates with all INTERPOL bureaus around the world and that it receives large numbers of various types of requests on a daily basis. Turnaround time for a request is approximately 30 days. The authorities also provided statistics for the number of incoming and outgoing reports through INTERPOL. The following statistics on incoming (and outgoing) reports are available. 2004: 15506 (12135); 2005: 13063 (11465); 2006: 15137 (12691); 2007: 12576 (11718); 2008: 13699 (11133). The authorities also provided specific numbers on exchanges with Egypt, France, India, and the Unites States.

General Directorate for Anti-Drugs (GDAD)

877. GDAD participates in meetings of narcotics control directors held in GCC or Arab countries and at the annual drug-related meeting held by UN Commission on narcotic drugs. GDAD also takes part in the first and second group of the Arab Countries Narcotics Control Directors meetings, held twice a year for the discussion of all drug matters and issues related to the Near East and the Middle East.

878. GDAD has 18 liaison officers for information exchange, who were appointed to work in many countries. The table below shows the number of controlled delivery cases from 2005 to 2009:

Number of controlled delivery cases 2005 - 2009[108]		
Country	**Year**	**Controlled Delivery Cases**
Bahrain	2008 - 2009	1
UAE	2005 – 2009	10
Kuwait	2005 – 2009	1
Yemen	2005 – 2009	2
Pakistan	2005 – 2009	5

[107] Ibid.
[108] Ibid.

Number of controlled delivery cases 2005 - 2009[108]		
Country	**Year**	**Controlled Delivery Cases**
Jordan	2005 – 2009	6
Syria	2005 – 2009	5
Lebanon	2005 – 2009	4
Turkey	2005 – 2009	6

Customs

879. Customs cooperates with its counterparts through the Regional Intelligence Liaison Office (RILO), related to the World Customs Organization (WCO), based in KSA and established by Ministerial order[109]. The office facilitates the exchange of information on drugs, business fraud, money laundering, transformative chemical materials, intellectual property and other issues. Although Customs is a law enforcement body based on FATF Terminology, it is not in the KSA context (it is part of MOF) and it has limited law enforcement powers. Notwithstanding its hybrid character, there is no specific information available (legal basis, statistics) relating to any of the criteria for Recommendation 40 for Customs, except for the fact that the authorities indicate that it cooperates within the WCO/RILO framework exclusively.

Supervisor to supervisor exchange of information (SAMA and CMA)

880. The information in this subsection applies equally to SAMA and CMA.

881. It is not known what the practical gateways or mechanisms are for supervisory bodies to facilitate and allow for prompt exchange of information with foreign counterparts. No legal basis, and no statistics are available7

882. Supervisory bodies can share information upon request, for ML and predicates, but the legal basis is unknown and there are no statistics available. It is not known if information can be shared by supervisory bodies with foreign counter parts spontaneously. The legal basis is unknown, and there are no statistics available.

883. Supervisory bodies can search their own databases upon request of foreign counterparts, but the legal basis is unknown and there are no statistics available. It is unknown if supervisory bodies can conduct inquiries with other bodies within KSA (*i.e.* search other databases) on behalf of foreign counterparts (unknown legal basis, lack of statistics).

884. Supervisory bodies are not authorized to conduct law enforcement investigations. This means that supervisory bodies can also not conduct investigations on behalf of foreign counterparts (which would only be required by the FATF Recommendations if supervisory bodies were permitted to do undertake such investigations).

885. The law does not provide that supervisory bodies have to adhere to disproportionate or unduly restrictive conditions to be able to exchange information, but no practical information was available, and no statistics or examples could be given. If supervisory bodies exchange information through SAFIU,

[109] Ministerial Order no. 45 dated 17/3/1418 AH.

article 22 of the AMLS applies (see above for FIU cooperation). The fact that a case would involve fiscal matters should not be a problem for supervisory bodies.

886. It is not known what the legal controls and safeguards are for supervisory bodies to ensure that information received is only used in an authorize manner. If supervisory bodies exchange information through SAFIU, article 22 of the AMLS applies (see above for FIU cooperation).

887. With regard to financial information, SAMA and CMA are cooperating with foreign supervisory and controlling authorities with similar activities for supervision and control purposes. Both supervisors are entitled to exchange information with counterparts on the basis of bilateral and international agreements or on the basis of reciprocity. However, as a matter of policy, SAMA would not conclude such agreements / MOUs because it deems these are not necessary. No legal explanation was available, no statistic were available to indicate the effectiveness of this policy.

888. The authorities indicate that SAMA cooperates with foreign partners in the following ways:

- Cooperation and exchange with other central banks, through SAMA's membership of various international and regional organisations (IMF, World Bank, Arab Monetary Fund, and GCC related Gulf controlling and supervising commissions).

- Direct cooperation and information exchange with central banks, which may include information on AML/CFT issues. Examples of SAMA counter parts are Bahrain, Canada, Germany, the Bank of England, the UAE, and the U.S Department of the Treasury.

- Cooperation and exchange with other domestic authorities, in the knowledge that other domestic authorities may receive international cooperation requests that should be handled by SAMA. Cases will be transferred to SAMA and SAMA would contact the international counter parts to share the results of the inquiry.

- Cooperation and exchange through FIs. Instructions issued to FIs allow cooperation and the provision of information on customers and financial transactions, whether directly (FI to FI) or through the supervisory authority.

- Exchange of information related to insurance activities, through SAMA's membership in the forum of Arab authorities for control and supervision on insurance activities (includes an MOU, no requests are pending).

6.5.2 Recommendations and Comments

889. International cooperation in KSA is based on the broader framework for mutual legal assistance, and on the AMLS (articles 11 and 22). Within that framework, competent authorities are able to cooperate with their foreign counterparts. The authorities have provided statistics where these were available. The statistics indicate that competent authorities make use of the instruments for non-MLA based cooperation. In general, cooperation is based on a broad interpretation of the law, and the assessment team does not contest these interpretations were statistics are available. However, for a sufficiently large number of agencies, the assessors were unable to confirm a general or specific legal basis for cooperation. In addition, statistics or case examples were not always available.

890. International cooperation by the FIU is sound on paper, but effectiveness is very low[110].

891. Law enforcement bodies are able to cooperate with foreign counterparts. Several gateways are available to law enforcement bodies, such as direct contacts, INTERPOL and SAFIU. As with the FIU, the number of information exchanges on a case level is not too high. However, one should take into account that this could also be caused by the reluctance of third countries to cooperate with KSA, caused by the differences in the range of potential penalties available to authorities in KSA compared to those in third countries. However, it is the assessment team's view that this factor should not be considered a shortcoming that should be attributed to KSA in the context of this evaluation. The overall judgment of effectiveness benefits from the information exchanged through INTERPOL KSA.

892. There are several gateways for supervisory cooperation, but most of these concern policy cooperation and not information exchange. The assessment team could not establish that supervisory bodies cooperate effectively.

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	**PC**	• International cooperation by supervisors (SAMA and CMA) FIU (SAFIU) and Customs is insufficient. • There is an unclear legal basis for some forms of international cooperation by some law enforcement bodies • Lack of statistics to confirm effectiveness for most forms of international cooperation, especially by supervisory bodies and the FIU.
SR.V	**PC**	• The deficiencies related to Recommendations 36 to 40 have a negative effect on the rating of this Recommendation.

7. OTHER ISSUES

7.1 Resources and statistics

893. 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. Section 7.1 of the report will contain only the box showing the rating and the factors underlying the rating, and the factors should clearly state the nature of the deficiency, and should cross refer to the relevant section and paragraph in the report where this is described.

	Rating	Summary of factors relevant to Recommendations 30 and 32 and underlying overall rating
R.30	**LC**	• Some supervisory authorities (for both FIs and DNFBP) need more human and technical resources and training to carry out their respective roles effectively.

[110] However, with the recent admission of SAFIU to the Egmont Group, effectiveness is already rapidly improving. But this falls outside the time framework of this assessment.

	Rating	Summary of factors relevant to Recommendations 30 and 32 and underlying overall rating
		• Insufficient operational independence of supervisors
R.32	**PC**	Lack of complete or reliable statistics concerning: • overall statistics on penalties upon convictions are not available • some statistical uncertainly about the difference between ML and TF • no separate statistics available on the use of seizure provisions • fragmented statistics relating to the numbers of (AML/CFT) staff and budgets of LEAs • Customs statistics are not very clear and hamper the ability to draw workable (AML/CFT) conclusions • Lack of lawyers-related STR • No specific statistics are generated or kept in relation to the results FI supervisory inspections • statistics to prove the effectiveness (R.38)

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[111]
Legal system		
1. ML offence	**LC**	• The AMLS / jurisprudence do not clearly cover self-laundering and do not clearly extend to predicate offences - that would traditionally be regarded as predicate offences - committed abroad. • Effectiveness of ML provisions could not be fully confirmed (definition of ML and TF). • Shortcoming in of criminalisation of terrorist financing possibly limits the number of designated predicate offences to 19.
2. ML offence – mental element and corporate liability	**LC**	• Criminal liability does not extend to (all) legal entities and the extent to which administrative or civil sanctions apply is unclear. • Effectiveness of ML provisions could not be assessed (penalties)
3. Confiscation and provisional measures	**PC**	• Insufficient protection of bona fide third parties • Effectiveness of the CPC is not established: o due to the lack of implementation (insignificant number and amounts) o due to lack of experience with the CPC provisions • Effectiveness of the AMLS system is limited because: o the confiscation provisions are not implemented as widely as their mandatory nature suggests • The framework to request for provisional measures does not clearly cover predicate offences • Interaction between AMLS and CPC unclear.
Preventive measures		
4. Secrecy laws consistent with the Recommendations	**LC**	• Limitations on the sharing of information between domestic and foreign banks in the implementation of R.7 and SR.VII • Exceptions to confidentiality provisions in the sharing of information between entities and institutions, foreign and domestic, not explicit

[111] These factors are only required to be set out when the rating is less than Compliant.

Forty Recommendations	Rating	Summary of factors underlying rating[111]
5. Customer due diligence	**PC**	• CDD requirements for insurance companies and authorized persons were recently circulated (at the time of the Onsite visit) which suggests that the effectiveness could not be properly addressed. • No primary or secondary legislation guaranteeing numbered accounts are maintained in such a way that full compliance with the FATF Recommendations can be fully achieved. • Ongoing due diligence requirement was not provided explicitly by primary or secondary legislation. • Insurance companies are not explicitly required to terminate the business relationship and consider making a suspicious transaction report in case required CDD measures could not be applied to existing customers and to cases whereby the institution has doubts about the veracity or adequacy of previously obtained customer identification data. • Banks, money exchange businesses, insurance companies and authorized persons are not explicitly required to apply CDD requirements to existing customers on the basis of materiality and risk. *Effectiveness* • Performing CDD measures based on doubts about the veracity of previously obtained information is possibly not being implemented at most financial institutions. • The identification and verification process is insufficiently implemented at some financial institutions. With money exchange businesses, it appeared possible to conduct business transactions simply against submitting a copy of identity. • Many financial institutions do not obtain information concerning the directors of legal entities. There was evidence that proofs of incorporation of these entities have not been retained in several instances. Financial institutions demonstrated a flawed understanding of the requirement to obtain and verify beneficial ownership. Some institutions did not seem to inquire the client about it. When some financial institution proved to be verifying ownership, it stated to perform it “up to the third level”, and in other instances “up to first level”; as for understanding the control structure of legal entities, it seemed that institutions knew little about it. It was frequently noted that adopted KYC forms do not contain fields by which such information can be retained; institutions appeared to be satisfied with reliance on received copies of official documents (mainly commercial registration and Articles of Association) to collect the information required above (which does not makes it possible for shareholders of bearer shares companies). • The scrutiny of transactions for consistency with due diligence data is likely not being conducted by non-bank financial institutions. The reported reliance of many banks on specialized transactions monitoring software for such scrutiny does not include matching with KYC data. • For banks and money exchangers, the transactions monitoring threshold parameter of SAR 60,000 means that most customer relationships may stay below the radar, which would exclude the requirement to undertake CDD measures when there is a suspicion of money laundering or terrorist financing below this threshold. The quality and frequency of updating of CDD data appeared to be questionable concerning many financial institutions.

Forty Recommendations	Rating	Summary of factors underlying rating[111]
		• Due diligence measures are not satisfactorily applied by many financial institutions (limited perception of who could be a high-risk customer, no classification of customers according to risk). Enhanced diligence is not satisfactorily applied in some sectors. • At some financial institutions, some customer files do not contain key documents pertaining to the identification process: It is not clear whether this situation reflects a failure in performing timely identification and/or a failure in satisfying the requirement to refuse or terminate relationship and report accordingly. • The extent (mainly for official documents) and quality of updating was not proper at some financial institutions. The updating process has often not been completed. CDD information for existing business relationships at many non-bank financial institutions is not up-to-date.
6. Politically exposed persons	**PC**	• Definition of PEPs only covers current and recent PEPs, with no definition of "recent". • Financing companies are not explicitly required, in addition to performing the CDD measures, to put in place appropriate risk management systems to determine whether a potential customer, a customer or the beneficial owner is a politically exposed person. • Insurance companies, authorized persons and financing companies are not explicitly required to seek senior management approval for continuing the relationship in cases where a beneficial owner is subsequently found to be, or subsequently becomes a PEP. • Insurance companies are not required to determine the source of wealth and source of funds for beneficial owners identified as PEPs, as well as source of wealth for customers identified as PEPs. • Financing companies are not explicitly required to determine source of wealth and source of funds for clients or beneficial owners identified as PEPs. • Inadequate implementation of several components of the due diligence requirements towards PEPs, notably with respect to the risk management systems in place to spot PEPs at insurance companies and money exchange businesses, senior management approval for continuation of business relationship, verification of source of wealth and enhanced ongoing monitoring.
7. Correspondent banking	**LC**	• Some banks did not seem to be implementing adequate due diligence towards correspondent relationships, notably the ones already established.
8. New technologies & non face-to-face business	**LC**	• Measures undertaken by financial institutions to prevent the misuse of new technologies and non face-to-face business relationships for ML and TF purposes are not effectively implemented.
9. Third parties and introducers	**LC**	*Regulatory* • The rules do not bind financial institutions by a time frame in order to obtain immediately necessary CDD information from third parties. • Banks are not required to satisfy themselves that the third parties are regulated and supervised. *Effectiveness* • Non-bank financial institutions (mainly insurance companies) did not seem to apply adequate diligence towards relied on third

Forty Recommendations	Rating	Summary of factors underlying rating[111]
		parties.
10. Record keeping	**C**	This recommendation is fully observed.
11. Unusual transactions	**PC**	• Legal framework establishes monitoring for unusual transactions as a means for crime detection. • Monitoring obligation is not explicit for all sectors. • Effectiveness issues: o Lack of distinction and awareness of the difference between monitoring unusual transactions and STR reporting requirements negatively impacts monitoring process. o Deficiencies related to supervision and enforcement hinders effectiveness o Monitoring threshold parameters for banking and insurance
12. DNFBP – R.5, 6, 8-11	**NC**	• DNFBPs are not required to understand the ownership and control structure of a customer that is a legal person or legal arrangement. • DNFBPs are not required to obtain information on the purpose and intended nature of the business relationship. • Ongoing due diligence requirement is not provided explicitly by primary or secondary legislation. • DNFBPs are not required to scrutiny transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the entity's knowledge of the customer, their business and risk profile, and where necessary, the source of funds. • DNFBPs are not required to consider making a suspicious transaction report whereas required CDD measures could not be applied. • DNFBPs are not required to terminate the business relationship and consider making a suspicious transaction report in case required CDD measures could not be applied to existing customers and to cases whereby the institution has doubts about the veracity or adequacy of previously obtained customer identification data. In such instances, it is also not required to consider making a suspicious transaction report. • DNFBPs are not required to apply CDD requirements to existing customers on the basis of materiality and risk and to conduct due diligence on such existing relationships at appropriate times. • There are no enforceable obligations with regard to Politically Exposed Persons. • DNFBPs are not required to include specific and effective CDD procedures in their measures for managing the risks related to non-face to face customers. • There are no enforceable obligations with regard to introduced business. • Lawyers and TCSPs are not required to pay special attention to unusual patterns of transactions that have no apparent or visible economic or lawful purpose and to examine as far as possible the background and purpose of these. • DNFBPs are not required to set forth in writing the examination of the background and purpose of complex, unusual large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose; DNFBPs are also not required to keep such findings available for competent

Forty Recommendations	Rating	Summary of factors underlying rating[111]
		authorities and auditors for at least five years. • Inadequate implementation, reporting and supervision.
13. Suspicious transaction reporting	**LC**	• Shortcomings in the criminalization of terrorist financing limit the reporting obligation. • *Effectiveness issues*: o Effectiveness is inconsistent across and within sectors o Lack of clear distinction between unusual and suspicious activity hinders effectiveness of STR reporting o Low reporting levels raise concerns about the effectiveness of the system o Monitoring threshold parameter for banks and insurance companies promotes a de facto reporting threshold
14. Protection & no tipping-off	**C**	This recommendation is fully observed.
15. Internal controls, compliance & audit	**LC**	• Independence and adequate resourcing of the audit function not explicitly provided for in case of insurance and securities companies. Deficiencies related to supervision and enforcement hinders effectiveness, particularly in insurance and securities sectors.
16. DNFBP – R.13-15 & 21	**NC**	*Application of R.13* • Low number of STR filing from dealers in precious metals and stones and accountants indicates low effectiveness. • Absence of STR filing from lawyers and real estate agents indicates no effectiveness. • Insufficient awareness among entities regarding ML/TF risks and identification thereof. *Application of R.15* • No specific regulations or guidance issued for lawyers and legal advisors. • Lack of supervision and enforcement renders low effectiveness. • Insufficient awareness among entities regarding ML/TF risks and identification thereof. *Application of R.21* • No requirement applying to lawyers and legal advisors. • MOCI does not provide appropriate guidance for all covered DNFBPs and requirements are not enforced.
17. Sanctions	**LC**	• Low levels of corrective measures applied by both SAMA and CMA.
18. Shell banks	**LC**	• Effectiveness deficiencies relating to Recommendation 7 have a negative impact on the ability to fully comply with Recommendation 18.
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	**PC**	• Absence of counter-measures • Insufficient guidance regarding what is required of institutions with respect to identifying those countries that do not sufficiently apply the FATF Recommendations

Forty Recommendations	Rating	Summary of factors underlying rating[111]
		• Overreliance on FATF statements and uneven adherence across sectors and entities hinders effectiveness.
22. Foreign branches & subsidiaries	**LC**	• Deficiencies related to Recommendation 21 have a negative impact on the ability to fully comply with Recommendation 22. • Deficiencies related to supervision and enforcement hinders effectiveness, particularly in insurance and securities sectors.
23. Regulation, supervision and monitoring	**LC**	• Fit and proper procedures have not been tested against real case scenarios for existing financial institutions (in relation to ownership) and with regards to non-Saudi nationals. • Low number of human resources available for insurance and authorized persons supervision. • Lack of adequate training for CMA's AML unit staff. • Low number of AML/CFT related examination on authorized persons.
24. DNFBP - regulation, supervision and monitoring	**NC**	• No effective system in place to supervise and examine the compliance of DNFBs with AMLS and its implementing regulations. • Lack of expertise of ML/FT risks within competent authorities and DNFBs.
25. Guidelines & Feedback	**PC**	• Feedback is inconsistently applied and not adequately used as a tool to further the effectiveness of AML/CFT provisions • Insufficient guidance regarding ML and TF methods and typologies • Guidance issued by supervisory authorities is not comprehensive and not industry specific. • No specific guidelines have been issued to assist all DNFBs • No feedback has been provided by SAFIU
Institutional and other measures		
26. The FIU	**LC**	• Effectiveness is under pressure by the insufficient number of processed STRs. • Annual reports lack most of the required information.
27. Law enforcement authorities	**LC**	• Unclear if all investigation authorities other then the PA have sufficient awareness and knowledge to properly investigate ML/FT. • Operational effectiveness could not fully be established as statistics are not specific and MOUs were not submitted.
28. Powers of competent authorities	**LC**	• The effective use of powers for purposes of fighting ML and the effectiveness of operational law enforcement cooperation could not be established.
29. Supervisors	**LC**	• No adequate number of staff or expertise to carry out examination within Insurance Control Unit in SAMA or CMA • Low number of AML/CFT related examination tasks performed by SAMA and CMA.
30. Resources, integrity and training	**LC**	• Some supervisory authorities (for both FIs and DNFBP) need more human and technical resources and training to carry out their respective roles effectively. • Insufficient operational independence of supervisors
31. National cooperation	**LC**	• Coordination on the policy level is insufficiently effective.

Forty Recommendations	Rating	Summary of factors underlying rating[111]
32. Statistics	**PC**	Lack of complete or reliable statistics concerning: • overall statistics on penalties upon convictions are not available • some statistical uncertainly about the difference between ML and TF • no separate statistics available on the use of seizure provisions • fragmented statistics relating to the numbers of (AML/CFT) staff and budgets of LEAs • Customs statistics are not very clear and hamper the ability to draw workable (AML/CFT) conclusions • Lack of lawyers-related STR • No specific statistics are generated or kept in relation to the results FI supervisory inspections • statistics to prove the effectiveness (R.38)
33. Legal persons – beneficial owners	**LC**	• Lack of direct and spontaneous access to the Commercial register information by competent authorities.
34. Legal arrangements – beneficial owners	**LC**	• The assessment team was unable to confirm that beneficial ownership is available
International Cooperation		
35. Conventions	**PC**	• Palermo Convention not fully implemented. • TF Convention not implemented
36. Mutual legal assistance (MLA)	**LC**	• The PCMLA should improve its coordination role in order to ensure the effective follow up of the implementation of foreign MLA requests. • No legal framework or effective mechanism for dealing with conflicts of jurisdiction which causes uncertainty about the willingness to retain jurisdiction over every investigation in these conflicts of jurisdiction cases. • The deficiencies in the TF criminalization may impact on the ability to provide MLA
37. Dual criminality	**LC**	• Not established that that there are no practical impediments for dealing with dual criminality in extradition cases
38. MLA on confiscation and freezing	**PC**	• There is no specific provision regarding the confiscation or seizure of property of corresponding value and international cooperation • Effectiveness cannot be assessed as a result of lack of implementation. • No legal framework for dealing with non-ML MLA confiscation cases. • The deficiencies in the TF criminalization may impact on the ability to provide MLA
39. Extradition	**LC**	• Unclear if and how KSA authorities submit the case to its competent authorities for the prosecution of the offences where extradition has been refused • Extradition on the basis of reciprocity not effective • Overall effectiveness of the system could not fully be confirmed
40. Other forms of cooperation	**PC**	• International cooperation by supervisors (SAMA and CMA) FIU (SAFIU) and Customs is insufficient. • There is an unclear legal basis for some forms of international

Forty Recommendations	Rating	Summary of factors underlying rating[111]
		cooperation by some law enforcement bodies • Lack of statistics to confirm effectiveness for most forms of international cooperation, especially by supervisory bodies and the FIU.

Nine Special Recommendations	Rating	Summary of factors underlying rating
SR.I Implement UN instruments	**NC**	• TF Convention not implemented • The failings related to UNSCRs 1267, 1373 and successor resolutions have a negative impact on this Special Recommendation.
SR.II Criminalize terrorist financing	**PC**	• No stand alone statutory TF offence • TF not criminalized in line with the TF Convention • TF as a ML offence does not extend to all legal entities • Insufficient definition of funds as required by TF Convention • TF as a ML offence does not cover acts by terrorist organisations of less than 3 persons • Unclear if funds have to be used for a specific terrorist act or linked to a specific terrorist act. • The term "financing" does not clearly cover the collection of funds. • The term "terrorism or terrorist act" does not clearly cover the acts contemplated by Article 2(1)(b) of the FT Convention. • The financing of terrorist acts contemplated by Article 2(b) of the FT Convention in relation to conventions not yet ratified by the KSA are not covered. • Financing a terrorist organisation or individual terrorist for any purpose (*i.e.* not related to a terrorist act) is not covered.
SR.III Freeze and confiscate terrorist assets	**PC**	Regarding UNSCR 1373: • UNSCR 1373 is not implemented (no legal basis, no procedure) Regarding UNSCR 1267: • Freezing actions do not apply to a sufficiently broad range of funds or other assets. • No communication mechanisms for non-bank FIs and DNFBPs. • No guidance for non-bank FIs and DNFBPs. • Protection does not extend to a sufficiently broad range of bona fide third parties • Lack of clear monitoring and sanctioning procedures to verify implementation of freezing requests
SR.IV Suspicious transaction reporting	**LC**	• Shortcomings in the criminalization of terrorist financing limit the reporting obligation. • *Effectiveness issues:* o Effectiveness is inconsistent across and within sectors o Lack of clear distinction between unusual and suspicious activity hinders effectiveness of STR reporting o Low reporting levels raise concerns about the effectiveness of the system o Monitoring threshold parameter for banks and insurance companies promotes a de facto reporting threshold.
SR.V International	**PC**	• The deficiencies related to Recommendations 36 to 40 have a

Nine Special Recommendations	Rating	Summary of factors underlying rating
cooperation		negative effect on the rating of this Recommendation.
SR VI AML requirements for money/value transfer services	**LC**	• Deficiencies identified and ineffective implementation in relation to obligations required under other Recommendations (5, 6, 7, 8, 9, 11, 13, 15, 17, 21 and 23) affect the rating of compliance with SR.VI.
SR VII Wire transfer rules	**PC**	*Regulatory* • Beneficiary financial institutions are not required to adopt effective risk-based procedures for identifying and handling wired transfers that are not accompanied by complete originator information. *Effectiveness* • Customer address is not included on the wire transfer. • In relation to the rules that have been enacted to replace risk based procedures: Banking relationships are not likely to be terminated based on receiving wire transfers lacking originator information from a remitting bank. Reporting accordingly is not likely to be performed either. • The shortcomings identified under Recommendations 17 (sanctions) and 23 (monitoring and supervision) have a negative impact on this Special Recommendation.
SR.VIII Non-profit organisations	**LC**	• No review of the adequacy of domestic laws and regulations that relate to NPOs, no domestic reviews for the purpose of identifying the elements and types of NPOs that are at risk of being misused for TF by virtue of their activities or characteristics; and no periodic reassessments by reviewing new information on the sector's potential vulnerabilities to terrorist activities • Record keeping requirements unclear (terms and legal basis).
SR.IX Cross Border Declaration & Disclosure	**PC**	• There is no effective, proportionate and dissuasive sanctions regime in place. • The overall effectiveness of the system could not be established due to a lack of comprehensive statistics that inform and support the AML/CFT regime. • Statistics to include a comprehensive overview of cases under investigation/law enforcement and sanctions. • The failings of Recommendation 3 and Special Recommendation III have a negative impact on the rating of this Recommendation.

Table 2: Recommended Action Plan to improve the AML/CFT system

Recommended Action (listed in order of priority)	
1. General	
2. Legal System and Related Institutional	
2.1 Criminalisation of Money laundering Measures (R.1 & R.2)	• The Saudi authorities should be more precise in the formulation of the ML criminalisation and should strive for clear provisions that establish, without ambiguity the issues in relation to foreign predicate offences and the criminalisation of self-laundering. • The authorities are also urged to make a conceptual distinction in the AMLS between the ML and TF. This difference would also be useful to gauge and enhance the effectiveness of the AML system, which is currently not fully possible. • Criminal liability for legal entities should extend to all legal entities.
2.2 Criminalisation of Terrorist Financing (SR.1)	• The Saudi authorities are advised to enact a full statutory criminalisation of TF, structuring it as a separate offence from the ML offence, to replace the current reference to TF in Article 2(d) of the AMLS in order to meet the requirements set out in Article 2 of TF Convention but also to clearly distinguish money laundering and terrorism financing offences. • All elements of Special Recommendation II and the TF Convention should be covered in KSA • The TF Convention needs to be specifically implemented into statutory law.
2.3 Confiscation, freezing and seizing of proceeds of crime (R.3)	• Expand the statutory mechanism for provisional seizures. • The protection of third parties acting in good faith should be accompanied by complimentary measures that protect bona fide third parties and those acting in good faith regardless of whether such persons are involved in any violation. • The authorities should take steps to ensure a broader application of seizure and confiscation measures.
2.4 Freezing of funds used for terrorist financing (SR.III)	• UNSCR 1373 should be implemented. • The Saudi authorities should establish a clear legal basis and procedure for the implementation of UNSCR 1373, identifying the competent authorities with responsibility for implementation and a procedure to monitor the freezing of funds as well as a procedure for the implementation of penalties should the financial authorities fail to comply with their duty to freeze funds. • The role of the different actors involved in the implementation of the UNSCRs should be made clear and the mandates of PCMLA and PCCT should be made clear. • Compliance with provisions should be enforced and non-compliance sanctioned • The deadlines for freezing funds are not clear. These should be revised to ensure consistency with the wording of the UN resolutions, which specify that funds should be frozen “without delay”. • There is no definition of the funds that should be the subject of freezing orders that is consistent with the TF Convention or with the UNSCRs. This should be corrected.
2.5 The Financial Intelligence unit and its functions (R.26)	• The numbers of STRs and disseminations should be increased. • SAFIU and PCCML should step up the supply of information on ML/FT typologies, methods and trends to reporting entities and to supervisory bodies. • It is advisable to continuously to update the current Guidance Manual in order to help to reach these goals. • The backlogs at yearends of STRs that have not yet been analyzed require to be analyzed as inefficiencies may exist in the operational processes.

Recommended Action (listed in order of priority)	
	• FT is considered a form of ML in the AMLS. It is important that all reporting entities, supervisory bodies and other government bodies are made aware of the fact that TF in practice is not equal to ML. • A distinction should also be made between ML and FT in the statistics. • Statistics should pertain to longer periods of time in order to cater for historical data so as to help understand developments in reporting, analysis and dissemination. This will also serve feedback and increase substance. • Statistics could be more precise and informative and could show which indicators / criteria were used for reporting, analysis and dissemination, as well as the outcome of investigation and law enforcement and convictions. • To enhance the visibility of SAFIU and the usefulness of the annual report, the annual report should list current and planned activities and cases and typologies, methods and trends. • SAFIU's work would become more efficient if other authorities would give SAFIU direct access to their databases.
2.6 Law enforcement, prosecution and other competent authorities (R.27 & 28)	• Statistics relating to the numbers of (AML/CFT) staff and budgets should be available • Sufficient resources for AML/CFT should be available. • Investigation authorities other than the PA should also have sufficient awareness and knowledge of ML/FT to ensure that offences are properly investigated. • Cooperation between the investigation authorities and the PA should be coordinated
2.7 Cross Border Declaration & Disclosure	• The new declaration system should be fully implemented. • The lack of statistics and the lack of declarations should be addressed. • The sanctions for false or non-declaration should be made effective and not only target cash amounts above the threshold of SAR 60,000. • There should be administrative or civil sanctions. • Criminal sanctions should be less restrictive. • There is sanction regime should be made effective, proportionate and dissuasive.
3. Preventive measures – Financial institutions	
3.1 Risk of money laundering or terrorist financing	
3.2 Customer due diligence, including enhanced or reduced measures (R.5 to 8)	*Recommendation 5* • Effectiveness of the implementation of CDD requirements for insurance companies and authorized persons, which were recently circulated (at the time of the Onsite visit), should be properly improved. • There should be a guarantee in a primary or secondary legislation that in case numbered accounts are opened, financial institutions are required to maintain them in such a way that full compliance with the FATF Recommendations can be achieved. • Ongoing due diligence requirement should be provided for explicitly by primary or secondary legislation. • Insurance companies should be explicitly required to terminate the business relationship and consider making a suspicious transaction report when required CDD measures cannot be applied to existing customers and in cases when the institution has doubts about the veracity or adequacy of previously obtained customer identification data. • Banks, money exchange businesses, insurance companies and authorized persons should be explicitly required to apply CDD requirements to existing

Recommended Action (listed in order of priority)	
	customers on the basis of materiality and risk. • Performing CDD measures based on doubts about the veracity of previously obtained information should be implemented by most financial institutions. • The identification and verification process should be sufficiently implemented at some financial institutions. With money exchange businesses, it should be clearly restricted to conduct business transactions against submitting a copy of identity. • All financial institutions should obtain information concerning the directors of legal entities. Proofs of incorporation of these entities have not been retained in several instances. • Financial institutions' understanding of the requirement to obtain and verify beneficial ownership should be improved. . The same applies to understanding the control structure of legal entities. KYC forms should contain fields by which such information can be retained. • It should be ensured that scrutiny of transactions for consistency with due diligence data is being conducted by non-bank financial institutions. The reported reliance of many banks on specialized transactions monitoring software for such scrutiny does not include matching with KYC data. • For banks and money exchangers, the transactions monitoring threshold parameter of SAR 60,000 means that most customer relationships may stay below the radar, which would exclude the requirement to undertake CDD measures when there is a suspicion of money laundering or terrorist financing below this threshold. Such FIs should be well informed of the fact that the said parameter should not be exclusively/largely depended on. The quality and frequency of updating of CDD data appeared to be questionable concerning many financial institutions. • Due diligence measures should be satisfactorily applied by financial institutions (vis-à-vis perception of who could be a high-risk customer, classification of customers according to risk). Enhanced diligence should be satisfactorily applied in all sectors. • It should be ensured that customer files with all FIs contain key documents pertaining to the identification process. • The extent (mainly for official documents) and quality of updating should be enhanced at all financial institutions. The updating process in some FIs has often not been completed. CDD information for existing business relationships at many non-bank financial institutions was not up-to-date. *Recommendation 6* • Definition of PEPs should not only cover current and recent PEPs (definition of “recent” should be clarified). • Financing companies should be explicitly required, in addition to performing the CDD measures, to put in place appropriate risk management systems to determine whether a potential customer, a customer or the beneficial owner is a politically exposed person. • Insurance companies, Authorized persons and Financing companies should be explicitly required to seek senior management approval for continuing the relationship in cases where a beneficial owner is subsequently found to be, or subsequently becomes a PEP. • Insurance companies should be required to determine the source of wealth and source of funds for beneficial owners identified as PEPs, as well as source of wealth for customers identified as PEPs. • Financing companies should be explicitly required to determine source of wealth and source of funds for clients or beneficial owners identified as PEPs. *Recommendation 7* • Banks should be required to ensure that AML/CFT responsibilities falling on each institution are documented. • Banks should apply adequate due diligence towards correspondent relationships,

Recommended Action (listed in order of priority)	
	notably the ones already established. *Recommendation 8* • Authorities should make sure that adequate attention is paid by financial institutions regarding AML/CFT-related risks that may be posed by new technologies.
3.3 Third parties and introduced business (R.9)	• The rules should bind financial institutions to obtain immediately necessary CDD information from third parties when relying on them to perform some of the elements of the CDD process or to introduce business. • Banks should be required to satisfy themselves that the third parties are regulated and supervised.
3.4 Financial institution secrecy or confidentiality (R.4)	• It is recommended that a legal basis regarding exceptions to confidentiality provisions in the sharing of information between institutions, domestic and foreign, be explicitly established.
3.5 Record keeping and wire transfer rules (R.10 & SR.VII)	• Beneficiary financial institutions should be required to adopt effective risk-based procedures for identifying and handling wired transfers that are not accompanied by complete originator information.
3.6 Monitoring of transactions and relationship (R.11 & 21)	*Recommendation 11* • The distinction between requirements to monitor unusual transactions (as required by Recommendation 11) and to report transactions that are identified as suspicious (as required by Recommendation 13) should be better understood by FIs and government authorities. Entities are often unsure of what are the appropriate parameters and considerations to apply to the monitoring of transactions (that is, what constitutes complex or unusual, and, in short, what they are monitoring for). These issues could be conquered over a reasonable amount of time through a combination of further clarification of rules and regulations, training, and supervision. • The fact that multiple versions of the AMLS coexist is in many ways problematic, not least in that it is not clear to which entities must adhere. As an absolute priority, authorities should ensure that there is one version of the AMLS, the exact wording of which is consistent in Arabic and English.112 • The AMLS and references to it in the RBME should furthermore be modified in such a way as to ensure that financial institutions' monitoring process is not prejudiced by the suggestion that the objective of the process is to detect criminal activity. • The RBME should be modified to make explicit the monitoring obligation for banks and money exchangers and to clarify guidelines for monitoring procedures to enable more effective implementation. References to monitoring threshold parameters in the RBME and RIC should also be removed. • Improved supervision of banks' AML/CFT procedures – and the levying of sanctions in the case of violations – should result in significantly more effective systems for the monitoring and evaluation of unusual activity. *Recommendation 21* • The authorities should seek to clarify what is required of institutions with respect to identifying those countries that do not sufficiently apply the FATF Recommendations, and to the handling of transactions and business involving such countries. • Additionally, counter-measures must be established for all sectors. • For all sectors, the competent authorities should provide better guidance to

[112] The assessment team notes that many senior management positions of banks are occupied by non-Arabic speaking individuals such that an accurate official version of the AMLS in English that is consistent with the Arabic is of critical importance.

Recommended Action (listed in order of priority)	
	institutions to assist in the identification of countries that do not sufficiently apply the FATF Recommendations. • Where SAMA does distribute by circular FATF statements identifying countries of concern, it should more explicitly note institutions' obligations with respect to use of this information. • Across all sectors, where it appears in rules and regulations governing the AML/CFT practices, reference to the NCCT list should be replaced with more comprehensive and up-to-date guidance.
3.7 Suspicious transaction reports and other reporting (R.13-14, 19, 25 & SR.IV)	*Recommendation 13 and Special Recommendation IV* • The low overall number of STR filings relative to the size of the economy and characteristics of the financial sector point to a lack of effectiveness and should be improved. • Further improvements should be made in the quantity and quality of STR reporting by more clearly explaining the distinction between monitoring transactions for unusual activity and identifying and reporting of suspicious activity. • Efforts to increase awareness – through training, provision of typologies and case studies, etc. – of the potential for money laundering and terrorist financing abuse is also recommended. • The monitoring threshold parameter for banks and insurance companies should be abolished. *Recommendation 14* • The sharing of STRs with supervisors (and effectively with accountants) increases the chance that a STR is tipped-off, and should be abolished. • Recommendation 25 • SAFIU and relevant competent authorities should seek to implement a comprehensive system of providing feedback that is in line with the FATF Best Practice Guidelines. • The FIU should endeavor to provide case-by-case feedback to all those filing STRs (including whether or not an STR resulted in an investigation and prosecution), and the development of case studies and typologies (in addition to indicators) relating the potential for ML and TF abuse across sectors. • SAMA and CMA should also seek to provide further guidance in the form of typologies to assist institutions with the development of their capabilities to identify unusual and suspicious transactions. • Special attention should be given in particular to the development of terrorism finance awareness.
3.8 Internal controls, compliance, audit and foreign branches (R.15 & 22)	• The independence and adequate resourcing of the audit function in the insurance and securities sectors should be explicitly required. • The rules and regulations pertaining to internal controls and policies should be applied consistently among financial institutions and smaller non-bank financial institutions in particular. • More should be done to both expand training opportunities across all sectors and to broaden the scope of training. More training to enhance an understanding of how various systems, sectors, and individual entities can be exploited for the purposes of money laundering and terrorism finance is recommended. • The assessment team found that in the nascent insurance industry, where comprehensive rules to address AML/CFT were very recently introduced, companies have not established robust internal policies and the team recommend that KSA addresses this. • The limited institutional awareness of AML/CFT threats regarding insurance and the measures companies must take against them should be addressed. • The evaluation team encourages the authorities to work with the nascent financing industry to effectively implement the robust provisions regarding internal controls

Recommended Action (listed in order of priority)	
	and policies that are laid out in the recently issued IFC.
3.9 Shell banks (R.18)	• Inadequate implementation of CDD measures in relation to correspondent banking relationships as noted in the discussion of Recommendation 7 have a negative effect on the ability of banks to ensure that the respondent bank is not a shell bank, or to ensure that the respondent bank does not permit (de facto or de jure) their accounts to be used by shell banks. This should be addressed.
3.10 The supervisory and oversight system – competent authorities and SROs. Role, functions, duties and powers (including sanctions) (R.23, 29, 17 & 25)	Recommendation 17 • The implementation level of these sanctions should be improved and corrective actions to be taken to include all types of units subject to supervision by SAMA and CMA. Recommendation 23 • Fit and proper criteria are to be tested against real cases scenarios to check the adequacy of such criteria on existing financial units (in relation to ownership) and with regards to non-Saudi nationals. • SAMA should apply the fit and proper requirements on financing l companies • Empower the Insurance Control Department in SAMA with adequate manpower and expertise to carry on the assigned duties as the insurance field continues to grow. • Provide CMA with proper enhanced training for its staff to perform the duties assigned to them. • Empower AML unit within CMA with adequate number of examiners with AML/CFT expertise to conduct related examination tasks as the number of APs is growing. Recommendation 25 • The current AML/CFT guidelines should be enhanced to include more clear description of business-related methods and to cover explicitly all types of financial institutions. Recommendation 29 • Enhance the expertise of the examiners especially in the field of AML/CFT with regards to insurance and financing companies. • Introduce more frequent on-site AML/CFT related examination missions by SAMA to cover banks, money exchange businesses, insurance and leasing companies. • Increase the number of AML/CFT related examination assignment has to be concluded by CMA for all licensed units. CMA should design a more frequent enhanced examination process carried by well trained CMA's AML unit staff.
3.11 Money or value transfer services (SR.VI)	• Authorities should remedy shortcoming under Recommendations 5, 6, 7, 8, 9, 11, 13, 15, 17, 21 and 23 in relation to the compliance with and implementation of the requirements of SR.VI
4. Preventive measures – Non-Financial Business and Professions	
4.1 Customer due diligence and record-keeping (R.12)	With respect to DNFBPs, it is recommended to: • Amend the AMLS or IRs to provide the Ongoing due diligence requirement. • Require the following, through law, regulation or other enforceable rules: • To understand the ownership and control structure of a customer that is a legal person or legal arrangement. • To obtain information on the purpose and intended nature of the business relationship. • To scrutiny transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the entity's knowledge of the customer, their business and risk profile, and where necessary, the source of funds. • To consider making a suspicious transaction report whereas required CDD

Recommended Action (listed in order of priority)	
	measures could not be applied. • To terminate the business relationship and consider making a suspicious transaction report in case required CDD measures could not be applied to existing customers and to cases whereby the institution has doubts about the veracity or adequacy of previously obtained customer identification data. In such instances, it should also be required to consider making a suspicious transaction report. • To apply CDD requirements to existing customers on the basis of materiality and risk and to conduct due diligence on such existing relationships at appropriate times. • To include specific and effective CDD procedures in their measures for managing the risks related to non-face to face customers. • To require from Lawyers and TCSPs to pay special attention to unusual patterns of transactions that have no apparent or visible economic or lawful purpose and to examine as far as possible the background and purpose of these. • DNFBPs should be required to set forth in writing the examination of the background and purpose of complex, unusual large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose; DNFBPs should be also required to keep such findings available for competent authorities and auditors for at least five years. • Issue through law, regulation or other enforceable rules: • Enforceable obligations with regard to Politically Exposed Persons. • Enforceable obligations with regard to introduced business. • Ensure proper and efficient implementation.
4.2 Suspicious transaction reporting (R.16)	• Authorities must make a concerted effort to raise awareness of ML and TF risks among DNFBPs and provide regular and consistent guidance to assist in the development of systems to address these risks. Additional effort must be made to make these entities aware of their legal obligations with respect to AML/CFT beyond STR filing and the authorities must actively enforce these obligations. • Authorities should seek to actively encourage compliance with the STR filing requirement, including through the issuance of typologies, increased training, and provision of feedback. The MOCI noted that they have never received feedback from the FIU regarding the results of any STR filed by an entity under their supervision. • The MOJ should issue additional regulation and guidance to legal services providers regarding AML/CFT measures.
4.3 Regulation, supervision and monitoring (R.24-25)	• Enhance the expertise and supervisory framework for DNFBs. • Enhance the knowledge and expertise in the filed of AML/CFT for DNFBs as the need for services of such sector is growing. • Produce typologies and best practice monitoring techniques based on past experience and the local market condition. • Enhance the feedback from and to both DNFBs and SAFU.
4.4 Other non-financial businesses and professions (R.20)	• The authorities should consider legally banning cash transactions above a certain threshold, in support of their policy to reduce the reliance on cash and encourage the use of modern secure payment techniques.
5. Legal Persons and Arrangements & Non-profit Organisations	
5.1 Legal Persons – Access to beneficial ownership and control information (R.33)	• Accessing Commercial Register information might require time as this information is only available within the 40 branches of Commercial Register Office. The team encourages the authorities to introduce direct and spontaneous access to the information by the competent authorities.
5.2 Legal Arrangements – Access to beneficial	• The lack of a requirement to disclose information on beneficial ownership (in addition to the beneficiary) on the trust deed should be addressed.

Recommended Action (listed in order of priority)	
ownership and control information (R.34)	
5.3 Non-profit organisations (SR.VIII)	• With many charities and *waqfs* with a multiple of transactions it is essential that MOSA and MOIA review the NPO system as a whole and identify elements of the system and types of NPOs that are at risk. It is unclear what the requirement and the legal basis are for the record keeping requirements, this should be made clear.
6. National and International Cooperation	
6.1 National cooperation and coordination (R.31)	• The authorities should better coordinate and streamline the mandates and work of the main coordinating bodies. • The authorities should also ensure that there is sufficient information flowing to ensure a proper understanding and implementation of the FATF Standards.
6.2 The Conventions and UN special Resolutions (R.35 & SR.I)	• It is recommended that Saudi Arabia fully implements the Palermo and TF Conventions, as well as UNSCR 1267 and 1373 to correct the deficiencies noted in relation to the implementation of the relevant international conventions and UNSCR as soon as possible.
6.3 Mutual Legal Assistance (R.36-38 & SR.V)	• There is a clear need to establish effective procedures for the implementation of requests for legal assistance which allow, in particular, for the follow-up of the execution and response to the request by the local authorities involved. • There should be a central body with responsibility for the coordination of follow-up of such requests. The PCMLA would seem to fit this role, regardless of the subject matter of the request, even though it should improve the coordination role and ensure the monitoring procedure in the implementation of requests by the competent authorities (as set out in its founding charter) and be fully aware of its functions under Articles 23 and 24 of the AML. • Due to a lack of a single set of comprehensive statistics, it was not possible to confirm effectiveness. Nevertheless, the statistics that are available do not confirm the presence of an effective system for MLA either. Hence, effectiveness needs to be improved. • The shortcomings related to Special Recommendation II (criminalisation of TF, as described in section 2.2 of this report), may have a negative effect of the implementation of this recommendation and should be addressed.
6.4 Extradition (R.39, 37 & SR.V)	• There is a need to implement International Agreements at domestic level in order to establish a clear basis that permits the prosecution of those citizens whose extradition has been refused. • In addition to this, these provisions should also establish a framework of cooperation with foreign authorities, in particular at the level of the collection and admissibility of evidence, for the effective prosecution of those individuals. • Additionally the Kingdom should conclude extradition agreements with more countries and do not narrow the scope of extradition requests in view of the reciprocity principle. • The nature of the statistics could not be fully understood or analyzed, which makes that effectiveness, although likely, could not fully be confirmed, which is something that should be addressed.
6.5 Other forms of cooperation (R.40 & SR.V)	• International cooperation by the FIU is sound on paper, but effectiveness is very low, this should be improved. • There are several gateways for supervisory cooperation, but most of these concern policy cooperation and not information exchange. The assessment team could not establish that supervisory bodies cooperate effectively. This should be improved.
Other issues	
7.1 Resources and statistics	The authorities should address the following issues:

Recommended Action (listed in order of priority)	
(R.30 & 32)	• Some supervisory authorities (for both FIs and DNFBP) need more human and technical resources and training to carry out their respective roles effectively. • Insufficient operational independence of supervisors • Lack of complete or reliable statistics concerning: • overall statistics on penalties upon convictions are not available • some statistical uncertainly about the difference between ML and TF • no separate statistics available on the use of seizure provisions • fragmented statistics relating to the numbers of (AML/CFT) staff and budgets of LEAs • Customs statistics are not very clear and hamper the ability to draw workable (AML/CFT) conclusions • Lack of lawyers-related STR • No specific statistics are generated or kept in relation to the results FI supervisory inspections • statistics to prove the effectiveness (R.38)
7.2 Other relevant AML/CFT measures or issues	-
7.3 General framework – structural issues	-

Table 3: Authorities' Response to the Evaluation (optional)

Relevant (Special) Recommendation(s)	Country Comments
Special Recommendation II	The KSA authorities do not agree with the assessor's conclusion that FT is not adequately criminalized under Saudi law. As indicated to the assessors, the FT offense is criminalized under the *Shari'ah* and cover most of the requirement of the FT offense as contained in the Terrorism Financing Convention. Taking under consideration the large number of cases provided to assessors, a partially compliant rating therefore does not accurately reflect the legal situation in the Kingdom and a largely compliant rating would be warranted.
Recommendation 3	The KSA authorities do not agree with the assessor's conclusion that some of the confiscation requirements (non ML predicate offenses) are not met. As indicated to the assessors, the *Shari'ah* Law applies to all other predicate offenses. The statistics and law cases provided to assessors prove the effectiveness of the KSA system. In addition, there must be consistent assessments among different reports adopted by the same organization where the KSA authorities requested to have the same rating as Turkey where both reports have the same underlying factors.
Special Recommendation III	The KSA authorities do not agree with the assessor's conclusion that the KSA does not have a mechanism in place to implement UNSCR 1373. Foreign requests to freeze assets of individuals or organizations designated under UNSCR 1373 are implemented through decision by the Permanent Committee on Combating Terrorism (Royal Decree 20168/S). Domestic terrorists or terrorist individuals may be designated under UNSCR 1373 by the Ministry of Interior and their assets be frozen (Royal Decree 3156). In addition, as indicated by the assessors in paragraph 160 of the report, the KSA has a comprehensive mechanism in place to address UNSCR 1267. The authorities are of the view that a partially compliant rating therefore does not accurately reflect the KSA's level of compliance with SR III and a largely compliant rating would be warranted.
Special Recommendation IX	Saudi law fully complies with 13 and partially complies with 2 essential criteria under SR IX. The KSA authorities are of the view that a partially compliant rating does not accurately reflect the legal situation in the Kingdom and a largely compliant rating would be warranted.
Recommendation 5	Given that no numbered accounts exist in the Kingdom, it would be futile to regulate this non-existing product in primary or secondary legislation. All FIs are under an implied obligation under Saudi law to conduct ongoing due diligence and are required to apply CDD to existing customers, whereby considerations of materiality and risk have been taken into account in drafting the relevant legal provisions. KSA law provides that FIs, including insurance companies, are to terminate any existing business relationship when CDD cannot be completed and are expected to file an STR in such cases. The authorities are of the view that the key factors on these points are thus not warranted. The remaining key factors relate to effectiveness issues and would justify a largely compliant rating.
Recommendation 6	As explained to the assessors, in Arabic the word "recently" and "current" have the same meaning. Financing companies are required to consider all PEPs as high-risk customers and therefore to apply the greatest level of risk management to PEPs and both financing and insurance companies are required to determine the source of funds and wealth for all legal and natural person clients, including PEPs. The key

Relevant (Special) Recommendation(s)	Country Comments
	factors on these points are thus not warranted and a largely compliant rating would be appropriate.
Special Recommendation VII	The authorities are of the view that a partially compliant rating does not accurately reflect the situation in the KSA. As indicated to the assessors, all banks and money exchanger are legally required to suspend incoming wire transfers that contain incomplete information and request the transmitting institutions to complete the information. If such information cannot be obtained, the FI has to reject the transfer and file an STR. In practice, the KSA is considered to be one of the countries characterized by high outgoing transfers with a relatively non-significant volume of incoming money transfers. The first key factor is thus not warranted and a largely compliant rating would be appropriate.
Recommendation 11	The KSA authorities are of the view that the second key factor is not warranted based on and the assessors conclusion in paragraphs 474 to 477 that the various regulations set out a direct or implied obligation for all FIs operating in the KSA to pay special attention to complex and unusual large or unusual patterns of transactions. The discussion in paragraphs 481-486 also raises no concerns with respect to the legal framework. The authorities thus consider that a largely compliant rating would be appropriate.
Recommendation 21	The authorities do not agree with the assessors' statement in paragraph 498 that there are no counter-measures in place for countries that do not or insufficiently apply the FATF standard. The KSA authorities have issued jurisdictions specific advisories to FIs and instructed them to take preventive measures for and apply enhanced monitoring and review procedures for all transactions from and to such countries, and to not open correspondent accounts with financial institutions located in such jurisdictions. SAMA has also followed up with FIs to verify that such safeguards were implemented in practice. The KSA authorities are therefore of the view that the first key factor is not warranted and that a largely compliant rating would be appropriate.
Recommendation 25	SAFIU has in the past provided extensive feedback to all reporting entities on any STRs received. This has been acknowledged by the assessors in paragraph 524. SAFIU also issues a detailed report on a regular basis which contain typologies and statistics regarding AML/CFT issues and to increase awareness amongst reporting entities. The KSA authorities are of the view that the two listed key factors are therefore not warranted and that a compliant rating would be appropriate.
Recommendations 12, 16, and 24	All DNFBPs as defined in the FATF standard are subject to the full range of preventive measures under the Saudi AML/CFT framework, including on CDD, PEPs, non-face to face customers, introduced business, account and transaction monitoring and STR reporting obligations as outlined in section 3 of this report. MOCI, the MOJ and the SOCPA as the supervisors of DNFBPs have issued a significant amount of guidance on all of these topics to assist DNFBPs in effectively implementing these obligations. All of the supervising authorities are equipped with the necessary powers, resources and know how to effectively implement their mandate with respect to supervision of DNFBPs. The authorities thus do not consider the non-compliant ratings for Recommendations 12, 16 and 24 to be warranted and are of the view that compliant ratings on these Recommendations

Relevant (Special) Recommendation(s)	Country Comments
	would be appropriate.
Recommendation 35	The authorities are of the view that most of the Palermo Convention provisions have been fully implemented in the KSA and that a largely compliant rating on Recommendation 35 would be appropriate. This view is supported by the comments on Special Recommendations II, III and Recommendation 5 above and the largely compliant ratings received on Recommendations 1, 2, 3, 10, 27, 28 and 36.
Special Recommendation I	The KSA authorities are of the view that the majority of the TF Convention provisions and UNSCRs 1267 and 1373 have been implemented in the KSA and that a largely compliant rating on Special Recommendation I would be appropriate. This view is supported by the comments on Special Recommendations II, III and V.
Recommendation 38	The authorities consider the third key factor to be invalid as it is not substantiated by the assessors' analysis under Recommendations 3 and 38. Furthermore, based on the comments on Special Recommendation II above, the authorities consider the last key factor to not be warranted. A largely compliant rating for Recommendation 38 would thus be accurate.
Special Recommendation V	Based on the largely compliant ratings for R 36 and 37 and in light of the authorities' comments on Recommendation 38 above, the authorities are of the view that a largely compliant rating on Special Recommendation V would be appropriate.

ANNEXES

ANNEX 1: LIST OF ABBREVIATIONS

ADD	Anti-Drugs Directorate
AML/CFT	Anti-Money Laundering/Combating of the Financing of Terrorism
AMLS	Anti-Money Laundering Statute and Implementing Regulations
BCL	Banking Control Law
CDD	Customer Due Diligence
CICL	Cooperative Insurance Control Law
CMA	Capital Market Authority
CML	Capital market Law
DNFBPs	Designated Non-Financial Businesses and Professions
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FCML	Financial Crimes and Money Laundering Committee
FIs	Financial Institutions
GCC	Gulf Cooperation Council
GDP	Gross Domestic Product
GID	General Intelligence Directorate
IFC	AML/CFT Instructions for Financing Companies
IMF	International Monetary Fund
IR	Implementing Regulations
KSA	Kingdom of Saudi Arabia
MENAFATF	Middle East and North Africa Financial Action Task Force
ML	Money Laundering
MLA	Mutual Legal Assistance
MOCI	Ministry of Commerce and Industry
MOF	Ministry of Finance and National Economy
MOI	Ministry of Interior
MOIA	Ministry of Islamic Affairs
MOJ	Ministry of Justice
MOSA	Ministry of Social Affairs
NPO	Non-Profit Organization
PCCML	Permanent Committee on Combating Money Laundering
PCCT	Permanent Committee on Combating Terrorism
PCMLA	Permanent Committee on Mutual Legal Assistance
PEP	Politically Exposed Persons
RAP	AML/CFT Rules for Authorized Persons
RBME	AML/CFT Rules for Banks and Money Exchangers
RIC	AML/CFT Rules for Insurance Companies
SAFIU	Saudi Arabian Financial Intelligence Unit
SAMA	Saudi Arabian Monetary Agency
SOCPA	Saudi Organization for Certified Public Accountants
TCS	Trust and Company Services
TCSP	Trust and Company Service Providers
TF	Terrorist Financing
UNSCR	UN Security Council Resolution

ANNEX 2: LIST OF PERSONS AND BODIES MET

High level representatives

- His Excellency Dr. Muhammad Al-Jasser, Governor of the Saudi Arabian Monetary Agency and Chairman of the Permanent Committee for Anti Money Laundering

Ministries

- Ministry of Commerce and Industry
- Ministry of Finance
- Ministry of Foreign Affairs
- Ministry of Islamic Affairs
- Ministry of Interior
  - General Security Directorate
  - General Department for Combating Narcotic Drugs
  - Legal Affairs Division
  - International Police Division
  - General Intelligence Division
- Ministry of Justice
- Ministry of Social Affairs

Other government entities

- Customs Directorate (part of the Ministry of Finance)
- Investigation and General Prosecution Authority (affiliated to the Ministry of Interior)
- Notary office (part of the Ministry of Justice)
- Saudi Arabia Financial Intelligence Unit (SAFIU) (part of the Ministry of Interior)

Governmental policy coordination bodies

- Permanent Committee for Anti Money Laundering (PCAML)
- Permanent Committee for Combating of Terrorism (PCCT)
- Permanent Committee for Mutual Legal Assistance (PCMLA)

Supervisory bodies

- Capital Market Authority (CMA) (securities supervision department)
- Saudi Arabian Monetary Agency (SAMA) (banking, insurance and financial leasing supervision departments)

Private sector entities

Banking and remittance

- Financial Crimes & Money Laundering Committee (FCMLC)
- The Self Supervisory Committee (SSC)
- One domestic bank
- Two domestic banks affiliated to a foreign banking group
- One domestic money remittance company
- One domestic money remittance company affiliated to a domestic bank that is affiliated to a foreign banking group

Other financial institutions

- One domestic security firm
- One domestic securities firm affiliated to a foreign financial services group
- One domestic cooperative insurance company
- One domestic insurance company affiliated to a foreign financial group
- One domestic leasing company

Designated Non-Financial Businesses and Professions

- One charted accountant
- One real estate broker
- One law firm
- Saudi Jewelers' association (including practitioners)
- Saudi Organization for Certified Public Accountants

ANNEX 3: LIST OF MOST/MAIN SUPPORTING MATERIAL AND PRESENTATIONS RECEIVED

1. The AML Law and its Implementing Regulations Issued by Royal Decree M/39 dated 25/6/1424H
2. The Council of Ministers' Resolution No. (168) dated 11/8/1419H, approving the Implementation Regulations of the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances
3. The Basic Law of Governance Royal Decree No. A/91 dated 1/3/1992M
4. The Law of Criminal Procedures issued by Royal Decree No. M/39 dated 28/7/1422H
5. Prime Minister's telegram No. S/2496 on 16/7/1424H concerning freezing funds and assets of any person or entity included in the UN lists
6. Linking the General Directorate for Combating Drugs with His Royal Highness the Assistant Minister of Interior under Supreme Order No. 5664/MB dated 23/6/1428H
7. The Law of Professional Companies Royal Decree M/6 dated 22/3/1385H
8. The Interior Minister's telegram No. S/51196 on 6/8/1428H concerning freezing funds Financial assets of person and entities included in the list of the UN
9. The Interior Minister's telegram No. 1S/35831 on 25/5/1428H concerning freezing money of Financial assets of those on the consolidated list of the UN
10. The Law of the Judiciary and the Law of the Grievances Board issued by Royal Decree M/78 on 9/9/1428H
11. Decree No. M/62 on 18/7/1428H, sanctioning the International Agreement on Cracking Down Terror and Terrorism Finance
12. The Interior Minister's telegram No. 19/39604/2SH on 20-21/7/1424H concerning sending STRs to SAFIU
13. The Interior Minister's telegram No. 1S/46287 on 1/8/1426H concerning sending STRs to SAFIU (STR form)
14. The Officers Service Law issued by Decree No. M/43 on 28/8/1393H
15. The Soldiers Service Law issued by Decree No. M/9 on 24/3/1397H
16. The Civil Service Law issued by Decree No. M/49 on 10/7/1397H
17. The Law of the Saudi Commission for Investigation and Prosecution – M/56 on 24/10/1409H
18. Council of Ministers Resolution No.2111/8 on 1/12/1400H – establishing an Investigation subdivision called the (Administrative Investigation), and the Law of Bribery was issued under Royal Decree M/36 on 29/12/1412H
19. The Council of Ministers' Resolution No.15 on 17/1/1420H, applying the 40 Recommendations of combating money laundering operations through the Committee
20. The Council of Ministers' Resolution No.278 on 14/11/1422H, moving the Committee's seat to SAMA
21. The Resolution of the Public Security Department No.11222 on 7/6/1424H, approving the organizational structure and regulatory lists
22. Circular No. 248S/11/M on 8/4/1428H, distributing the Manual of Declaration Procedures to customs outlets (Arabic + English)
23. Statistical report on total amounts of Cash precious metals which were declared from 26/5/1429H to 26/11/1429H
24. Banking Control Law – Royal Decree M/5 on 22/2/1386H
25. The Decision of Minster of Finance No 3/920 regulating the business of money exchanging
26. The Law on Supervision of Cooperative Insurance Companies issued by Royal Decree M/32 on 2/6/1424H
27. Regulations of combating money laundering and terrorism finance companies
28. The Capital Market Law issued by Royal Decree M/30 dated 2/6/1424H
29. The Rules of opening bank accounts with commercial banks (1) Second Update 2007
30. The Rules of opening bank accounts with commercial banks (2) Third Update 2008
31. SAMA's Circular No. M A T/866 on 29/12/1420H to money exchanging firms
32. SAMA / the Rules of AML/CFT 1st Update 2003
33. SAMA / the Rules of AML/CFT 2nd Update 2008
34. The Authorized Person Regulations Issued by the Board of Capital Market Authority dated 21/5/1426H
35. The Rules of AML/CFT ((Capital Market Authority)) issued on 3/12/1429H
36. Ministry of Interior's Letter No. 19S/1075 on 9/3/1400H – the importance of maintaining secrecy in bank dealings
37. SAMA Circular No.15537/M/433 dated 30/11/1395H Notification of Suspects during Pilgrimage Season
38. SAMA Circular No. 199 dated 28/5/1399H Notification of Suspicion
39. SAMA Circular No. 7737/MA/98 dated 16/5/1403H Request for Notifying the Intelligence or the Police of Suspicious Transactions when transferring funds abroad
40. SAMA Circular No. 3151 dated 14/3/1417H Suspicious Transactions
41. SAMA Circular No. 4696 dated 19/3/1408H Enhancing Reports of Suspicious Transactions
42. SAMA Circular No. 3291/M/A/73 dated 16/2/1409H Regulatory Controls for Verifying ID Cards

43. SAMA Circular No. 452/MA/10 dated 10/1/1411H Circular on Reports of Suspicious Transactions
44. SAMA Circular No. 88/MAT/1712 dated 6/2/1416H Directives for Combating Money Laundering
45. SAMA Circular No. 159/MT dated 21/10/1421H Requirements of STRs for Banks
46. SAMA Circular No. 160/MAT dated 21/10/1421H Requirements of STRs for Money Exchangers
47. SAMA's circular No. 27355/MAT/333 dated 23/12/1424H to Money Exchangers Obtaining all data related to a customer from an official ID Card
48. SAMA's circular No. MAT/75 dated 22/2/1424H to Banks and Money Exchangers Obtaining all data from Customer
49. SAMA's circular No. 2858/MAT/437 F dated 10/8/1426H Submission of notifications by Banks and Money Exchangers to the FIU
50. SAMA's circular No. 242/14632 dated 25/5/2005 Applying Control and Compliance with Laws
51. SAMA's circular No. 8733/M A SH/ 138 dated 3/3/1426H Requirements for appointment in senior positions in banks operating in the Kingdom
52. The by-laws of the Permanent Committee for Combating Money Laundering
53. The guidance Manual of Combating Money Laundering transactions ((Manual of Combating Money Laundering)) SAMA Issued in 1995
54. Law of Commercial Registers, Royal Decree M/61 dated 17/12/1409H
55. Circular Issued by the Ministry of Commerce for merchants on how to notify and Report No. 1312/11 dated 15/5/1422H
56. The rules for regulating real estate offices Issued by The Ministry of Commerce
57. Law of Precious Metals and Stones, Issued by virtue of Royal Decree M/42 dated 10/7/1403H
58. Regulations to Certified Accountants, by virtue of Royal Decree M/12 dated 13/5/1412H
59. The Implementing Regulations of Notaries Public (Ministry of Justice)
60. The Implementing Regulations of the Code of Law Practice
61. The Ministry of Commerce's circular No. 447/W D dated 29/11/1428H to the branches of Ministry for notifying of any unnatural or unusual transactions
62. The Ministry of Commerce's circular No. 315/11 dated 22/1/1424 requiring companies, organizations and professions to notify of suspicious transactions
63. The Ministry of Commerce's circular No. 487/1/2/T dated 3/8/1424H Informing chambers of commerce to send notifications to the FIU
64. The Guidance Manual for combating money laundering Issued by The MOCI in 1425H
65. The Ministry of Commerce's circular No. 206/ W. D dated 10/5/1428H Requesting communication with chambers to notify the staff of compliance with the International Law of export and import
66. The Ministry of Commerce's circular No. 191/W.D dated 2/5/1428H Emphasizing the use of letters of credit
67. The Ministry of Commerce's circular No. 454/W. D dated 19/12/1428H Regarding taking prudential measures for protecting companies from being exploited in money laundering
68. Companies Law/ Royal Decree No. 38 dated 22/10/1377H
69. The Rules of Charitable Associations and Organizations Issued by Ministry of Labor and Social Affairs
70. Ministry of Labor and Social Affairs Circular C/3577 dated 22/10/1406H, prohibiting the use of coupons and hung Boxes for collecting donations
71. Ministry of Labor and Social Affairs Circular No. 41735 dated 23/9/1424H, emphasizing the notification of cases of money-laundering activities when visiting charitable associations
72. Letter of the Ministry of Social Affairs No. 92980 and the date 29/10/1429 H containing the courses of action through the definition of money laundering and how to discover it
73. The Ministry of Social Affairs' Circular No. 6/79621/Sh dated 12/11/1427H on regulating the closing of the accounts of charitable societies/organizations
74. The Ministry of Interior's Telegram No. IS/65853 dated 9-10/11/1426H, emphasizing the importance of notifying suspected operations
75. The UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, which was sanctioned per Royal Decree No. M/19 dated 15/7/1410H
76. The Council of Ministers' Resolution No. 82 on 19/3/1422H, setting an appropriate mechanism for adopting the Implementing Regulations related to the UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic substances
77. The Council of Ministers' Resolution No. 225 dated 19/3/1422H concerning coordination among relevant authorities for the application of the UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances
78. Royal Decree No. M/20 on 24/9/1425H Sanctioning the UN Convention Against Transnational Organized Crime
79. Royal Decree No. M/62 dated 18/7/1428H Ratifying the UN Convention for Suppression of Terrorism-Financing
80. Royal Decree No. M-52 dated 2/9/1426H on Joining the GCC Convention for Combating Terrorism
81. Royal Decree No. M/31 dated 5/8/1421H Ratifying the Islamic Conference Organization Convention for Combating International Terrorism
82. Council of Ministers' Resolution No. 129 dated 16/10/1419H Ratifying the Code of Conduct Rules for

Member Countries in the Islamic Conference Organization Convention

83. Royal Decree No. M/16 on 10/6/1419H Approving the Arab Convention for Combating Terrorism

84. Royal Decree No. M/16 dated 2/4/1402H Sanctioning the Agreement for Security Cooperation and the Extradition of Criminals with the government of Bahrain

85. Royal Decree No. M/21 dated 28/5/1402H Ratifying the Agreement for Security Cooperation and the Extradition of Criminals with the government of Sultanate of Oman

86. Royal Decree No. M/22 dated 28/5/1402H Ratifying the Agreement for Security Cooperation and the Extradition of Criminals with the UAE

87. Royal Decree No. M/20 dated 28/5/1402H Sanctioning the Agreement for Security Cooperation with Qatar

88. Council of Ministers' Resolution No. 156FY dated 14/6/1403H Ratifying the Agreement for Security Cooperation with Morocco

89. Royal Decree No. M/2 dated 2/3/1416H Sanctioning the Agreement for Security Cooperation with Tunisia

90. Royal Decree No. M/5 dated 15/1/1427H Sanctioning the Agreement for Security Cooperation with Sudan

91. Royal Decree No. M/4 dated 15/1/1427H Ratifying the Cooperation Agreement Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances with Sudan

92. Royal Decree No. M/1 dated 8/1/1418H Approving the Agreement for Security Cooperation with Yemen

93. Royal Decree No. M/2 dated 8/1/1418H Approving the Cooperation Agreement Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances with Yemen

94. Royal Decree No. M/23 dated 20/11/1420H Approving the Cooperation Agreement Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances with Syria

95. Royal Decree No. M/8 dated 14/3/1419H Approving the Agreement for Security Cooperation with Libya

96. Approving the Agreement for Cooperation with Iran under Royal Decree No. M/31 dated 6/7/1422H

97. Royal Decree No. M/43 dated 1/7/1427H Approving the Cooperation Agreement Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances with Turkey

98. Royal Decree No. M/10 dated 24/1/1428H Approving the Agreement for Security Cooperation with China

99. Royal Decree No. M/2 dated 24/1/1419H Approving the Agreement for Security Cooperation with Senegal

100. Decree M/7 on 9/4/1411 H on Convention on the Investigation of Drug Trafficking and Confiscation of Proceeds of Trafficking, with the United Kingdom

101. Decree M/1 on 5/1/1418 H on Agreement on Memorandum of Understanding to Combat Crime with India

102. Memorandum of Understanding with Italy against Terrorism and Illegal Drug Trafficking, Decree M/12 on 10/9/1417 H

103. Memorandum of Understanding with Britain to Fight Terrorism, Drugs and Organized Crime, telegram of Royal Order 5/B/6737 on 1/5/1410 H

104. Resolution of the Minister of Interior No. 4507 on 26/7/1424 H follow-up requests of mutual assistance

105. The Law of Procedure Before Sharia Courts. Implementation Regulations of Law of Procedures before Sharia Courts

106. Letter of the Minister of Interior No. 36/14/41060/2S on 21/7/1425 H. to organize Extradition files

107. Circular 579 S /12/ S on 9/7/1428 H. from Customs to send monthly report to the FIU on the process of disclosure

108. Council of Ministers' Resolution on the establishment of a regional office in the Kingdom for information exchange

109. Law of Commercial Register Issued by Royal Decree No M/1 on 12/2/1416 H

110. Introductory Booklet of the functions and competence of the Regional Office

111. STR Disclosure Form (Declaration Form)

112. Guidance Manual on Combating Embezzlement and Financial Fraud, issued by SAMA under Circular on 2008G

113. Charter of the Saudi Arabian Monetary Agency, issued by Royal Decree No. 23 Dated 23/5/1377 H

114. Regulatory Rules for Audit Committees at Saudi Banks under No. 196/MAT dated 12/3/1417 H

115. Circular No. 819/MAT dated 13/11/2007 Concerning risks of financial dealing with some parties (Iran)

116. Circulars issued from the General Department of Charity Organizations and Institutions No. 37/G dated 22/2/1412 H to charity institutions concerning rules of receiving and disbursing the organizations' funds and how to apply processes of charitable organizations' funds

117. Circulars for all banks and money-Exchanging firms operating in the Kingdom No. 110/MAT dated 22/3/1424 H. requiring all accounts of charity organizations and institutions at each bank –if any- to be identified and consolidated in one major bank account in its name

118. Royal Order No. A/1 dated 6/1/1425 H approving the Draft Charter of the Saudi Civil Commission for Relief and Charity Work abroad

119. SAMA circulars for banks operating in the Kingdom Circular No. 5082/MAT/55 dated 2/3/1424 H of rules for opening accounts in commercial banks and general operational rules
120. Implementation Regulations of Bank's FC/AML Committee, January 2007
121. Appointment of the Ministry of Justice's representative in the membership of the Permanent Committee for Combating Money Laundering under letter No. 93631/26 dated 16/11/1426 H
122. Statistics and data related to money laundering and terrorism financing (SAMA)
123. Terms of Reference Self Supervisory Committee
124. Circular of SAMA No.1298/MP/MAT dated 11/6/1428 H Establishment of an AML Unit at the Bank's
125. Supervision Department's Circular No. 35372/MAS/584 dated 21/10/2006 Basel Committee Document Compliance Function
126. Ministerial Resolution No. 1/30317 dated 21/7/1420 H on regulating financial activity
127. Telegram No. 5/B/48044 dated 9/10/1424 H of the prime minister concerning approval of signing the International Convention of Combating Corruption
128. Sample set of letters issued by SAMA concerning punishment and dismissal of banks' employees
129. Inspection Manual Examination Guidance (SAMA)
130. Instructions issued by SAMA on application of penalties on banks employees
131. Organizational Structure of the SAMA
132. Organizational Structure of the Capital Market Authority
133. Statement of the number of financial institutions licensed by SAMA
134. Statement of the number of companies licensed by the Capital Market Authority and the number of notifications and training courses
135. Telegram from the president of the Court of the Council of Ministers No. 11567 / B and the date of 9/3/1429 H, on the approval of the Career Center (annex Royal Decree No. M / 17 and the date of 8/3/1428 H, and the annex to the Council of Ministers resolution No. (79) and the date of 7 / 3 / 1428, the annex to the fight against computer crime)
136. Bylaws of the Standing Committee of the fight against terrorism
137. Rules of the Supreme Committee to Combat Terrorism
138. Model for the maintenance staff Monetary discourages recruitment
139. A sample of inspection reports (SAMA)
140. Circular No. 22407 m / 285, date 28/10/1424 H, to extend the time limit for the freezing of bank accounts not updated to the end of March 2004
141. Circular No. 3748 / O / 29 and the date of 7/2/1425 H
142. Overseas banks to open accounts to apply the principle of "know your customer"
143. Circular No. 24896 / O To / 391 and the date of 3/7/1427 H, on the codification of civil registration number to the agent in the agencies open bank accounts
144. Organizational structure of public security / public administration of criminal investigations and research
145. Circular of the Minister of Trade and Industry No. 819 / and. D and the date of 14/9/1429 H, on the fight against organized crime, economic, as well as the establishment of a financial investigation Unit FIU in order to receive communications
146. Circulation of the Ministry of Social Affairs No. 105517 and date of 28/11/1429 H may provide a copy of charitable institutions anti-money laundering regime and it's implementing regulations
147. Letter of the Ministry of Social Affairs No. 105865 and date of 28/11/1429 H, on the importance of establishing a number of courses in the regions of the Kingdom of money laundering and damages to the State and the international community
148. Circulation of the Ministry of Social Affairs No. 107318 and date of 2/12/1429 H, on the need to set up a website on the Internet
149. Circulation of the Ministry of Social Affairs No. 97290 and date of 11/11/1429 H, on how to keep regular records, securities, receipts and accounting books
150. Statistics for Anti-Narcotics General
151. Organizational structure of the Directorate General of Drug Control / Division of Anti-Money Laundering
152. Resolution of the Ministry of Finance (No. 689) dated 16/3/1428 H, on the adoption of the organizational structure of the Customs Department (copy of the organizational structure)
153. Royal Decree No. M / 49 and the date of 10/7/1397 H, containing the abolition of staff General and approval of the Civil Service system
154. Resolution No. 951 and the date of 27/6/1397 H, on the approval of the civil service system (annex civil service system)
155. Organizational Structure of the Commission for Investigation and Prosecution
156. Naif University For Security Sciences document
157. Model communication from a financial suspect (name of the shop / institution / company)
158. Model communication from a financial suspect (name Accounting Office)
159. Circulated by the Ministry of the Interior and the Financial Investigation Unit No. 53 / dated 15/9/1426 H. on the confidentiality of information (with photo images of the pledge)

160. Sessions of employees of financial investigations of years (1426 to 1429 H)
161. Statistics on money-laundering cases in the Kingdom of years (1425 to 1429 H)
162. Resolution No. 547 and the date 30/3/1396 e, to approve the Regulation of fund-raising for Charitable Purposes (annex to the list of fund-raising for Charitable Purposes)
163. AML/CFT Rules (SAMA) for Insurance Companies
164. Combating Computer Crimes
165. Fight against drugs and psychotropic substances
166. Public order of the Environment of the Royal Decree No. (M / 34) and the date of 28/7/1422 H
167. Royal Decree No. M / 56 and the date of 11/6/1428 H, containing the approval of the Protocol against the Smuggling of Migrants by Land, Sea and Air
168. Royal Decree No. M / 56 and the date 11/6/1428 H containing the approval of the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children
169. Declaration of the Saudi Chartered Accountants No. 408/12 and the date of 3/12/1429 based on the declaration of the Ministry of Trade and Industry No. 1157/w. D and the date of 1/12/1429 against the Chartered Accountants on the application of regulations and instructions for the fight against money laundering
170. Royal Decree No. 55 / m and the date 3/9/1429 to approve on the agreement of Kingdom of Saudi Arabia and the Republic of Chad to cooperate in the fight against terrorism, illicit drugs and psychotropic substances, and smuggling it
171. Rules and standards of professional authority of the financial market
172. Royal Decree No. 3 / m and the date of 12/2/1429 in regards to the approval of the Kingdom's jointure to the Protocol against the illicit manufacturing of firearms, their parts and components and ammunition and illicit trafficking
173. Minister of the Interior declarations No. 66304 and the date 14/7/1428 and No. 37494 and the date of 10/3/1429 on the mechanism for the implementation of the protocols and application
174. Compliance Manual for Banks Operating in KSA (SAMA)
175. Royal Decree No. M/3 and the date of 28/4/1417 in regards to the Agreement On Executing Judgments, Judicial Delegations And Summonses In The Arabian Gulf Cooperation Council Countries
176. Judgment rendered by the Court, number 120/34, dated 10/6/1428 AH
177. Letter of the Ministry of Justice number 28/76, dated 29/3/1429 AH
178. Brief schedule of the twenty crimes
179. Statistics about the cases considered by the courts regarding money laundering between 2004 AD and 2008 AD
180. Judgment number 0003 rendered by the Ministry of Justice
181. Judgment number 0001 rendered by the Ministry of Justice
182. The 13 agreements
183. Judgment rendered by the Ministry of Justice, number 231/23, dated 30/12/1426 AH
184. Mechanism of Implementation of the resolution of the Security Council 1267 (1999 AD) regarding those listed on the unified list
185. Statistics about the accounts, properties, records and frozen portfolios of local persons, according to the resolution of the Security Council 1373 pertaining to the financing of terrorism and terrorism acts
186. Statistics about the cases referred to the permanent committee for execution of the mutual legal help cases
187. Statistics about the incoming requests to KSA and related answers (the permanent committee for the combating of terrorism)
188. Notice form to Mr. Yassin Kadi, consisting in lodging a request to the Security Council, upon request, to remove his name from the unified list of the penalties committee at the UN
189. Details of the investment and bank accounts regarding the listed parties, according to the resolutions of the Security Council pertaining to the parties listed on the unified list of the committee (1268)
190. The organizational structure of the investigation authority and the training schedules
191. The organizational structure of the Director of the General Directorate for Criminal Evidences and Investigations, and the training schedules
192. The organizational structure of the General Directorate for Anti-drugs, and the training schedules
193. Detailed report about the disclosure of tourist checks (for individuals)
194. Detailed report about the disclosure of tourist checks (for financial institutions)
195. Schedules about the laws and rules, and related dates of issue and issuing authorities
196. Circulars about the dealing with some countries
197. Circulars of the Monetary Agency regarding dealing with external parties
198. Circular of the Monetary Agency number M A T / 97, dated 13/4/1424 AH
199. Schedules with the number of inquiries issued and received by the local and abroad banks
200. Agreement of the Financial Investigation Unit and the Monetary Agency regarding the way of sending STRs

201. Sample of the transfers in which some information was not completed
202. Sample of the letters of the Monetary Agency addressed to the banks regarding the enclosure of the final full-scope examination reports copies and requesting for follow-up reports
203. Statistical schedule of the notifications kept and those sent to the central units at banks
204. Schedule of dates of last Quarterly Follow-up Reports received from local banks for full scope examination
205. Implementing Regulation of the FCML Committee
206. Implementing Regulation of the SSC Committee
207. Guide for Fraud Prevention and Supervision Guidelines
208. 2 circulars from the Monetary Agency to two financing companies dated 1424 AH, and the circular regarding the notification of AML rules for the year 1426 AH
209. Dates of visits of the Monetary Agency to the Saudi bank branches outside the Kingdom
210. Form about an AML training session clarifying the objectives of the sessions, its contents and those persons qualified to attend it
211. The organizational structure of the department of banking inspection at the Monetary Agency and some pertinent information and information about the employees working therein
212. The organizational structure of the department of banking technology at the Monetary Agency
213. The organizational structure of the insurance control department
214. The organizational structure of the Capital Market Authority and some relevant information
215. Qualification certificates and sessions dedicated to those affiliated to the Capital Market Authority
216. Structure of the distribution of the employees at the department of banking inspection at the Monetary Agency
217. Schedule about the sessions offered to the employees of the department of banking inspection at the Monetary Agency
218. Dates of visits of the money exchangers and financing companies and SAMA's letters
219. Dates of visits of the full-scope examination to local banks and foreign branches
220. Ministerial Order number 1/1566, dated 21/7/1420 AH, for the governing of the finance lease activity.
221. Example about the violations and penalties issued by the Saudi Arabian Monetary Agency to some local banks
222. Circular of the Monetary Agency regarding the leading positions requirements at local banks
223. Schedule of Dates of the Last Limited Scope Examination
224. Schedule of supervision visits for Central banks regulate foreign banks branches' which operate in KSA. Head offices in their home country
225. Instructions about AML/CFT for the financing company for the year 2008 AD
226. Example about the violations and penalties issued to some money exchangers
227. Resolution of the Council of Ministers number 168, dated 11/8/1419 AH regarding the approval of the implementing regulation of the UN Convention against illicit trafficking in drugs (Vienna Convention)
228. Statistics of the number of the Persons Extradited to their countries
229. Table for the information exchange memoranda in the field of CFT
230. Statistics about the number of original offenses
231. Statistics about the notifications, investigation, and prosecution related to ML and FT cases
232. Income Tax Law
233. Order of the Council for Ministers number 80, dated 29/1/1393 AH regarding the approval of the governing regulation of charity endowments
234. The Ministry of Justice circular no 13/T/1520 issued on 29/1/1430 AH addressed to courts and notaries and no 13/T/3493 issued on 3/11/1429 AH addressed to lawyers on informing the financial investigation unit about suspected transactions
235. The Ministry of Islamic Affairs circular no 4/9/188 issued on 15/8/1426 AH on informing the financial investigation unit about suspected transactions
236. The Ministry of Trade circular no 454/W D issued on 19/12/1428 AH and no 1312/11 issued on 15/5/1422 AH
237. Schedule about the sessions offered to the employees of General Intelligence/ Administrative Intelligence
238. Brief of the twenty crimes
239. Royal Order 51196, dated 6/8/1428 AH to continue the update of the unified list of the Sanction Committee imposed on al Qaeda or Taliban or the related individuals through the website, and then the accounts and financial assets and properties freezing of those listed
240. Circulars about UNSCR 1373
241. Presentation of a Securities Firm
242. Presentation of Customs
243. Presentation of the Ministry of Interior
244. Presentation of the Saudi Arabia FIU
245. Presentation of the Financial Crime and Money Laundry Committee
246. Presentation of the Self-Supervisory Committee
247. Presentation of a bank
248. Presentation of a bank

249. Arab News 2 March 2009 "Al-Jasser may usher in new banking era"
250. Customs Declaration Procedure Guide
251. Customs Declaration form and information (English and Arabic)
252. Customs Training Courses
253. Customs Declaration Statistics 2008
254. All SAMA sanctions 1423 - 1426H
255. Ministry of Islamic Affairs outreach (Arabic only)
256. Example of Money Transfer and Draft Request
257. Example of Foreign Currency / Draft / Travelers Cheques exchange request
258. Saudi Arabia FIU Annual Report 2006
259. Saudi Arabia FIU Annual Report 2007
260. Saudi Arabia FIU Annual Report 2008
261. Saudi Arabia FIU Statistics 2004 - 2008
262. SAFIU Reporting guidance and manual
263. Strategy of the Permanent Committee on AML
264. Number and Example Topics of PCAML Minutes, plus Samples (Arabic)
265. Samples of Insurance License Certificates
266. Banking Inspection Department Organizational Chart and Description
267. Number of licensed banks and branches of foreign banks
268. Statistics on AMLCFT Training by the Institute of Banking (IOB) 2004 - 2008
269. Statistics from the Ministry of Justice part 1
270. Statistics from the Ministry of Justice part 2
271. Statistics of seizure requests from SAMA to Banks
272. Statistics on ML cases from the Prosecution Authority
273. PCMLA internal rules or by-laws
274. Royal Order 20167 establishing MFA Committee for US-Designated Terrorist Organisations
275. Royal Order to establish the PCCT Arabic
276. Royal Order to establish the PCCT English
277. Interpol extradition statistics part 1
278. Interpol extradition statistics part 2
279. Table on FATF Financial activities (Section 1)
280. ML jurisprudence from MJO case 76/28
281. Implementing Regulations of CIC Supervision Law
282. Updated cash courier declaration form
283. List of money exchangers
284. Minutes of the PCAML on implementation of Recommendation 19
285. DNFBPs, table for section 1
286. CMA registration form for authorized dealers
287. Requirements brokerage firms re senior and executive positions
288. The Unified System of the Charitable Societies
289. Predicate Offences overview
290.

ANNEX 4: ANTI MONEY LAUNDERING STATUTE 2003 (AMLS)

Kingdom of Saudi Arabia
Ministry of Interior
Anti-Money Laundering Law & its *Implementing Regulations*
Royal Decree No. M/39
25 Jumada II 1424/23 *August 2003*

Article 1

The following terms and phrases, wherever mentioned in this Law, shall have the meanings expressed next to them, unless the context requires otherwise:

1. Money Laundering: Committing or attempting to commit any act for the purpose of concealing or disguising the true origin of funds acquired by means contrary to *Shari'ah* or law, thus making them appear as if they come from a legitimate source.
2. Funds: Assets or properties of whatever type, tangible or intangible, movable or immovable, as well as legal documents and deeds proving ownership of the assets or any right pertaining thereto.
3. Proceeds: Any funds obtained or acquired directly or indirectly by committing a crime punishable pursuant to the provisions of this Law.
4. Means: Anything used or prepared for use in any form for committing a crime punishable pursuant to the provisions of this Law.
5. Financial and Non-Financial Institutions: Any institution in the Kingdom undertaking one or more of the financial, commercial or economic activities, such as banks, money exchange, investment and insurance companies, commercial companies, sole proprietorships, vocational activities or any other similar activity specified by the Implementing Regulations of this Law.
6. Transaction: Any disposal of funds, possessions or proceeds in cash or in-kind, including, for example: deposit, withdrawal, transfer, sale, purchase, lending, exchange or use of safe deposit boxes and the like, as specified by the Implementing Regulations of this Law.
7. Criminal Activity: Any activity constituting a crime punishable by *Shari'ah* or law, including the financing of terrorism, terrorist acts and terrorist organizations.
8. Preventive Seizure: Temporary ban on transport, transfer, exchange, disposal, movement, possession or temporary seizure of funds and proceeds, pursuant to an order issued by a court or a competent authority.
9. Confiscation: Permanent dispossession and deprivation of funds, proceeds or means used in a crime, pursuant to a judicial judgment rendered by a competent court.
10. Monitoring Agency: The governmental agency empowered to license, monitor or supervise financial and non-financial institutions.
11. Competent Authority: Any governmental agency entrusted, according to its jurisdiction, with combating money laundering transactions.

Regulation 1-1

One of the funds in paragraph (2) of this article financial instruments negotiable bearer or endorsed without restriction in favor of an unknown or beneficiary becomes the right of ownership when extradition is not documentation contained the names of the beneficiaries such as traveler's checks, checks, Sear, and payment orders.

Regulation 1-2

The following are deemed activities provided for in paragraph (5) of this Article:
(a) Acceptance of deposits, borrowing, opening of accounts.
(b) Insurance, finance lease.
(c) Money transfer services.
(d) Issuance and management of means of payment (credit cards, traveler's checks, bank cards).
(e) Issuance of guarantees and credits.
(f) Trading or dealing in monetary instruments or dealing in foreign currencies.
(g) Trading and financial brokerage.
(h) Real estate transactions and Trust service.
(i) Dealing in valuable metals, precious stones or rare commodities, like antiques.
(j) Trade in goods with high value such as luxury cars and goods offer in auction houses.
(k) Law practice and company service.
(1) Accounting and auditing.

Regulation 1-3

The following are deemed activities provided for in paragraph (6) of this Article:
(a) Mortgage.
(b) Transfer between accounts.
(c) Gifts.
(d) Currency exchange.
(e) Trading securities.
(f) Purchase or sale of any stocks, securities or certificates of deposits.

(g) Authentication of contracts and power of attorney by the notary publics.

Regulation 1-4
The authority in charge of preventive seizure provided for in paragraph (8) of Article (1), is the Bureau of Investigation and Public Prosecution, pursuant to what is provided for in Article 12 of The Anti-Money Laundering Law and its Implementing Regulations.

Article 2
Anyone who commits any of the following acts shall be committing a money laundering crime:
(a) Conducting any transaction involving funds or proceeds, with the knowledge that they are the result of a criminal activity or from unlawful or illegal sources.
(b) Transporting, acquiring, using, keeping, receiving, or transferring funds or proceeds with the knowledge that they are the result of a criminal activity or from unlawful or illegal sources.
(c) Concealing or disguising the nature of funds, proceeds or their source, movement, ownership, place or means of disposal, with the knowledge that they are the result of a criminal activity or from unlawful or illegal sources.
(d) Financing terrorism, terrorist acts and terrorist organizations.
(e) Participating by way of agreement, aiding and abetting, incitement, counsel, advice, facilitating, collusion, covering or attempting to commit any of the acts stated in this Article.

Regulation 2-1
Financing terrorism, terrorist acts and terrorist organizations includes funds resulting from lawful sources.

Regulation 2-2
Knowledge can be inferred from the objective and factual conditions and circumstances; thus creating an element of criminal intent constituting one of the crimes provided for in this Article.

Regulation 2-3
Examples of the criminal activities or the unlawful or illegal sources whereby the dealing in funds resulting therefrom is deemed a money laundering crime are as follows:
(a) Crimes provided for in Article (1) of the Implementing Regulations of the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, for the year 1988, which was ratified by the Council of Ministers' Resolution No (168) dated 11/8/1419H.
(b) Organized crimes provided for in the United Nations Convention for Controlling Transnational Organized Crimes (Palermo Convention) issued in December 2000 and ratified by Royal Decree No. (m / 20) and the date of e 24/3/1425.
(c) The crimes set out in paragraph (5) of Article II of the International Convention on the Suppression of the Financing of Terrorism, ratified by Royal Decree No. (m / 62) and the date of e 18/7/1428.
(d) Smuggling, manufacturing, trading in or promoting intoxicants.
(e) Crimes of money counterfeiting provided for in the Royal Decree No (12) dated 12/7/1379H.
(f) Forgery crimes provided for in the Anti-Forgery Law issued by Royal Decree No (114) dated 26/11/1380H amended by Royal Decree No (53) dated 5/11/1382H.
(g) Bribery crimes provided for in the Anti-Bribery Law issued by Royal Decree No (36) dated 29/12/1412H.
(h) Smuggling weapons and ammunitions or explosives, or manufacturing or trading in them.
(i) Procurement and preparation of brothels or exercising of debauchery.
(j) Plundering or armed robbery.
(k) Thefts.
(1) Defraud and swindling.
(m) Embezzlement of public funds of government bodies or that which the state contributes to, as well as private funds of companies and commercial establishments and the like.
(n) Engaging in banking activities illegally, as provided for in Article (2) of the Banks Monitoring Law, issued by Royal Decree No (5) dated 22/2/1386H
(o) Mediation in the securities without a license provided for in Article (31) and dealing in security based on information obtained from an insider provided for in Article (50) of the Capital market law by Royal Decree No. (M / 30) and the date of e 2/6/1424.
(p) Mediation in the insurance business without a license provided for in Article (18) of the Cooperative Insurance Companies law by Royal Decree No. (m / 32) and the date of 2/6/1424 e.
(q) Crimes related to commercial activities such as fraud in brands, weights and prices as well as imitation of goods and commercial concealment as provided for in Article (1) of Anti-Commercial Concealment Law, issued by Royal Decree No (M/49) dated 16/10/1409H .

(r) Smuggling provided for in the Unified Customs Law for the GCC States, issued by Royal Decree No (241) dated 26/10/1423H Tax evasion crimes.

Article 3

Anyone who commits or participates in any of the acts specified in Article (2) of this Law, shall be committing a money laundering crime, including chairmen of the boards of directors of financial and non-financial institutions, board members, owners, employees, authorized representatives, auditors or their hired hands who act in these capacities, without prejudice to the criminal liability of the financial and non-financial institutions for that crime if it has been committed in their names or on their behalf.

Regulation 3-1

Provisions of this Law and its Implementing Regulations shall apply to financial and non-financial institutions established in the free zones within the Kingdom.

Regulation 3-2

Provisions of this Law and its Implementing Regulations shall apply to financial and non-financial institutions and their branches and subsidiaries operating within and outside the Kingdom.

Regulation 3-3

The crime was committed in the name or on behalf of the financial and non-financial institution for the purpose of direct or indirect material or immaterial gain.

Article 4

Financial and non-financial institutions shall not conduct any financial or commercial transaction, or otherwise under a false or unknown name. The identity of the clients shall be verified against official documents, at the outset of dealing with these clients or when concluding commercial deals whether directly or on their behalf. Such institutions shall verify the official documents of the corporate entities showing the name of the institution, its address, names of proprietors and managers authorized to sign on its behalf and the like, as provided for in the Implementing Regulations of this Law.

Regulation 4-1

Financial and non-financial institutions and professions shall fully comply with instructions issued by the monitoring entities such as the Saudi Arabian Monetary Agency, Capital Market Authority, Ministry of Commerce and Industry and Ministry of Justice, pertaining to the principle of "know your client" and due diligence provided that it shall include the following as a minimum:

4-1-1 Verifying the identities of all permanent or occasional clients of financial and non-financial institutions against Valid officially certified original documents proving their identities as follows:

(a) Saudi nationals:

• National identification card or family record.

• Address of the person, place of residence and place of work.

(b) Individual expatriates:

• residence permit (Iqamah) or a five-year special residence permit or a passport or National identification for GCC nationals or a diplomatic identification card for diplomats.

• Address of the person, place of residence and place of work.

(c) Corporate persons:

• Licensed companies, establishments and stores:

- Commercial register issued by the Ministry of Commerce and Industry.

- License issued by the Ministry of Municipal and Rural Affairs for service establishments and private stores.

- Articles of association, if any.

- National identification card for the Saudi national who owns the commercial firm or the licensed service company to ensure that the merchant's name in the commercial register or the licenses is identical to his name and other details in the national identification card and that such card is valid.

- A list of the persons who own the firm whose names are provided in the articles of association and their amendments, if any, and a copy of the identification cards of each of them.

- A list of the persons authorized by the owner who are qualified to deal with the accounts, pursuant to what is provided for in the commercial register or according to a power of attorney issued by a notary public, or an authorization made at the bank and a copy of the identification card of each.

• Resident companies:

- A copy of the commercial register issued by the Ministry of Commerce and Industry.

- A copy of the articles of association and their annexes.

- A license activity.

- A copy of the identification card of the manager in charge.

- A power of attorney issued by a notary public or a special authorization from the person(s), who, pursuant to the articles of association, have the power to authorize individuals to sign on their behalf.
- A copy of the identification cards of the firm owners whose names are provided in the articles of associate on and their amendments.

Regulation 4-2
Verifying the identity and legal status of actual clients and beneficiaries for all customers defined as the natural person ultimately owning or controlling a customer or on whose behalf a transaction is being conducted, before opening an account or the initiation of transaction with any financial and non-financial institution.

Regulation 4-3
Data related to the verification of identity shall be updated periodically or whenever there is a doubts about the accuracy or adequacy of the data obtained in advance at any stage of dealing with the actual client or true beneficiary, and whenever there is a suspicion of money laundering or terrorist financing regardless Amounts of the limits of the process.

Regulation 4-4
Determine whether any customer is acting on behalf of another person and to take measures to identify and verify the identity of that person, with particular attention to accounts and business relationships operated under power of attorney.

Regulation 4-5
Enhanced due diligence performed for higher-risk categories of customer, business relationships, or transactions.

Regulation 4-6
Simplified due diligence measures are not acceptable whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply.

Regulation 4-7
It shall not be acceptable from an agent, such as a lawyer, an accountant or a broker, and the like, to use the non-disclosure of clients' confidential information as an excuse when completing identity verification data in the manner mentioned above.

Article 5

Financial and non-financial institutions shall keep, for a period of not less than ten years from the date of completion of the transaction or closing of the account, all records and documents to show the financial dealings, commercial and cash transactions, whether domestic or foreign and, to retain account files, business correspondence and copies of personal identification documents.

Regulation 5-1
Financial and non-financial institutions shall retain a copy of the personal identification documents of their clients and of any document pertaining to the transactions conducted.

Regulation 5-2
Financial and non-financial institutions shall maintain a record including all details of the transactions made to ensure:
(a) Fulfillment of the requirements of the Anti-Money Laundering Law.
(b) Sufficient to enable the Financial Intelligence Unit and the investigation and a judicial authority to trace and reconstruction of each transaction.
(c) Answering, within the specified period, all inquiries made by the Financial Intelligence Unit and the investigation or a judicial authorities.

Regulation 5-3
If financial and non-financial institutions are required, pursuant to the provisions of this Law, to maintain any transaction or account records beyond the minimum time required by the law, they shall keep the original records or documents until the conclusion of the time specified in the request.

Article 6
Financial and non-financial institutions shall establish precautionary and internal monitoring measures to uncover and foil any of the crimes provided for in this Law and comply with the instructions issued by the competent monitoring authorities in this field.

Regulation 6-1
The competent monitoring authorities shall set and develop the appropriate regulatory instructions and rules to be applied against the crimes prescribed by law, and the means and controls necessary to ensure compliance of financial and non-financial institutions with laws, rules and regulations to combat money laundering and the financing of terrorism.

Regulation 6-2
Precautionary and internal monitoring measures established by the financial and non-financial institutions to uncover the crimes provided for in this Article, shall include the following:
(a) Setting written and effective controls to prevent exploitation of those institutions in money laundering transactions and/or the financing of terrorism and to assist in uncovering suspicious transactions, and to prevent the misuse of technological developments in money laundering or terrorism financing schemes, and to address and manage the risks associated with non-face to face business relationships or transactions.
(b) Ensuring that the instructions issued by the monitoring authority are the minimum applicable instructions.
(c) Following up and monitoring to ensure application of instructions and adequacy of measures.
(d) Updating such controls periodically in line with developments in money laundering or the financing of terrorism activities.

Article 7
Upon availability of sufficient indications and evidence showing that a complex, an immense or an unusual deal or transaction has been made, or that an activity of suspicious nature or purpose is underway, or is related to money laundering, financing terrorism, terrorist acts, or terrorist organizations, financial and non-financial institutions shall promptly take the following measures:
(a) Immediately report said transaction to Financial Intelligence Unit provided for in Article (11) of this Law.
(b) Prepare a report detailing all available data and information about such transactions and the parties involved, and provide the Intelligence Unit with such report.

Regulation 7-1
Financial and non-financial institutions shall establish indicators of suspicion of money laundering or the financing of terrorism. They shall continuously update such indicators to keep up with developments and diversification of means for conducting such transactions while complying with instructions issued by monitoring agencies in that regard, and to pay special attention to unusual patterns of transactions that have no apparent or visible economic or lawful purpose.

Regulation 7-2
Financial institutions and non-financial institutions are required to report to the Financial Intelligence Unit all suspicious transactions, including any attempts to carry out such transactions.

Regulation 7-3
Notification of the Financial Intelligence Unit shall be according to the form approved by the Unit, provided that the notification shall include the following information at a minimum:
(a) Names of the accused, information about their addresses and telephone numbers.
(b) A statement of the suspicious transaction, parties involved circumstances of its discovery and its current status.
(c) Determining the amount subject of the suspected transaction and relevant banking or investment accounts.
(d) Reasons and causes for suspicion upon which the reporting officer relied.

Regulation 7-4
The report prepared by the financial and non-financial institutions regarding reported transactions shall observe the following:
(a) Financial institutions shall submit the report to the Financial Intelligence Unit within ten days from the date of notification, provided that it includes the following:
- Account statements for a period of six months.
- Copies of the documents attached to the documents for opening the account.
- Data related to the nature of the transactions reported.
- Indications and justifications for suspicion along with supporting documents.
(b) When requested by the Unit, non-financial institutions shall submit their reports on the notifications within two weeks from the date of request. The request may include the following:
- Information on the reported party.
- Statement of the business or financial transactions concerning the reported person or the related parties.
- Submission of indications and grounds for suspicion together with supporting documents.

Article 8
As an exception to the provisions concerning banking confidentiality, financial and non-financial institutions shall submit documents, records and information to the judicial or competent authority upon request.

Regulation 8-1
The judicial authority or the Bureau of Investigation and Public Prosecution or the Financial Intelligence Unit shall request the documents, records, and information from the financial and nonfinancial institutions through the Anti-Money Laundering Unit at the Saudi Arabian Monetary Agency for financial institutions under its supervision, through the Anti-Money Laundering Unit at the Ministry of Commerce and Industry for non-financial institutions, and through the Anti-Money Laundering Unit at the Capital Market Authority for stock exchange transactions and institutions under its supervision, and through the Ministry of Justice for fixed properties.

Regulation 8-2
All documents, records and information shall be promptly submitted by financial and non-financial institutions to the judicial authority or the Bureau of Investigation and Public Prosecution or the Financial Intelligence Unit, upon request, through the Anti-Money Laundering Unit at the Saudi Arabian Monetary Agency for the financial institutions under its supervision, and through the Anti-Money Laundering Unit at the Ministry of Commerce and Industry for the non-financial institutions, and through the Anti-Money Laundering Unit at the Capital Market Authority for stock exchange transactions and institutions under its supervision, and through the Ministry of Justice for fixed properties.

Regulation 8-3
Financial and non-financial institutions may not use the principle of confidentiality of accounts, identity of clients or information recorded pursuant to any other law as a pretext for withholding information.

Article 9
Financial and non-financial institutions as well as their staff and others subject to the provisions of this Law shall not alert clients or allow for their alert or alert other related parties of suspicions regarding their activities.

Regulation 9-1
In implementing this Article and in order to avoid any act that may alert clients or others, the following shall be observed:
(a) Formal acceptance of transactions from clients and not rejecting them for appearing unusual or suspicious.
(b) Avoiding suggesting alternatives to clients or providing them with advice or counsel in order to avoid instructions concerning the transactions conducted.
(c) Keeping confidential reporting of transactions or clients or related information to the Financial intelligence Unit.
(d) Communication with clients or foreign parties to inquire about the nature of the transactions shall not lead to suspicions.
(e) Not informing clients that their transactions are under review or monitoring or the like.

Article 10
Financial and non-financial institutions shall introduce programs for Anti Money laundering transactions, provided that said programs include the following as a minimum:
(a) Developing and implementing policies, plans, procedures and internal controls, including appointment of qualified officers at the higher administrative level to implement the same.
(b) Setting up internal audit and control systems to ensure that basic requirements for combating money laundering are in place.
(c) Setting up continuing training programs for employees concerned, to acquaint them with the latest developments in the field of money laundering transactions and to improve their abilities to recognize such transactions, their patterns and ways of combating them.

Regulation 10-1
The director general or whoever he authorizes in the financial and non-financial institutions shall be responsible for implementing and developing policies, plans, procedures and internal controls pertaining to combating money laundering or terrorist financing.

Regulation 10-2
Financial and non-financial institutions shall designate an employee or a department to be responsible for reporting and communicating with the Financial Intelligence Unit provided for in Article (11) of this Law. With regard to small non-financial sole proprietorships, reporting shall be directly made by the establishment owner or whoever he authorizes.

Regulation 10-3
Financial and non-financial institutions shall establish a monitoring unit for conducting monitoring programs and internal audit in the field of combating money

laundering or terrorist financing, provided that the task of the external auditor, if any, shall include a special program to ensure the extent of adherence of the financial and nonfinancial institutions to the polices of combating money laundering or terrorist financing.

Regulation 10-4
Financial and non-financial institutions shall seek the assistance of the competent monitoring authorities when introducing means to ensure adherence to laws, regulations, and rules prescribed for combating money laundering or terrorist financing.

Regulation 10-5
Financial and non-financial institutions shall set up plans, and programs and allocate budgets for training and qualifying their staff in the field of combating money laundering or terrorist financing according to the size and activity of such institutions, in coordination with the relevant monitoring authorities.

Regulation 10-6
Assistance of specialized domestic and foreign institutions shall be sought in implementing the preparation, qualification and training programs in the field of combating money laundering or terrorist financing. Said training programs shall cover the following:
(a) Agreements, laws, rules and instructions related to combating money laundering or terrorist financing.
(b) Policies and laws of the monitoring authorities in the field of combating money laundering or terrorist financing.
(c) New developments in the field of money laundering transactions and terrorist financing and other suspicious transactions and ways of recognizing such transactions, their patterns, and ways of combating them.
(d) Civil and criminal liability of each employee pursuant to the pertinent laws, regulations and instructions.

Article 11
A unit for combating money laundering shall be established under the name of "Financial Intelligence Unit". Its responsibilities shall include receiving notifications, analyzing them and preparing reports regarding suspicious transactions in all financial and non-financial institutions. The Implementing Regulations of this Law shall specify the seat of this Unit, its formation, powers, method of discharging its duties as well as to whom it reports.

Regulation 11-1
The Unit's seat and to whom it reports: The Unit shall report to the Assistant to the Minister of Interior for Security Affairs. Its main seat shall be in the city of Riyadh. It may have branches in different parts of the Kingdom.

Regulation 11-2
Formation of the Unit: It shall be formed of a chairman and an assistant and a sufficient number of specialists in money laundering crimes or terrorist financing, in the financial, accounting, legal, computer and security fields.

Regulation 11-3 Jurisdiction of the Unit: The Unit shall have power to:
(a) Receive notifications from financial and non-financial institutions and other government agencies and individuals concerning transactions suspected of being money laundering or terrorist financing crimes.
(b) Create a database to be provided with all reports and information related to money laundering or terrorist financing. This database shall be regularly updated, kept confidential and make them available to competent authorities.
(c) Request and exchange information with related agencies and take the necessary measures to combat money laundering or terrorist financing.
(d) Request and exchange information with other financial investigation units with respect to combating money laundering or terrorist financing, pursuant to Article (22) of this Law.
(e) Prepare the forms used by financial and non-financial institutions in reporting transactions suspected of money laundering or terrorist financing. Such forms shall include data that assist the Unit in gathering information, analysis, and investigation, entering them in the database and updating them if necessary.
(f) Gather information on reports it receives about transactions suspected to be money laundering or terrorist financing. The Unit may seek the assistance of necessary experts and specialists from agencies concerned.
(g) The Financial Intelligence Unit shall conduct field investigation and inquiry and may request the same from the security sectors at the Ministry of Interior. In the presence of sufficient evidence that the transactions reported are related to money laundering or terrorist

financing, it shall refer them to the agency in charge of investigation and prepare a detailed report providing sufficient data about the committed crime, the culprit(s) and the nature of such evidence, accompanied by the opinion, together with all relevant documents and information.
(h) Request the Bureau of Investigation and public Prosecution to carry out the preventive seizure of funds, properties and means relating to a money laundering or terrorist financing crime as provided for in Article (12) of this Law.
(i) Take action with regard to reports, and information where information gathering and analysis indicate the absence of evidence or suspicion of the commission of any of the acts provided for in Article (2) of this Law.
(j) Coordinate with the authorities monitoring financial and non-financial institutions to make available means necessary to verify the adherence of such institutions to the laws, regulations and instructions prescribed for combating money laundering or terrorist financing.
(k) Provide feedback to financial and non-financial institutions reporting and to the competent authorities with combating money laundering and terrorist financing.
(1) Participate in organizing awareness programs on combating money laundering or terrorist financing, in coordination with the Permanent Committee for Combating Money Laundering.
(m) Submit necessary recommendations to the Permanent Committee for Combating Money Laundering about the difficulties and suggestions in the field of combating money laundering or terrorist financing.
(n) The Financial Intelligence Unit may enter into memorandums of understanding with other financial investigation units pursuant to applicable laws and procedures.
(o) Take necessary legal procedures to join the Financial Investigation Units Group (The Egmont Group).

Regulation 11-4
Departments of the Unit: The Unit shall be composed of the following departments:
(a) Department of Reports.
(b) Department of Information Gathering and Analysis
(c) Department of Information Exchange.
(d) Department of Information and Studies.
First: Department of Reports:
(1) Receiving reports on dubious and suspicious transactions regarding their nature and purpose or that they relate to money laundering or terrorist financing.
(2) Receiving reports by fax or any other means. In case of telephone reports, they shall be confirmed as soon as possible in any written form.
(3) Receiving reports shall be in the form prepared by the Unit and provided to all related departments and financial and non-financial institutions.
(4) Recording the reports in special records with serial numbers, under which all necessary information is entered.
(5) Referring reports to the Department of Information Gathering and Analysis to determine the existence of suspicion and indications of a money laundering or terrorist financing crime.
Second: Department of Information Gathering and Analysis:
(1) Ensuring that the report includes the necessary information as well as attaching documents necessary for analysis.
(2) Requesting the relevant agency to provide information, reports, and documents needed for analysis when necessary.
(3) Reviewing data and information included in the report and comparing them with information available to the Department to verify their accuracy and assess their appropriateness, making use of records of security, financial, commercial and other related agencies.
(4) In the presence of sufficient indications that the transactions stated in the report are related to money laundering or terrorist financing, and a need arises for field investigations or the arrest of persons or tracking funds or assets under suspicion, the Unit shall do so. It may request the relevant security agencies in charge of investigation and inquiry at the Ministry of Interior to do the same. Hence, prepare an analytical report including their views, accompanied by the relevant report, and documents to complete the procedures and refer it to the agency in charge of investigation.
(5) Requesting the Bureau of Investigation and public Prosecution to carry out preventive seizure of funds, properties, and means related to a crime of money laundering as stipulated in Article (12) of this Law.
(6) Deal with reports and information, where information gathering and analysis indicate the absence of evidence or suspicion of the commission of any of the acts provided for in Article (2) of this Law.
Third: Department of Information Exchange and Follow up:

(1) Exchange of information with domestic authorities and similar units in foreign countries with respect to combating money laundering or terrorist financing.
(2) Providing the Department of Information and Studies with the number of requests received by the Department periodically every month, whether domestic or foreign.
Fourth: Department of Information and Studies:
(1) Creating a database for the following:
(a) Reports on suspicious transactions received and analyzed and traced.
(b) Reports referred to security agencies to complete the investigation and inquiry procedures or to the competent investigation agency.
(c) Reports leading to judicial or administrative action.
(d) Convictions in money laundering or terrorist financing cases.
(e) Requests for exchange of information received by the Unit from local authorities and foreign counterparts.
(f) Number of reports shelved and grounds thereof.
(2) Monitoring indicators of money laundering or terrorist financing crimes in financial and non-financial institutions and ways of perpetrating them as well as proposing solutions and measures to be taken for combating them and referring the same to the Permanent Committee for Combating Money Laundering.
(3) Preparing an annual report on the unit's work and forwarding it to the Minister of Interior as well as providing the Permanent Committee for Combating of Money Laundering with a copy thereof.
(4) Keeping apprised of recent developments related to money laundering or terrorist financing crimes through relevant regional and international organizations and commissions.
(5) Participating in organizing awareness programs with respect to combating money laundering or terrorist financing, in coordination with the Permanent Committee for Combating Money Laundering.

Article 12
The Financial Intelligence Unit upon establishment of suspicion shall request the authority in charge of investigation to carry out preventive seizure to the funds, properties and means associated with a money laundering crime, for a period not exceeding twenty days. Should there be a need for the preventive seizure to continue for a longer period, it shall be pursuant to a judicial order from the court of competent jurisdiction.

Regulation 12-1
The preventive seizure shall take place on all funds, properties or means owed to the suspect(s) and are in the possession of individuals, companies, financial and non-financial institutions or any other entity.

Regulation 12-2
The request for preventive seizure shall be issued by the Head of Financial Investigation Unit or whoever he deputizes.

Regulation 12-3
The preventive seizure request shall be made by a memorandum that includes a full statement of the following:
(a) Detailed information of the persons whose funds, properties or means to be seized.
(b) Specification of funds, properties and means to be seized.
(c) Suspicions, recitals and confirmed reasons supporting the seizure.
(d) Duration of the preventive seizure shall not exceed the period stated in this Article.

Regulation 12-4
The request for preventive seizure shall be sent in an appropriate confidential manner to the Bureau of Investigation and Public Prosecution. The request for seizure shall be promptly acted on, and the Financial Investigation Unit shall be notified of the decision within 48 hours.

Regulation 12-5
The period of the preventive seizure specified in this Article shall start from the date of its imposition.

Regulation 12-6
Upon issuance of the approval of the Bureau of Investigation and Public Prosecution of the request of the Financial Intelligence Unit, the Unit of combating money laundering at the Saudi Arabian Monetary Agency shall be addressed to seize funds deposited in financial institutions, the Ministry of Commerce and Industry to seize properties and whatever relates to the activities of nonfinancial institutions, the Ministry of Justice to seize lands and real estate, the Directorate of Public Security to seize means, the Customs Authority to seize goods and means under its control and the Capital Market Authority to seize securities. The Financial Intelligence Unit shall be notified thereof.

Regulation 12-7
Procedures regarding the request or an order for continuation of seizure shall be taken before the end of the twenty- day period by a sufficient time.

Regulation 12-8
The investigation authority, upon issuance of an order for continuation of the preventive seizure, shall inform the monitoring and security agencies to enforce the court order and notify the financial Intelligence Unit thereof.

Regulation 12-9
If the authority in charge of the investigation deems that it is not necessary to impose preventive seizure on funds, properties and means, mentioned in the request submitted by the Unit, such authority shall promptly notify the Unit in writing of its disapproval of such request, giving its views thereon.

Regulation 12-10
The monitoring agencies and authorities in charge of combating money laundering may request through the Financial Intelligence Unit the imposition of the preventive seizure in compliance with the period specified in the Law.

Regulation 12-11
The request for the continuation of the preventive seizure shall be through a petition deposited with the court, including the following:
(a) The court with which the lawsuit is filed.
(b) Date of submission of request.
(c) Subject of the lawsuit and what is requested by the public prosecutor and supporting evidence.
(d) The requested duration of seizure.

Article 13
Information disclosed by financial and non-financial institutions may be exchanged, according to the provisions of Article (8) of this Law between these institutions and the competent authorities, should such information be related to a violation of the provisions of this Law. The competent authorities shall observe the confidentiality of such information and not disclose it, except as necessary for use in investigations or lawsuits related to the violation of the provisions of this Law.

Article 14
The Implementing Regulations of this Law shall determine the rules and procedures of disclosure of cash amounts and precious metals permitted to enter or leave the Kingdom and shall determine the amounts of money and weights required to be disclosed.

Regulation 14-1
Estimated cash or financial instruments negotiated by the bearer or precious metals that must be disclosed when leaving or entering the Kingdom of "60.000" sixty thousand riyals or its equivalent in foreign currency.

Regulation 14-2
Prevent exit or entry of any traveler cash or financial instruments of negotiable bearer or precious metals exceeding the limit without the mobilization model disclosure in the case of controlling the security authorities, customs or the amount of financial instruments or negotiable bearer or precious metals that have not and disclosed more than the limit referred to the customs (the official) to investigate the reasons for non-disclosure if the reasons for his conviction required the mobilization of the passenger model disclosure and complete the remaining procedures for disclosure and allowed to leave or enter, including him, but in the absence of belief in the customs official reasons or suspected money laundering or the financing of terrorism reference is the traveler to the competent authority for investigation and to inform the Financial Intelligence Unit to do so.

Regulation 14-3
In the event of the outgoing passenger carrying precious metals worth more than sixty thousand riyals and wished to remove them from Saudi Customs shall review the disclosure by a performing seal and model disclosure and bill the purchase to ensure their value and if they applied for commercial purposes right the Unified Customs Law and its implementing regulations.

Regulation 14-4
In the seizure of the outgoing passenger next to the Kingdom or in cases of repeated or not releasing in the event of releasing the relationship of suspicion and generate funds out suspicious money laundering or financing terrorism or providing false statements about him disclosure of cash or financial instruments that can be converted or precious metals over Value limit and be prepared record by the officer, which shall refer it to Customs and the Customs and then transmitted to the competent authority to investigate

the claim to punish him according to article "20" of the anti-money laundering regime or the customs system, as is clear from the investigation and notify the Financial Intelligence Unit and the excess amount shall be deposited The limit by customs in a special account secretariats and precious metals are impounded by Customs pending the receipt of a signal from the investigation.

Regulation 14-5
Customs inspections on the basis of a random sample or provide information on the suspected money laundering or the financing of terrorism and out of control for cash or financial instruments negotiable bearer or precious metals.

Regulation 14-6
Unveiled at next to Saudi customs officer to get him to cash or financial instruments of negotiable bearer or precious metals worth more than the limit For the customs officer in the port to ensure the safety of cash from counterfeiting by the representative of SAMA, and for precious metals It is required to prove ownership under the invoice and if it finds it for commercial purposes is administered by the Unified Customs Law and its implementing regulations.

Regulation 14-7
Send a copy of the information disclosure forms as agreed upon by the Customs Department of Financial Intelligence Unit set forth in the article "11" from the system of checking people from a crime of money laundering or terrorist financing or any other crimes.

Regulation 14-8
Review in the absence of owners of these funds or precious metals after the expiration of the period of "90" ninety days treated in accordance with applicable regulations seizures.

Regulation 14-9
These procedures apply to companies or financial institutions and nonfinancial and gold shops and missions of the Hajj and Umrah and service companies for the transfer of cash or postal parcels and other postal and missions while maintaining its right to exercise its work.

Regulation 14-10
Customs Department to develop a database of names of persons who had previously disclosed or not to know the purpose of which is repeated with the notice of the Financial Intelligence Unit.

Regulation 14-11
Customs prepare the model disclosure referred to in this article after coordination with the Financial Intelligence Unit and distribution outlets.

Regulation 14-12
The Ministry of the Interior and the Ministry of Finance to report such actions necessary instructions to various means available and provide guidance in several paintings prominently at the entry and exit points around pointing out the procedures and sanctions to be applied in case of violating the order.

Article 13
If a judgment to confiscate funds, proceeds or means is rendered pursuant to the provisions of this Law, and they are not required to be destroyed, the competent authority shall dispose of them according to the law or share them with countries which are parties, with the Kingdom, to agreements or treaties in force.

Regulation 15-1
The competent authority provided for in this Article and which is in charge of disposal of confiscated funds, proceeds and means is the authority enforcing the preventive seizure.

Regulation 15-2
The competent authority provided for in this Article and which is in charge of sharing confiscated funds, proceeds and means with countries that are parties with the Kingdom to agreements or treaties in force is the Mutual Legal Assistance at the Ministry of Interior.

Regulation 15-3
The request for confiscation of funds, proceeds or means shall be stated in the prosecution's accusatory pleading and in the judicial judgments rendered by the courts in this regard.

Regulation 15-4
The confiscation judgment shall include funds, proceeds or means subject of the crime, whether seized or not seized inside or outside the country.

Regulation 15-5
In implementing this Article regarding funds, proceeds or means confiscated pursuant to a judgment, the following shall be observed:

(a) Article (94) of the Law of Criminal Procedures and its Implementing Regulations regarding materials that perish over time or the preserving of which requires huge expenses that consume its value.
(b) Depositing confiscated funds, proceeds or means with the state treasury.
(c) The Council of Ministers' Resolution No. (47) dated 28/1/1421H providing for the transfer, to an independent account at the Saudi Arabian Monetary Agency, of funds seized in the possession of the accused in drug cases and the value of materials regarding which confiscation judgments were rendered. Funds in said account shall be used towards covering the needs of the General Directorate for Combating Drugs.

Article 16
Anyone who commits a crime of money laundering, as provided for in Article (2) of this Law, shall be subject to imprisonment for a period not exceeding (10) years and a fine not exceeding five million riyals, or by either punishment, along with the confiscation of funds, proceeds and means subject of the crime. Should the funds and proceeds mix with funds acquired from legitimate sources, said funds shall be subject to confiscation within limits equal to the estimated value of the illegal proceeds.

The competent court may exempt from these punishments the owner, possessor, or user of the funds or proceeds subject of incrimination, if he notifies the authorities prior to their knowledge of the sources of the funds or proceeds and the identity of accomplices, without him benefiting from their revenues.

Regulation 16-1
The investigating authority shall assess the estimated value of the illegal proceeds by seeking the assistance of experts. A judgment from a competent court shall be rendered in this regard.

Regulation 16-2
Request for consideration of exemption from punishments of the notifying person shall be made by the authority in charge of investigation.

Regulation 16-3
Upon receiving such notifications, procedures for investigation and inquiry shall be taken so as to ensure that the authorities have no knowledge of the crime.

Article 17
The punishment of imprisonment shall be for a period not exceeding fifteen years and a fine not exceeding seven million Saudi riyals, if the money laundering crime is coupled with one of the following cases:
(a) The perpetrator's committing the crime through an organized crime syndicate.
(b) The perpetrator's use of violence or weapons.
(c) The perpetrator's holding of a public post to which the crime is connected or exploiting his authorities or influence in the commission of the crime.
(d)Deceiving or exploiting women and minors.
(e) Committing the crime through a correctional, charitable or educational institution or in a social service facility.
(f) Issuance of previous domestic or foreign judgments convicting the perpetrator, especially for similar crimes.

Article 18
Without prejudice to other laws, any chairman of the board of directors of financial and non-financial institutions, board member, owner, manager, employee, authorized representative, or hired hand acting in these capacities, who fails to fulfill any of the obligations provided for in Articles (4, 5, 6, 7 ,8, 9 and 10) of this Law shall be subject to imprisonment for a period not exceeding two years and a fine not exceeding five hundred thousand riyals or by either punishment. The punishment shall apply to those engaging in the activity without obtaining the required licenses.

Regulation 18-1
In this Article, "other laws" means all laws issued by agencies monitoring financial and non- financial institutions, such as Companies Law, Law of Commercial Register, Banks Monitoring Law and the Capital market law.. etc.

Article 19
Pursuant to a judgment based upon a petition submitted by the competent authority, a fine of not less than one hundred thousand riyals and not exceeding the value of funds subject to the crime may be imposed on financial and non-financial institutions whose liability is proven pursuant to the provisions of Articles (2) and (3) of this Law.

Regulation 19-1
The competent authority in this Article IS the Bureau of Investigation and Public Prosecution.

Regulation 19-2
The liability lawsuit of financial and non-financial institutions shall be based on technical reports issued by the monitoring agencies in addition to other proving methods.

Regulation 19-3
Application of punishments provided for in this Article shall not conflict with administrative or disciplinary penalties provided for in other laws which may be imposed on financial and non- financial institutions by the monitoring agencies with regard to establishing their liability.

Article 20
With the exception of punishments provided for in this Law, anyone violating its provisions shall be subject to imprisonment for a period not exceeding six months and a fine not exceeding one hundred thousand riyals, or by either punishment.

Article 21
The punishments specified in this Law shall not apply to those who violate it in good faith.

Regulation 21-1
Good faith shall be determined by the competent judicial authority and shall be inferred from the objective conditions and circumstances.

Article 22
Information disclosed by financial and non-financial institutions may be exchanged between those institutions and the competent authorities in other countries which are parties, with the Kingdom, to agreements and treaties in force or on the basis of reciprocal treatment, pursuant to established legal procedures, provided that this shall not prejudice the provisions and practices related to the confidentiality of financial and non-financial institutions.

Regulation 22-1
Competent authorities in other countries provided for in this Article refer to the Financial Intelligence Unit or its equivalent in terms of functions.

Regulation 22-2
Information disclosed by the financial and non financial institutions concerning a money laundering or terrorist financing crime shall be exchanged through the Financial Intelligence Unit.

Regulation 22-3
When exchanging information pursuant to the provisions of agreements and treaties in effect or on the basis of reciprocal treatment, the following shall be observed:
(a) Information exchanged shall only be used for the purpose it is requested for.
(b) Information exchanged shall not be disclosed to a third party except with the approval of the Financial Intelligence Unit.

Article 23
Upon request from a court or a competent authority in another country which is a party with the Kingdom to an agreement or treaty in force or on the basis of reciprocity, the judicial authority may order seizure of funds, proceeds or means related to a money laundering crime, according to the laws in force in the Kingdom. Upon request from a competent authority in another country, which is a party with the Kingdom to an agreement or treaty in force or on the basis of reciprocity, the competent authority may order tracing of funds, proceeds or means associated with a money laundering crime, according to laws in force in the Kingdom.

Regulation 23-1
Requests received from other countries regarding seizure or tracing of funds, proceeds or means related to money laundering or terrorist financing crime, shall be deemed one of the functions of the Mutual legal Assistance Committee based in the Ministry of the Interior and problem resolution by the Council of Ministers (No. 168) in e 11/8/1419 Amended Resolution No. (3) 7/1/1424 e, and legal procedures shall be taken in such a matter.

Regulation 23-2
Requests related to seizure of funds, proceeds or means regarding money laundering crime, shall be referred to the Board of Grievances to render the judicial judgments for implementation by the competent monitoring agencies. The Financial Investigation Unit shall be informed thereof.

Regulation 23-3
Requests related to tracing of funds, proceeds or means regarding a money laundering or terrorist financing crime shall be referred to the Bureau of Investigation and Public Prosecution, for implementation by the competent monitoring agencies.

Regulation 23-4
Any request submitted pursuant to this Article shall include the following:
(a) Specifying the entity submitting the request.
(b) Subject and nature of the investigation, tracing, or the judicial procedures to which the request relates, as well as the name and jurisdiction of the authority conducting these investigations, tracing or judicial procedures.
(c) A summary of relevant facts and the procedures taken.
(d) Specifying the type of request or any special procedure, which the requesting party wishes to be traced.
(e) Specifying the identity of any person concerned, his location and nationality.
(f) Specifying the funds, proceeds and means required to be seized or traced.
(g) Specifying the requested duration of seizure.
(h) Proof of judicial jurisdiction of the requesting country.

Article 24
Any final judicial judgment providing for the confiscation of funds, revenues or means related to money laundering crimes, rendered by a competent court in another country, which is a party with the Kingdom, to an agreement or treaty in force or on the basis of reciprocity, may be recognized and enforced if the funds, proceeds or means provided for in this judgment may be subject to confiscation in accordance with the applicable law in the Kingdom.

Regulation 24-1
Requests for execution of judgments received from other countries in relation to a money laundering or terrorist financing crime shall be deemed part of the functions of the Mutual legal Assistance Committee.

Regulation 24-2
Requests related to execution of foreign judgments relating to a money laundering crime shall be referred to the Board of Grievances.

Regulation 24-3
Any judgment to be recognized and executed shall include, in addition to paragraphs from (a) to (h) of Article 23-6 of these Regulations, the following:
(a) Confiscation shall be pursuant to an enforceable final judicial judgment in one of the crimes provided for in Article (2) of this Law.
(b) The confiscation judgment shall be enforceable in the Kingdom.
(c) Funds or proceeds to be confiscated may not have been previously subject of the confiscation as a result of another judicial judgment or by a competent authority.

Article 25
Chairmen of the boards of directors of financial and non-financial institutions, board members, owners, employees, hired hands or their authorized representatives, shall be exempted from criminal, civil or administrative liability which may result from the performance of the duties provided for in this Law or upon violation of any restriction imposed to ensure confidentiality of information, unless their actions are proven to be in bad faith, with the intent to harm the person conducting the transaction.

Regulation 25-1
Bad faith shall be determined by the competent judicial authority and shall be inferred from the factual or objective and circumstances.

Article 26
General courts shall have jurisdiction to decide all crimes provided for in this Law.

Article 27
The Bureau of Investigation and Public Prosecution shall investigate and prosecute before general courts crimes provided for in this Law.

Article 28
The Minister of Interior, in coordination with the Minister of Finance and National Economy, shall issue the Implementing Regulations of this Law within ninety days from the date of its issuance.

Regulation 28-1
The Implementing Regulations shall be reviewed for the purpose of updating within five years or when necessary.

Article 29
This Law shall be published in the Official Gazette and shall be effective sixty days from the date of its publication.

ANNEX 5: RULES GOVERNING ANTI MONEY LAUNDERING AND COMBATING TERRORIST FINANCING, AKA AML/CFT RULES FOR BANKS AND MONEY EXCHANGERS 2008 (RBME)

Saudi Arabian Monetary Agency
Banking Inspection Department
Second Update
December 2008

TABLE OF CONTENTS

1. Introduction

1.1 Saudi Arabia Initiatives

The past few years have seen rapid and far-reaching developments in the international financial sector involving a comprehensive and coordinated fight against money laundering and terrorist financing. Consequently, the Kingdom of Saudi Arabia has

adopted a variety of initiatives involving legislative and other measures that are responsive to international developments. Some of these initiatives adopted by Saudi Arabia are listed below:

1.1.1 International Level

- Saudi Arabia signed and ratified the United Nations Convention on Illicit Traffic of Narcotic Drugs & Psychotropic Substances (1988, Vienna).
- Saudi Arabia has signed and ratified the International Convention for the Suppression of the Financing of Terrorism (1999, New York).
- Saudi Arabia has signed and ratified the United Nations Convention against Transnational Organized Crime (2000, Palermo).
- Saudi Arabia has implemented all relevant United Nations Security Council (UNSC) Resolutions, such as Resolutions # 1267 (1999), 1333 (2000), 1373 (2001).
- Saudi Arabia is a member country of the Gulf Cooperation Council (GCC), which is a full member of the Financial Action Task Force (FATF).
- In September 2003, Saudi Arabia completed the Mutual Evaluation by a team of FATF assessors, based on the 40+8 FATF Recommendations and was one of the first countries evaluated under this new methodology. The result of this evaluation was discussed in February 2004 Plenary Meeting in Paris and was highly positive.

1.1.2 Regional & Group Level

- At a convention held in April 1998, Saudi Arabia signed and ratified the Arab Anti-Terrorism Agreement under the auspices of the Arab League.
- In July 1999, Saudi Arabia signed and ratified the Organization of Islamic Conference (OIC) Agreement for the suppression of international terrorism.
- In May 2004, Saudi Arabia signed and ratified the GCC Anti-Terrorism Security Agreement.
- Saudi Arabia is a founding member of the Middle East-North Africa FATF (MENA-FATF), which was created in November 2004 with the purpose of promoting and implementing international AML/CTF standards in the region, and adopting the FATF 40+9 Recommendations on Anti-Money Laundering and Combating Terrorist Financing.

1.1.3 National Level

- Saudi Arabia enacted the Anti-Money Laundering Law and Bylaws, under the Royal Decree # M/39 dated 25/6/1424H, ratifying the Council of Ministers Decision # 167 dated 20/6/1424H, providing a statutory basis for criminalizing money laundering and terrorist financing activities.
- In accordance with the Saudi AML Law Article 11, the Saudi Arabia Financial Intelligence Unit (SAFIU) was established under the control of the Ministry of Interior, as the central authority for receiving and analyzing suspicious transaction reports relating to money laundering and terrorist financing activities.
- Saudi Arabia has set up two National Permanent Committees from different Ministries and Government Agencies, including SAMA, to respectively deal with money laundering and terrorist financing issues in the Kingdom.

1.2 SAMA Initiatives

Since its inception in 1952, the Saudi Arabian Monetary Agency (SAMA) has been issuing various directives to banks and money exchangers relating to establishing customers' identity and other information, observing necessary due diligence when dealing with customers, record keeping of relevant documents and records as well as reporting of suspicious transactions to the competent authorities. These directives have since been put together into the following major regulatory manuals:

1.2.1 AML/CTF Regulations

In November 1995, SAMA issued its first set of guidelines relating to AML activities to all banks operating in Saudi Arabia. Consequently, in recognition of the international and legal supervisory efforts to combat the spread of money laundering, And terrorist financing SAMA further updated the initial 1995 AML Guidelines and in May 2003, issued a more extensive set of "Rules Governing Anti-Money Laundering & Combating Terrorist Financing".

The First Update issued in May 2003 provided a substantial improvement to the initial regulations and also included regulations relating to combating terrorist financing. It provided basic measures and actions to be taken to prevent, detect, control and report money laundering and terrorist financing activities. Since then, in its continued efforts to further improve and refine the regulations, and to keep abreast with the developing trends locally, regionally and globally, SAMA has issued this Second Update.

Banks and money exchangers are required to make these regulations an integral part of their systems and procedures aimed at controlling, detecting, preventing, and reporting such activities. In this regard, SAMA

intends to verify the implementation of these rules by banks and money exchangers operating in Saudi Arabia through SAMA's on-site inspections, receipt of regular compliance reports and certification by external auditors.

1.2.2 Account Opening Regulations for Banks

In May 2002, SAMA issued its first set of "Rules Governing Opening of Bank Accounts & General Operational Guidelines". The new rules, in addition to consolidating all the previous SAMA circulars on the subject, were significantly improved with new requirements to facilitate implementation and conform to the best international banking practices in line with the Basel Committee principles. The rules outlined the standard requirements applicable to all banks to serve as a regulatory instrument to strengthen internal controls with regards to opening and operation of bank accounts maintained by customers, with a view of protecting the banking industry against illegal financial activities.

In order to keep abreast with the ongoing developments and to provide more explanation and clarification to the issues raised by local banks, the initial rules were further enhanced in the First Update released in April 2003. The Second Update of the rules was issued by SAMA in February 2007, and the third Update on December 2008. SAMA is continuously reviewing and updating the Account Opening regulations and will be issuing new updates to banks and money exchangers in future.

1.2.3 Other Relevant Regulations

SAMA has also issued a number of other regulations in support of its efforts to combat money laundering, terrorist financing and other financial crime activities. Therefore, these AML/CTF Rules should be read in conjunction with the following documents issued by SAMA, in addition to the AML Law and Bylaws issued by the Saudi Government:

- Guidelines for Combating Embezzlement & Fraudulent Transactions,(second issue) in August 2008
- Qualification Requirements for Appointment to Senior Positions in Banks, issued in April 2005
- Guidelines for Banks in Saudi Arabia for Organizing Audit Committees, issued in July 1996
- Internal Control Guidelines for Banks Operating in the Kingdom, issued in December 1989
- Other relevant SAMA Regulatory Circulars, issued on various dates

1.3 Objectives

The core objectives of SAMA in issuing these regulations are as follows:

1. To ensure banks and money exchangers in Saudi Arabia comply with the Saudi AML Law & Bylaws.
2. To help banks and money exchangers operating in Saudi Arabia to comply with the Banking Control Act, AML Law, SAMA Regulations, and all relevant United Nations Security Council Resolutions.
3. To implement policies, standards, procedures and systems for the prevention, detection, control and reporting of money laundering and terrorist financing activities in accordance with the Basel Committee Principles and the FATF 40+9 Recommendations on AML/CTF.
4. To protect banks and money exchangers operating in Saudi Arabia from being exploited as channels for passing illegal transactions arising from money laundering, terrorist financing and any other financial criminal activities.
5. To maintain, enhance and protect the credibility, integrity and reputation of the Saudi Arabian banking and financial systems.
6. To provide security and appropriate degree of protection for costumers.

1.4 General Developments & Trends

By all accounts, worldwide money laundering activities, particularly those related to drugs, now constitute a multi-billion dollar business annually. It is inconceivable and unlikely that such large amounts of money can be stored or moved without the cooperation or willing participation of many international financial institutions and banking systems. In many quarters, money laundering is considered a serious threat to the integrity of many international banks and even banking systems.

Money laundering has become a widespread phenomenon involving highly sophisticated techniques to penetrate different banking systems. This has led lawmakers, law enforcement agencies and supervisory authorities in many countries to cooperate, locally and internationally, to combat this phenomenon. In this respect, the FATF was created and has carried out extensive work and issued 40+9 Recommendations to counter the spread of money laundering and terrorist financing.

The techniques used by money launderers constantly evolve to match the sources and volume of funds to be laundered, and the legal, regulatory, law enforcement

environment of the market place in which the money launderers operate.

2. Legal Framework & Regulatory Requirements

2.1 The Saudi AML Law & Bylaws

The Kingdom of Saudi Arabia, in its contributions towards the international initiatives to combat money laundering and terrorist financing crimes, has enacted the Anti-Money Laundering Law in August 2003. The Law criminalizes money laundering and terrorist financing acts and has created offenses, responsibilities and penalties for violation, aimed at preventing these crimes.

The AML Law, through its 29 Articles and the Bylaws, is applicable to all banks and money exchangers and requires all financial institutions to have in place adequate policies, systems, measures and controls in place, relating to customer identification, know your customer/ due diligence, risk assessment, monitoring and reporting suspicions, training and record keeping to deter and prevent money laundering and terrorist financing acts.

2.2 SAMA – Regulatory & Supervisory Body

The Saudi Arabian Monetary Agency (SAMA), in accordance with the authority and powers vested on it under the following relevant Saudi laws, is the legislative body responsible for exercising regulatory and supervisory control over banks and money exchangers, issuing general rules and overseeing that all banks and money exchangers comply and effectively implement the relevant laws and regulations.

1. The Charter of Saudi Arabian Monetary Agency – Articles 1 (c) and 3 (d).
2. The Banking Control Law – Article 16 (3).
3. The Anti-Money Laundering Law – Article 6 and its Bylaws 6.1 and 6.2.
4. Decision of the Minister of Finance & National Economy on Regulating Money Changing Business.

SAMA regards the adoption and implementation by all banks and money exchangers of effective policies, procedures and controls for the deterrence and prevention of money laundering, terrorist financing and other financial crimes as very vital. SAMA expects all banks and money exchangers and their employees to conduct business in accordance with these rules and all applicable laws by applying the highest ethical standards. SAMA will use these rules and other standards to measure the adequacy of each bank's or money exchanger's implementation strategies. SAMA will take appropriate disciplinary measures and actions against banks and money exchangers for any violations, in accordance with the Banking Control Law Article 25 (Rules for Enforcing Provision of the Banking Control Law).

As the regulatory and supervisory body for banks and money exchangers, SAMA has a duty not only to ensure banks and money exchangers maintain high KYC standards to protect their own safety and soundness but also to protect the integrity of their national banking system. Therefore, SAMA will exercise the following responsibilities:

1. Monitoring that banks and money exchangers are applying sound KYC procedures and are sustaining ethical and professional standards on a continuous basis.
2. Ensuring that appropriate internal controls are in place and banks and money exchangers are in compliance with supervisory and regulatory requirements.
3. SAMA examination will include review of bank's and money exchanger's policies and procedures, customer files including sampling of some accounts, documentation related to accounts maintained and the analysis made to detect unusual or suspicious transactions.
4. Taking appropriate action against banks or money exchangers and their officers and employees who demonstrably fail to follow the required procedures and regulatory requirements.

2.3 Overseas Branches & Subsidiaries of Saudi Banks & Money Exchangers

As per the Saudi AML Law Article 3 Bylaw 3.2, these regulations are also applicable to overseas branches and subsidiaries of all Saudi banks and money exchangers operating in the Kingdom. Therefore, banks and money exchangers should ensure all their foreign branches and subsidiaries apply the requirements of both the Saudi AML Law and these Rules.

In addition, banks and money exchangers should ensure the following:

1. Paying particular attention to their foreign branches and subsidiaries located in countries that do not or insufficiently apply FATF Recommendations.
2. Ensuring their foreign branches and subsidiaries apply the higher requirements of either the host country or the home country in case the requirements of the host and home countries differ.
3. Informing SAMA when a foreign branch or subsidiary is unable to observe appropriate AML/ CTF

requirements because it is prohibited by its local laws, regulations or other measures.

2.4 Legal Responsibilities of Banks/ Money Exchangers & Employees

The Saudi AML Law and Bylaws stipulate responsibilities, offenses, violations and penalties that have direct or indirect implications to the institution and to its staff personally.
(For full details of the AML Law and Bylaws, refer to Appendix7- A):

2.5 Financial Intelligence Unit (FIU)

Information gathering, investigation and analysis processes are critical elements by the concerned authorities to effectively combat and prevent money laundering, terrorist financing and other financial crimes. In response, countries around the world have created specialized governmental agencies, known as Financial Intelligence Units, to be the central office for obtaining such financial information reports.
Similarly, Saudi Arabia, as per Article 11 of the Saudi AML Law, has given a mandate to form a Financial Intelligence Unit (SAFIU) to be responsible for receiving, analyzing and disseminating to competent authorities disclosures of financial information reports on suspicious activities from financial and non-financial institutions. SAFIU has been established under the authority of the Ministry of Interior.

2.6 Cooperation Among Authorities & Banks/ Money Exchangers

Cooperation among banks/ money exchangers and various competent authorities, in the exchange and sharing of relevant information, is very vital in the AML/CTF initiatives. However, such exchange and sharing should be coordinated and achieved only through SAMA to maintain controlled flow of confidential information.

2.6.1 Cooperation With Local Authorities

Under Article 13 of the Saudi AML Law, financial institutions are authorized and required to cooperate and share relevant information with local competent authorities, such as FIU and law enforcement authorities, for matters relating to money laundering, terrorist financing and other financial crimes. Banks and money exchangers should, therefore, have in place appropriate policies and procedures, as follows:
1. Establishment of a Money Laundering Control Unit (MLCU) or a designated Compliance Officer within the bank or money exchanger, responsible for internal reporting and informing FIU with a copy to SAMA, when money laundering or terrorist financing activities are suspected. (Refer to Rule 4.7.4 of these Rules for details of MLCU).
2. The manner and method in which the MLCU/ designated Compliance Officer should contact the authorities and pass relevant transactional information to them.
3. Where records are to be provided to the authorities, establishing the form of such records (original or copies) and the receipt and forms to be used for providing and receiving information by the MLCU/ designated Compliance Officer.
4. When information is to be provided verbally to authorities, establishing the manner and form of such information.
5. In some instances, depending upon the case, a new or a different procedure may need to be developed. For example, in the event of a large cash transfer, telephone notification may be quicker than filing a report especially if immediate decision to prevent the transfer is required.

2.6.2 Cooperation Among Banks & Money Exchangers Operating in the Kingdom

Banks and money exchangers should cooperate locally through their representatives in the Financial Crimes & Money Laundering Committee (FCML) for AML/CTF matters. This should be done through the exchange of information with banks' and money exchangers' officers, and SAMA, about cases and transactions that they may discover, or suspect to be of money laundering or terrorist financing nature as required by the Saudi AML Law and Bylaws. However, at the same time they must strictly follow the legal and regulatory procedures that aim to protect customer confidentiality and banking secrecy. SAMA guidance should be obtained, if banks and money exchangers agree to mutually assist or exchange information pursuant to agreements between them.

2.6.3 International Cooperation

Recognizing the need to cooperate with international community in the fight and prevention of money laundering, terrorist financing and other financial crimes, Saudi Arabia has provided for this provision in the Law subject to agreed conventions and reciprocity arrangements. In accordance with Articles 22 and 23 of the Saudi AML Law, which allow cooperating with international governmental authorities for cases involving money laundering and terrorist financing, any sharing of information with a foreign party

whether with another bank (affiliation, branch, correspondent) or a foreign governmental authority should not be done without the prior approval of and in coordination with SAMA.

3. Money Laundering & Terrorist Financing

3.1 Money Laundering

3.1.1 Definition of Money Laundering

The Saudi AML Law defines money laundering as: any actual or attempted act aimed at concealing or camouflaging the nature or illegally or illegitimately earned property to make it look as proceeds from legal sources. The AML Law - Bylaw Article 2 states the underlying crimes relating to money laundering.

FATF defines money laundering as the process by which proceeds from criminal activities are disguised to conceal their illegal origin in order to legitimize the ill-gotten gains of crime.

Criminal activities, such as drug trafficking, illegal arms sales, smuggling, human trafficking, prostitution, corruption, embezzlement, and other activities of organized crimes, tend to generate large amounts of profits for the individuals or groups carrying out the criminal act. However, by using funds from such illicit sources, criminals risk drawing the authorities' attention to the underlying criminal activity and exposing themselves to criminal prosecution. In order to benefit freely from the proceeds of their crime, they must therefore conceal the illicit origin of these funds.

The United Nations Vienna Convention (1988) and the United Nations Palermo Convention (2000) provisions describe money laundering as the process by which proceeds from a criminal activity are disguised to conceal their illicit origin, and may encompass three distinct, alternative acts:

1. The conversion or transfer, knowing that such property is the proceeds of crime;
2. The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime;
3. The acquisition, possession or use of property, knowing, at the time of the receipt, that such property is the proceeds of crime.

3.1.2 Processes of Money Laundering

There are three stages of money laundering, explained as follows:

1. Placement

Placement involves the introduction of illegally obtained funds into the financial system, usually through banks. This is achieved through cash deposits, purchase of monetary instruments for cash, currency exchange, purchase of security or insurance contract, check cashing services, the retail economy (through cash purchases), and smuggling of cash between countries.

2. Layering

The next phase is the layering, which usually consists of a series of transactions, through conversions and movements of funds, designed to conceal the origin of the funds. This may involve sending wire transfers to other banks, purchase and sale of investments, financial instruments, insurance contracts, phony investments or trade schemes, and the like.

3. Integration

The last phase is integration, which involves the re-entering of the funds into the legitimate economy. This is accomplished through the purchase of assets, securities/ financial assets, or luxury goods, and investment in real estate or business ventures.

3.2 Terrorist Financing

3.2.1 Definition of Terrorist Financing

The Saudi AML Law Article 1.7 defines criminal activity as: any activity sanctioned by Shari'ah or law including the financing of terrorism, terrorist acts and terrorist organizations. The Bylaw 2.1 of the AML Law Article 2 describes "financing terrorism, terrorists' acts and terrorist organizations include property that comes from legitimate sources".

The United Nations 1999 International Convention for the Suppression of the Financing of Terrorism describes terrorist financing in the following way:

"Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully or willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

a. An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex.

b. Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act."

Saudi Arabia is committed to all relevant United Nations Security Council Resolutions directed towards fighting terrorist financing and has criminalized financing of terrorism, terrorist acts and terrorist

organizations, under Article 2.d of the Saudi AML Law.

SAMA requires strict compliance with UN and FATF directives. If a bank or money exchanger has any reason to believe that individual, commercial establishment or organization is, by any means, directly or indirectly, providing or collecting funds in the knowledge that such funds will be used for illegal purposes, the bank or money exchanger must refrain from entering into transactions and must report the matter to the competent authorities.

3.2.2 Processes of Terrorist Financing

The techniques used to finance terrorism are essentially the same as those used to conceal the sources and uses of money laundering, however, the main differences between the two are that (a) often small amounts are required to commit individual terrorist acts, making it difficult to track the terrorist funds; and (b) terrorists can be funded from legitimately obtained income, making it difficult to identify the stage at which legitimate funds become terrorist funds. Terrorists may derive their income from a variety of sources, often combining both lawful and unlawful funding. The forms of financing can be categorized into the following types:

1. Financial Support

This funding could be in the form of charitable donations, community solicitation and other fund raising initiatives, which may come from entities or individuals.

2. Criminal Activity

This funding is often derived from criminal activities such as money laundering, fraud and other financial crimes.

3. Legitimate Source

This form of funding may originate from legitimate business activity, established to fully or partially fund these illegal activities.

3.3 Typologies

The various techniques or methods used to launder money or finance terrorism are generally referred to as typologies. A typology study is a useful tool to examine in depth a particular issue of concern with a view to providing insight and knowledge on emerging threats and how these might be addressed.

FATF and MENA-FATF regularly issue documents relating to money laundering and terrorist financing typologies, and banks and money exchangers should update themselves with the new typologies applicable to their businesses. The following are examples of typical typologies relating to money laundering and terrorist financing:

- Alternative remittance services (hawala, hundi, etc.): Informal mechanisms based on networks of trust used to remit monies. Often work in parallel with the traditional banking sector but are illegal. Exploited by money launderers and terrorist financiers to move value without detection and to obscure the identity of those controlling funds.
- Structuring (smurfing): A method involving numerous transactions (deposits, withdrawals, transfers), often various people, high volumes of small transactions and sometimes numerous accounts to avoid detection threshold reporting obligations.
- Currency exchanges/ cash conversion: Used to assist with smuggling to another jurisdiction or to exploit low reporting requirements on currency exchange houses to minimize risk of detection, e.g., purchasing of travelers checks to transport value to another jurisdiction.
- Cash couriers/ currency smuggling: Concealed movement of currency across borders to avoid transaction/ cash reporting measures.
- Use of credit cards, checks, etc.: Used as instruments to access funds held in a bank, often in another jurisdiction.
- Purchase of valuable assets (e.g., real estate, vehicles, shares, etc.): Criminal proceeds are invested in high-value negotiable goods to take advantage of reduced reporting requirements to obscure the source of proceeds of crime.
- Use of wire transfers: To electronically transfer funds between banks and often to another jurisdiction to avoid detection and confiscation.
- Trade-based money laundering: Usually involves invoice manipulation and uses trade finance routes and commodities to avoid financial transparency laws and regulations.
- Abuse of non-profit organizations: May be misused to raise funds for terrorist purpose, obscure the source and nature of funds and to distribute terrorist finances.
- Investment in capital markets: To obscure the source of proceeds of crime to purchase negotiable instruments, often exploiting relatively low reporting requirements.
- Mingling (business investment): A key step in money laundering involves combining proceeds of crime with legitimate business monies to obscure the source of funds.
- Use of shell companies/ corporations: A technique to obscure the identity of persons controlling

funds and exploit relatively low reporting requirements.

- Use of offshore businesses, including trust company service providers: To obscure the identity of persons controlling funds and to move monies away from interdiction by domestic authorities.
- Use of nominees, trusts, or third parties, etc: To obscure the identity of persons controlling illicit funds.
- Use of foreign bank accounts: To move funds away from interdiction by domestic authorities and obscure the identity of persons controlling illicit funds.
- Identity fraud/ false identification: Used to obscure identification of those involved in many methods of money laundering and terrorist financing.
- Use professional services (lawyers, accountants, brokers, etc.): To obscure identity of beneficiaries and the source of illicit funds. May also include corrupt professionals who offer 'specialist' money laundering services to criminals.

4. Policies & Standards

4.1 Risk-Based Approach

Banks and money exchangers should adopt a risk-based approach in designing their Anti-Money Laundering (AML) and Combating Terrorist Financing (CTF) programs to ensure that measures used to mitigate money laundering and terrorist financing are commensurate to the risks identified in their organizations. This will allow resources to be allocated in the most efficient ways. Some of the benefits of utilizing risk-based approach in discharging banks' or money exchangers' AML/CTF responsibilities are:

1. Allowing banks and money exchangers to differentiate between customers risk in a particular business by focusing on higher threats, thus improving the outcome of the overall process;
2. While establishing minimum standards, allowing a bank or money exchanger to apply its own approach to systems and controls, and arrangements in particular circumstances, thus allowing more flexibility to adapt as risks evolve; and
3. Helping to create better management of risks and cost effective system.

A risk-based approach will serve to balance the burden placed on individual banks and money exchangers and on their customers with a realistic assessment of the threat of a business being used in connection with money laundering or terrorist financing by focusing effort on areas where it is needed and has most impact.

Banks and money exchangers may face some challenges that they need to consider while implementing the risk-based approach. These challenges should be regarded as offering opportunities to implement a more effective system in the fight against money laundering and terrorist financing activities. Some of these challenges can be summarized as follows:

1. Risk Assessment Methodology: Identifying appropriate information to conduct a sound risk analysis and overall assessment.
2. Judgmental Decisions: Greater needs for more expert staff capable of making sound judgments regarding risk identification and evaluation.
3. Transitional Cost: Cost relating to transition from prescription method to risk based method.
4. Fear Factor: Regulatory response to potential diversity of practice.

The risk-based approach requires certain actions to be taken in assessing the most cost effective and proportionate ways to manage and mitigate the money laundering and terrorist financing risks faced by a bank. These actions are:

1. Identifying the money laundering and terrorist financing risks that are relevant to the bank or money exchanger in order to ensure that the approach is built on sound foundation, and that the risks are well understood.
2. Assessing the identified risks presented by the bank's or money exchanger's particular aspect:
   a. Customers;
   b. Products and services;
   c. Delivery channels;
   d. Geographical area of operation.

The weight given to the above risk categories in assessing the overall risk of potential money laundering and terrorist financing may vary from one bank or money exchanger to another, depending on their respective circumstances. Consequently, each bank or money exchanger will have to make its own determination as to the risk weights.

3. Establishing and implementing controls to mitigate these assessed risks.
4. Monitoring and improving the effective operation of these controls.
5. Recording appropriately what has been done and explaining the reasons and rationale.

4.1.1 Business Risk Assessment

Banks and money exchangers should conduct and document the above business risk assessment. In particular, banks and money exchangers should update this assessment on annual basis, to identify changes in their business environments (such as organizational

structure), its customers, the jurisdictions with which its customers are connected, its products and services, and how it delivers those products and services. Banks and money exchangers must build their AML/CTF programs based on the conclusions and the residual risk identified in the business risk assessment. To achieve an adequate assessment, a bank or money exchanger should establish that it has considered its exposure to money laundering and terrorist financing risk by:

1. Covering all risks posed by money laundering and terrorist financing relating to different businesses within the bank or money exchanger.
2. Considering organizational factors that may increase the level of exposure to the risk of money laundering and terrorist financing, e.g., business volumes and capacity issues.
3. Considering the nature, scale and complexity of its business, the diversity of its operations (including geographical diversity), the volume and size of its transactions, and the degree of risk associated with each area of its operation.
4. Considering the type and nature of its customers and what they do.
5. Considering whether any additional risks are posed by the jurisdictions with which its customers (including intermediaries and introducers) are connected. Factors such as high levels of organized crime, increased vulnerabilities to corruption and inadequate frameworks to prevent and detect money laundering and financing of terrorism will impact the risk posed by relationships connected with such jurisdictions.
6. Considering the characteristics of the products and services that the bank or money exchanger offers and assessing the associated vulnerabilities posed by each product and service, including delivery methods. For example:

a. Products such as current accounts are more vulnerable because they allow payments to be made to and from third parties, including cash transactions.
b. The use of third parties such as group entities, introducers and intermediaries to obtain information about the customer.
c. Pooled relationships with intermediaries are more vulnerable, because of the anonymity provided by the co-mingling of assets or funds belonging to several customers by the intermediary.
d. Conversely, those products that do not permit third party transfers or where redemption is permitted only to an account from which the investment is funded will be less vulnerable.

7. Considering how it establishes and delivers products and services to its customers. For example, risks are likely to be greater whether relationships may be established remotely (non-face-to-face), or may be controlled remotely by the customer (straight-through processing of transactions).
8. Recording, updating and retaining its business risk assessment.

4.2 AML / CTF Compliance Programs

Article 10 of the Saudi AML Law requires financial institutions to develop appropriate AML/CTF programs which should include, as a minimum, the following:

1. Developing and implementing policies, plans, procedures and internal controls, including the appointment of qualified employees at the level of senior management to implement the same.
2. Developing internal accounting and auditing systems to supervise the availability of basic requirements to combat money laundering and terrorist financing.
3. Developing ongoing training programs for specialized employees to keep them informed about new technologies in combating money laundering and to upgrade their skills to identify such operations, their patterns and the method of combating them.

Therefore, banks and money exchangers should prepare adequate AML/CTF Compliance Program, basically covering the following elements:

1. Setting out in detail the above elements and the banks' or money exchangers' plans and strategies for ensuring compliance with its written policies and procedures to effectively cover AML/CTF requirements.
2. Including planned reviews and self-assessment processes to monitor effectiveness of AML/CTF controls.
3. Detailing assigned responsibilities and specific actions to be taken during the year in addition to any pending corrective actions based on audits and assessment reviews.
4. Including appropriate staff awareness and training efforts for the year.
5. The program should be prepared and reviewed on an annually basis, to reflect ongoing trends and risks of money laundering and terrorist financing in order to ensure its effectiveness.

The program should stipulate appropriately what has been done and why, in regards to the risk-based approach. Therefore, each bank or money exchanger

should tailor the program policies and procedures for the AML/CTF to capture the following:

1. How the bank or money exchanger assesses the threats and risks of being used in connection with money laundering or terrorist financing.
2. How the bank or money exchanger implements the appropriate system and procedures, including due diligence requirements in the light of its risk assessment.
3. How the bank or money exchanger monitors and improves the effectiveness of its system and procedures.
4. Reporting process to senior management on the operation of its control procedures.

4.3 Know Your Customer Standards (KYC)

4.3.1 Customer Due Diligence/ Know Your Customer

Customer Due Diligence/ Know Your Customer is intended to enable a bank or money exchanger to form a reasonable view that it knows the true identity of each customer and, with an appropriate degree of confidence, knows the types of business and transactions the customer is likely to undertake. Bank's and money exchanger's procedures should include measures to:

1. Identify and verify the identity of each customer on a timely basis;
2. Take reasonable risk-based measures to identify and verify the identity of any beneficial owner;
3. Obtain appropriate additional information to understand the customer's circumstances and business, including the expected nature and level of transactions.

The starting point is for a bank or money exchanger to assess the risks that the customer may pose taking into consideration any appropriate risk variables before making a final determination. Banks and money exchangers should determine the due diligence requirements appropriate to each customer, including the following:

1. A standard level of due diligence, to be applied to all customers.
2. The standard level being reduced in recognized lower risk scenarios, such as:

a. Publicly listed companies subject to regulatory disclosure requirements.
b. Other banks or financial institutions (domestic or foreign) subject to an AML/CTF regime consistent with the FATF Recommendations.
c. Individuals whose main source of funds is derived from salary, pension or social benefits from an identified and appropriate source and where transactions are commensurate with the source of funds.
d. Transactions involving small amounts or particular types of transactions.

3. Simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply.
4. An increased level of due diligence with respect of those customers that are determined to be of higher risk. This may be the result of the customer's business activity, ownership structure, anticipated or actual volume or types of transactions, including those transactions involving higher risk countries or defined by the applicable law or regulation as posing higher risk, such as correspondent banking relationships and politically exposed persons.

When designing and implementing controls to manage and mitigate the assessed risks, under the risk-based approach, banks and money exchangers should include the following steps:

1. Managing and mitigating the identified and assessed risks, the bank or money exchanger will develop measures to verify the customer's identify; collect additional KYC information about the customer and monitor the customer's transactions.
2. Establishing control procedures to:

a. Introducing a customer identification program that varies the procedure in respect of customer appropriate to their assessed money laundering and terrorist financing risks.
b. Requiring the quality of evidence, documentary/ electronic/ third party assurance to be of certain standard.
c. Obtaining additional customer information, where this is appropriate to their assessed money laundering and terrorist financing risks.
d. Monitoring customer transactions/ activities.

3. Establishing a customer identification program that is graduated to reflect risk, involving:

a. A standard information database to be held in respect of all customers.
b. A standard verification requirement for all customers.
c. More extensive due diligence on customer acceptance for higher risk customers.
d. Limited identity verification measures for specific lower risk customer/ product combination.
e. An approach to monitor customer activity and transactions that reflect the risk assessed.

4. Understanding of where the customer's funds and wealth come from for customers assessed as carrying a higher risk.
5. Developing monitoring guidelines for higher risk customers versus lower risk customers.

4.3.2 Customer Identification Process

Article 4 of the Saudi AML Law requires financial institutions not to carry out any financial, commercial or similar operations under anonymous or fictitious names. SAMA also prohibits banks from opening numbered accounts. Banks and money exchangers must verify the identity of the client, on the basis of official documents, at the start of dealing with such client or upon concluding commercial transactions therewith in person or in proxy. Banks and money exchangers must further verify the official documents of juristic person that indicate the name of the entity, its address, name of its owners, managing directors, and other relevant data.

Banks and money exchangers should apply the following rules, as a minimum, for appropriate customer identification:

1. Establish valid identification by reference to proper, acceptable official documents in accordance with SAMA Account Opening Rules.
2. At the outset of the relationship or account, obtain a copy of the customer identification document and verify them against the original document.
3. Obtain SAMA approval for opening accounts or establishing relationships for any non-residents, except for GCC citizens.
4. Not to establish accounts or relationships for any non face-to-face customers (refer to SAMA Account Opening Rules), and subject all accounts to interview and identity verification.
5. Identification is not limited to customers having accounts with the bank; it should also include those who benefit from other banking/ financial services, such as credit cards, express remittances, large transfers/ transactions, foreign exchange transactions and safe deposit boxes, and should cover owners, authorized signers, powers-of-attorney, directors, trustees and partners.
6. Establish a systematic procedure for identifying customers and not to set up a relationship or process a transaction until the personal or commercial valid identity of the individual or legal entity has been established and satisfactorily verified.
7. Obtain customer personal information, such as name, address, signature, contact telephone numbers, occupation, source of funds/ income, and other information, depending on the type of customer, as stated in the SAMA Account Opening Rules.
8. Ask the customer to provide information about any existing bank accounts or relationships with other local banks, which should be followed up if suspicions arise.
9. Conduct further due diligence if there are doubts about the integrity or adequacy of previously obtained customer identification data, in which case re-verify the identity of the customer and re-assess the relationship.
10. Not to accept any transactions from walk-in customers, with the exception of permissible transactions as stated in the SAMA Account Opening Rules.

11. No new account, business relationship or transaction should be accepted, and any existing account, business relationship or transaction should be frozen, where:

a. Identity of the customer cannot be verified;
b. Identity of the beneficial owner is not known; and/ or
c. There is a failure to obtain information on the purpose and intended nature of the business relationship.

- In case banks or money exchangers identify any of the above cases, they should immediately report them to the SAFIU with a copy to SAMA.

4.3.3 Beneficial Owners (Natural & Legal)

Banks and money exchangers should establish the beneficial ownership for all accounts and relationships and should conduct due diligence on all principal beneficial owners identified in accordance with the following principles:

1. Natural Persons

When the account or relationship is in the name of an individual, the bank or money exchanger should determine whether the client is acting on his/her own behalf. If doubt exists, the bank will establish the capacity in which and on whose behalf the customer is acting. Identity should be established to the bank's or money exchanger's satisfaction by reference to official identity documents. Banks and money exchangers should also ensure that any person purporting to act on behalf of the customer, is so authorized, and identify and verify the identity of that person.

2. Legal Persons / Companies

Where the customer is a legal person/ company, the bank or money exchanger should understand the structure of the company sufficiently to determine the

provider of funds, principal owners of the shares and those who ultimately own or have control over the assets, e.g., the directors and those with the power to give direction to the directors of the company.

With regards to a joint stock company, the bank or money exchanger should establish the identity of all shareholders who own 5% and more of the company's shares. Banks and money exchangers should obtain documentary evidence of the legal entity and existence along with the identity of the beneficial owners including the actual natural persons owning or controlling the entity.

In all the above cases, if a customer states that he/she is acting on his/her own, then a declaration to this effect, whether as a separate document or as a part of the account opening agreement, should be obtained from the customer, as follows:

a. For new customers: at the time of opening an account, establishing a relationship or conducting a significant transaction;

b. For existing customers: (i) whenever there is a suspicion that the account, relationship or transaction is being used for a different or illegal purpose, thus requiring more information from the customer; or (ii) during the mandatory periodic updation of customer information, as per SAMA Account Opening Rules.

4.3.4 Customer & Transaction Profiling

Banks and money exchangers should have a process in place to capture sufficient information about customers, and their anticipated use of their products and services, that will allow to develop a customer profile of expected activity to provide a basis for recognizing unusual and higher risk activities and transactions, which may indicate money laundering or terrorist financing. The information should be obtained at the establishment of a relationship or opening of an account and prepared for all types of relationships, including accounts and credit cards.

The extent and nature of the information details depend on the different types of customers (individual, corporation, etc.) and the different levels of risk resulting from the customer's relationship with the bank or money exchanger. Higher risk relationships, accounts and transactions will require greater scrutiny than lower risk ones.

The information should be kept up-to-date and monitoring of activity and transactions should be undertaken throughout the course of the relationship to ensure that the activity or transaction being conducted is consistent with the bank's or money exchanger's knowledge of the customer. Customer Profiles and Transaction Profiles should be reviewed and updated at least annually, or whenever there is a suspicion of illegal activities.

1. Customer Profile

A customer profile is a means of collecting detailed information on a customer or an account/ relationship. Depending on the type of the customer, profiling will include basic information such as owners' names (including beneficial owners), partners, shareholders (except for minor shareholders of a joint stock company, holding less than 5%), authorized signers, power of attorney holders, etc.; customers' addresses including phone numbers, postal and street/ location address, e-mail, fax, etc.; purpose and the intended nature of business relationship, information of the business activities, financial information, capital amount, source of funds, source of wealth, branches, countries and products dealing in, etc. At the discretion of the bank or money exchanger, this could be an automated process.

2. Transaction Profile

A transaction profile should be prepared to capture the number of transactions expected to be used by a customer, and the value of transactions for an average month, for each product and service. Banks and money exchangers should develop a system using specialized software to provide automatic preparation of transaction profiles and detect unusual patterns of transactions and trends that may indicate suspicious activities that are not consistent with initial assessments or expectations. All efforts should be made to establish the source of funds to the bank's or money exchanger's satisfaction and the customer and transaction profiling methodology should assist in establishing source of funds.

Transaction profile is not required for employed/ payroll, pension and fixed-income individual accounts or relationships, whose source of funds and usage of account can be determined, provided the account or relationship is used for the intended purpose. However, for accounts and relationships used for business purpose and for high-risk accounts, an appropriate transaction profile based on risk assessment, should be prepared to include all types of products and services expected to be used by the customer in the account, during the period of a month, the number of expected transactions, and their estimated monetary value, especially for high-risk products/ services such as cash, transfers, etc. The transaction profile should be reviewed and updated on an annual basis, to establish continued consistency between the profile and the

actual transactions. Major inconsistencies should be investigated.

Banks and money exchangers may prepare a transaction profile on the basis of generic expected activity and transactions for certain types of products and services, however, for more complex products or services a tailored transaction profile will be necessary.

4.3.5 Name Checking of Designated Persons

Saudi Arabia is committed to all relevant United Nations Security Council Resolutions directed towards fighting terrorist financing and has criminalized financing of terrorism, terrorist acts and terrorist organizations, under Article 2 of the Saudi AML Law and Bylaws. The UN, through its Security Council Resolutions (UNSCR 1267 of 1999 and successor resolutions), issues a listing of "designated persons", that are subject to certain sanction measures. Based on Saudi competent authorities' instructions, SAMA also notifies banks and money exchangers the names of "designated persons" and requires banks and money exchangers to implement the Saudi laws and the UN resolutions in this regard, including freezing of assets of individuals and entities who have been categorized as designated persons by UN or SAMA.

The following measures should be implemented by all banks and money exchangers:

1. Put in place an effective process to check all their customers' names (individuals, entities, beneficial owners, etc.) against the names that have been categorized as “designated persons” by SAMA and the UN, prior to opening account, establishing a relationship or conducting a transaction, especially for transfers in which case both the remitter's and the beneficiary's names should be checked.
2. In case a customer has been identified as being a “designated person”, immediately freeze the account, relationship or the transaction and notify SAFIU and SAMA, giving full details of the account or transaction. The account or transaction should continue to be frozen until SAMA provides its direction to the bank or money exchanger.
3. For the purpose of continuous monitoring and suspicious should be reported to SAMA as per SAMA instructions.
4. Banks and money exchangers should also obtain the UN sanctions list from the following website:
http://www.un.org/sc/committees/1267/consolist.shtml
5. Ensure to continuously check the UN List and keep it updated in their records.
6. Observe sanctions lists issued by other countries, and check all transactions and transfers against these lists, to avoid potential conflicts when conducting business with other countries' banks and entities, and to prevent the customers' transactions or transfers from being blocked.
7. In case an asset (account, relationship, transaction, etc.) has to be unfrozen because the designated person has been de-listed (removed from the sanctions list) by the UNSC, notify SAMA for approval to release the frozen assets of the customer. For names previously frozen at SAMA's instructions, SAMA will provide the bank or money exchanger with instructions to release the frozen assets.

4.4 Customer Risk Assessment

Every relationship, account or transaction should be risk assessed from a money laundering and terrorist financing perspective. The complexity of the risk assessment process should be determined according to factors established by the business risk assessment.

The basis for the customer risk assessment should include factors such as:

1. High-risk jurisdictions/ countries, as defined by UN or FATF's NCCTs, as explained in Rule 5.2;
2. High-risk businesses or customers, as explained in Rule 4.5;
3. High-risk products and services the customer may be dealing in, as explained in Rule 5.1;
4. The delivery method, such as the way the relationship is set up (directly/ face-to-face or indirectly) or the manner the products/ services are delivered to customers (e.g., internet, phone banking, etc.);
5. Other risk variables should also be considered when risk assessing a customer, as explained in Rule 5.3.

Customers to whom one of the above high-risk categories applies should be rated as high risk. However, the rating could be changed to a lower risk, provided the customer profiling is considered satisfactory and the rating change is justified and approved by a senior management. Such accounts classified as high risk should be subject to enhanced due diligence, closer monitoring and their risk statuses reviewed and updated at least on annual basis.

4.5 Customer Risks

Customer risks are those that a particular customer or a category of customers may create due to their activities or behavior. Determining the potential money

laundering or terrorist financing risks, to the extent that such risk can be identified, posed by a customer, or category of customers, is critical to the development of an overall risk-based framework. Based on its own criteria, a bank or money exchanger should determine whether a particular customer poses a higher risk and the potential impact of any mitigating factors on that assessment. Application of risk variables may mitigate or aggravate the risk assessment.

The types of customers or relationships, and the potential risks they may pose, are described below:

4.5.1 Individual Personal Accounts

These are accounts of individuals who open personal accounts for non-commercial and personal use. This category includes mainly employed/ payroll, fixed-income, pensioners, and self-employed individuals. Such personal accounts normally constitute a mass consumer business for many banks and generally do not involve close relationship management by a specific relationship manager. The sheer number of these accounts and the scale of transactions, usually small tickets, make the processes of monitoring demanding for banks.

While the AML risks for employed/ payroll individuals, pensioners and fixed income may be regarded as low, due to the fact that their sources of income can reasonably be established and are generally of smaller value, banks should be alert and exercise more due diligence for individuals who are self-employed. For these customers, it is difficult to reasonably determine their sources of income due to lack of any formal/ official supporting documents. In addition, self-employed individuals are relatively of higher risk due to their free-lancing activities. They may act as agents, on behalf of others, in real estate or other activities and receive a commission in return. However, they sometimes use their accounts as a transitory depository for their customers' funds, relating to a deal, pending final disposal. This poses additional AML risks for these accounts.

The following rules should apply as minimum standards for accounts of individual customers:

1. Employed/ Payroll, Pensioners & Fixed Income Individuals

These are individuals who are employed/ on payroll, on pension or with a regular fixed income and whose main source of income is derived from salary, pension, social benefits and the like, from an identified and appropriate source and whose transactions commensurate with the funds. Such customers are considered as low-risk and the following basic information is sufficient to constitute customer profile:

1. Obtaining proper and valid identification of the customer as stated in SAMA Account Opening Rules.
2. Ensuring customer's identification shows ID number, name, nationality and date/ place of birth.
3. Ensuring customer is not a PEP; otherwise extra due diligence is required as per Rule 4.5.4.
4. Obtaining address and telephone/ mobile number. Also fax number and/ or e-mail address, if available.
5. Account is used for the purpose intended and not for commercial purpose; otherwise it should be treated as commercial account and additional information on the business activity obtained.
6. Taking reasonable measures to determine source of funds/ income; for example, using any one of the following means:

a. Employment identification card for government, public and private sectors employees;
b. Payroll slip, pension slip (for pensioners), electronic or paper salary certificate, or letter from employer;
c. Copy of statement of another bank if salary is transferred to that bank;
d. If salary is directly transferred to the same bank (individually or through payroll system) no need of further evidence;
e. Salary transferred through SARIE, indicating thereon as payroll/ salary;
f. Customer's self-declaration indicating his/her employer's name, salary/income and position; or
g. Any other reasonable means satisfactory to the bank and money exchanger;
h. However, in case of doubt, an official documentary confirmation of the customer's salary/ income should be obtained.

7. Conducting extra due diligence if a bank or money exchangers becomes aware that another bank or money exchanger has refused to deal with a particular customer on AML/ CTF grounds.

2. Self-Employed Individuals (Free Dealers, Agents, etc.)

For self-employed, in addition to above requirements, a self-declaration signed by the customer confirming his/her income, source of funds and business activity should be obtained. In case of doubt, efforts should be made to determine the source of funds, and the type of activity the customer is engaged in, as these individuals are relatively of higher risk due to their free-lancing activities.

3. High Net Worth Individuals

For High Net Worth Individuals, who are considered as high-risk due to the size and nature of their activities and transactions, in addition to above, an enhanced due diligence is required and a detailed customer and transaction profiles should be prepared to also include the customer's source of funds and source of wealth, and anticipated account activity.

In all the above cases, where any doubt or suspicion arises as to the identity, address or source of income/ funds or any other information of a customer during the course of the relationship, the bank or money exchanger should re-verify all the information by reasonable means and reassess the relationship.

4.5.2 Walk-In Customers

A walk-in or occasional customer is one who conducts a transaction with a bank or money exchanger but does not maintain an account or any type of relationship with the bank or money exchanger. These include residents as well as visitors on a temporary visa/ residence. As banks and money exchangers do not have adequate background information about these individuals, banks or money exchangers may be at risk if they conduct financial transactions for them. Therefore, as per SAMA Account Opening Rules, banks and money exchangers should not accept any transactions (in particular, all types of funds transfers) from walk-in customers unless they fall under the following categories:

1. Resident Non-Account Holders: Banks and money exchangers are allowed to accept settlement of bills of services and public utilities (electricity, water, telephone) and payments to state authorities and government dues (traffic, passports, etc.).
2. Visitors (Foreign Pilgrims, Tourists, Businessmen & Diplomats): Banks and money exchangers are allowed to accept settlement of bills of any services and public utilities, payments to state authorities and government dues, and encashment of travelers checks, banks checks, etc.
3. Visitors on a temporary visa/ residence, in addition, are permitted to exchange foreign currency bank notes up to SAR 7.500 per transaction per day, within the validity of the visa, but not exceeding the equivalent of SAR 60,000 in total. Amounts in excess of SAR 60,000 or equivalent should be reported to FIU with a copy to SAMA.
4. For the allowed transactions, a copy of the passport should be obtained including the page evidencing the visa. Other details such as home country address, contact in Saudi Arabia and signature should be obtained.
5. In case of suspicion, the bank or money exchanger should report the transaction to FIU with a copy to SAMA, enclosing copies the passport and the transaction, and customer details.
6. Banks and money exchangers should comply with SAMA Account Opening Rules relating to walk-in customers requirements.
7. Incoming transfers and checks may be accepted for walk-in customers, in the following cases:

a. If the transfer or check is made from an account with the bank to a beneficiary (natural or legal) on any branch of the same bank, the transfer or check may be paid in cash to the beneficiary or his legal proxy.

b. If the transfer or check is from a local bank to another local bank within Saudi Arabia, it shall be required to be from the account of transferor to the account of the transferee.

c. If the transfer is received from outside Saudi Arabia in the personal name of the beneficiary, it should be paid through an account only, which may be opened by the customer upon receipt of the transfer, subject to SAMA Account Opening Rules.

4.5.3 Commercial Entities Accounts

These are accounts opened by legal entities for the purpose of conducting commercial activities. Commercial entities include small enterprises such as sole proprietorships and establishments to large companies and corporations. Banks should maintain a customer profile for each commercial relationship, which should cover business and financial related information, source of funds, purpose of account, deposits and banking needs. The extent of details and nature of the information to be requested will vary in relation to the size, structure, risk and type of commercial activities of the business entities, as described below.

1. Small Business Entities

Small businesses are defined as those commercial entities with lower turnover of transactions (e.g., less than SAR one million per annum). These entities range from sole traders/ proprietorships, small establishments and small family concerns to partnerships, professional firms and small private companies.

2. Corporations & Large Business Entities

These are incorporated legal bodies such as corporations, public companies, private companies, partnerships, etc. large businesses are defined as those with significant turnover (e.g., SAR one million per annum and above), whether they are sole traders/ proprietorships, small establishments, small family

businesses, partnerships, professional firms or small private companies.

3. General Requirements

For all commercial entities, the principal guidance is to look behind the entity to identify those who have control over the business and entity's assets. As a commercial entity can be used as a front to provide cover for money laundering activities, especially cash-intensive businesses, banks should ensure they obtain adequate information about the entity's business/ trading activities and the expected use of the bank's products and services.

Banks should obtain the following information for all commercial entities at the time of opening account/ relationship for applying the customer due diligence in accordance with the risk assessment of the customer:

1. Valid and original identification documents as required in the SAMA Account Opening Rules.
2. Large business entities and corporations: The financial structure and nature of the business entity and its annual financial statements.
3. Small business entities: An assessment of the business entity's financial statements, turnover and revenue/ income.
4. Names of beneficial owners, partners, managers, powers-of-attorney, authorized signatories, shareholders (except for minor shareholders of joint stock companies, owning less than 5%), etc., as applicable.
5. Description of customer's line of business and business activities.
6. Types and nature of products and services the entity may be dealing in.
7. List of significant suppliers, customers and their geographical locations, as applicable.
8. Description of geographical coverage where the business entity carries out its activities, as applicable.
9. List and locations of branches and outlets, if any.
10. Purpose and intended nature of the business relationship/ account.
11. For large business entities and corporations, bank employees should pay site visits to acquaint themselves with the nature of business activities. All customer visits should be properly documented and the records maintained.
12. For small business entities, where feasible/ practical, bank employees may pay site visits to acquaint themselves with the nature of business activities, and the customer visits documented and records maintained.
13. Individual accounts used for commercial purposes should be treated as small business entities in terms of profiling.
14. Banks should seek information on the customer's relationship with other banks and seek information from these banks if suspicions arise about their dealings with the customer. Extra due diligence is needed, if the bank has reason to believe that other bank(s) rejected this relationship.
15. Banks should collect direct or indirect information about the business entity from any known or available sources.
16. Banks should ascertain the accuracy of the information provided by the business entity when opening an account, e.g., ascertaining the business address, etc.
17. Banks should use their best efforts, through customer profiling and transaction profiling, to ascertain the sources of all deposits, paying particular attention to cash deposits more than SAR 60,000 or equivalent.

4.5.4 Politically Exposed Persons

Individuals who are or have been entrusted with prominent public functions, for example heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve reputation risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories.

The political influence and power of PEPs could give rise to misuse of the positions to illegally amass wealth, the proceeds of which are often transferred and concealed under the names of relatives or close associates. Banks and money exchangers should apply the following standards, as a minimum:

1. Comply with all the SAMA Account Opening Rules relating to opening accounts for individuals.
2. Have policies in place to identify and categorize PEPs and related individuals for closer scrutiny. Identification of PEPs should include the existing & new customers as well as the beneficial owners.
3. To put in place appropriate risk management systems to determine whether a potential customer, existing customer or the beneficial owner is a politically exposed person.
4. Determine the source of funds, source of wealth and beneficial owners for all PEPs.

5. Where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a PEP, Banks and money exchangers should be required to obtain senior management approval to continue the business relationship.
6. Categorize all such accounts and relationships as High Risk for extra due diligence, and should require approval of a General Manager, Managing Director, or CEO
7. Where Banks and money exchangers are in a business relationship with PEP, they should be required to conduct enhanced ongoing monitoring on that relationship.
8. Accounts of PEPs and related individuals should be reviewed on an annual basis and must be approved by General Manager, Managing Director, or CEO for retaining the relationship/ account.

4.5.5 Private Banking Customers

Private Banking is the term used for preferential banking services provided to high net-worth customers by a bank. Private Banking normally caters for very wealthy, powerful and influential individuals, including PEPs. These customers are assigned a private banker or relationship manager to act as a liaison between the customer and the bank, and to facilitate the customer's use of a wide range of financial services and products that usually involve complex transactions and large sums of money, including investment services, trust vehicles and wealth management. These clients demand a high level of confidentiality. As a result, Private Banking is exposed to greater money laundering vulnerability and banks should apply enhanced due diligence to such operations.

Banks should have clear customer acceptance policies for handling Private Banking customers, recognizing the money laundering risks inherent in this category of accounts. Banks should endeavor to accept only those clients whose source of wealth and funds can reasonably be established to be legitimate. The following rules should apply as a minimum:

1. Establish the identity of the clients and all the beneficial owners.
2. Obtain proper and valid identification documents as per SAMA Account Opening Rules.
3. If there are any intermediaries involved, extra due diligence should be required to cover the intermediary as well.
4. The profiling process for a Private Banking account should include obtaining and recording the following minimum information:

a. Purpose and reasons for opening the account.
b. Anticipated account activity.
c. Source of wealth (description of customer's commercial/ economic activities which have generated the net worth) and estimated net worth of the customer.
d. Source of funds (description of the origin and the means of transfer for monies that are expected for the account opening and subsequent large transfers).
e. References or other sources to corroborate reputation, where available.

5. Bank officers handling the account should personally meet the prospect.
6. Anonymous, fictitious name, coded or numbered accounts should not be allowed.
7. All account opening should be subject to senior management approvals in addition to the relationship manager.
8. If the Private Banking customer is also a PEP, then the requirements for PEP should apply, as per Rule 4.5.4 above.
9. All Private Banking accounts should be subject to close monitoring by a senior officer, covering unusual or suspicious activities.
10. Large cash transactions in excess of SAR 60,000 or equivalent should be scrutinized more closely.

4.5.6 Charity & Non-Profit Organizations

Charity or non-profit organization refers to a legal entity or organization that primarily engages in raising/ collecting donations and/ or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying our of other types of benevolent deeds.

Banks and money exchangers should have in place policies, procedures and controls to comply with SAMA Account Opening Rules requirements regarding the handling of accounts and transactions for charity organizations. When dealing with accounts, relationship or transactions of any charity organizations, banks and money exchangers should observe the following:

1. Not to open account or set up a relationship for any charity organization (local or international) without SAMA's prior written approval and without official registration by the relevant government ministry or authority, specifying the purpose and activity.

2. To strictly comply with the SAMA Account Opening Rules relating to specific requirements and restrictions when dealing with charity organization accounts.
3. Not to open accounts in the names of chairmen or managers of charities for managing charity funds.
4. To classify charity organization accounts as High Risk and exercise extra due diligence.
5. Not to accept any transfers or payments (incoming or outgoing) of any donations or contributions into or out of Saudi Arabia except with the prior written approval from competent authorities through SAMA. This is regardless of whether the funds originate from natural persons, legal entities, organizations and multi-national organizations, independent or public charities.
6. Not to enter into any transaction, knowing that the funds or property involved are owned or controlled by criminals or criminal organizations, or that a transaction is linked to, or likely to be used in criminal activity, and should report such case to FIU with a copy to SAMA.
7. To freeze any transaction and immediately report the matter to FIU with a copy to SAMA, in case of reasonable grounds to suspect that that an individual or entity is, by any means, directly or indirectly, providing or collecting funds in the knowledge that such funds will be used for illegal purposes,
8. To design their fund transfer systems (for incoming and outgoing transfers) to be capable of detecting customer names against designated persons of UN or SAMA, prior to processing the transaction for the purpose taking appropriate action.
9. Not to allow any of their customers to transfer funds in favor of any known charity organizations outside the Kingdom of Saudi Arabia.
10. In compliance with the FATF SR 7 on anti-terrorist financing, to provide the remitter's name, address and account number for all outgoing transfers.

4.5.7 Trustees, Nominees & Intermediaries Accounts

1. Trustee & Nominee Accounts

These accounts are normally used to provide an extra layer of security to protect the confidentiality of legitimate customers. However, these structures can also be misused to circumvent customer identification procedures for the purpose of money laundering. Therefore, it is essential that the true relationship is understood. Banks should have in place procedures to ensure the following:

1. Establish whether the customer is taking the name of another customer, acting as a "front", or acting on behalf of another person as trustee or nominee.
2. If the customer is acting on behalf of another person, ensure that he/she has the authorization to do so, and identify and verify the identity of that person.
3. Where the customer is a trustee, understand the structure of the trust sufficiently to determine the provider of funds, those who have control over the funds (trustees) and any persons or entities who have the power to remove the trustees.
4. Make a reasonable judgment as to the need for further due diligence and obtain appropriate evidence of formation and existence along with identity of the settlers/ grantors, trustees or persons exercising effective control over the trust and the principal beneficiaries.
5. Exercise special care in initiating business transactions with companies that have nominee shareholders or shares in bearer form; obtain satisfactory evidence of the identity of beneficial owners of all such companies; and monitor the identity of material beneficial owners and hold such bearer shares in their custody to prevent the shares changing hands to unknown parties without the bank's knowledge.

2. Intermediaries' Clients Accounts

These are accounts opened by professional intermediaries (such as lawyers, , independent financial advisors, etc.) who act as professional asset managers on behalf of other clients (individuals or corporations). These accounts could be pooled accounts managed by professional intermediaries on behalf of entities such as, pension funds, or managed by lawyers or that represent funds held on deposit or in escrow for a range of clients.

These types of accounts are potentially vulnerable to the layering of laundered funds subsequent to the placement phase. Specific vulnerable activities include:

1. Intentional or unwitting facilitation of a customer's money laundering scheme and the activities of rogue employees who undertake illegal activities.
2. Wash sales or other fictitious trading schemes to transfer money.
3. Transfer of value between parties through the sale of shares in small, illiquid issues at artificially arranged prices, without regard to fair market value.

Banks should have procedures in place and ensure the following:

1. The intermediary is registered and regulated.
2. Perform due diligence on the intermediary itself and the account should be classified as High Risk.

3. Verify and be satisfied with the intermediary's reputation and integrity.
4. Establish that the intermediary has in place a sound documented due diligence process, including KYC and identification requirements, and activity monitoring for its customers and beneficial owners, which is satisfactory to the bank.
5. Establish that the intermediary has in place written policies, procedures and internal controls to address and the risks of its business being used as a vehicle for illegal activities, including the establishment of management controls to prevent the involvement of the intermediary in money laundering and terrorist financing schemes.
6. When a bank has knowledge or reason to believe that a client account opened by a professional intermediary is on behalf of a single client, that client must be identified.
7. Where funds held by the intermediary are not co-mingled at the bank, but where there are "sub-accounts" which can be attributable to each beneficial owner, all beneficial owners of the account held by the intermediary must be identified.
8. Where the funds are co-mingled, the bank should look through to the beneficial owners, unless the bank can establish that the intermediary is subject to the same regulatory and money laundering legislation and procedures, and in particular is subject to the same due diligence standards in respect of its client base as the bank.
9. Banks should accept such accounts only on the condition that they are able to establish that the intermediary has engaged in a sound due diligence process and has the systems and controls to allocate the assets in the pooled accounts to the relevant beneficiaries.
10. In the absence of the above requirements, then the bank should not permit the intermediary to open an account.

4.5.8 Insurance Companies Accounts

These are accounts opened by insurance companies who offer insurance products directly to their customers or through agents. The insurance sector is potentially at risk and can provide the opportunity for misuse, knowingly or unknowingly, for money laundering and financing of terrorism although its vulnerability is not regarded to be as high as for banking sector.

As insurance companies deal with their own customers, banks should exercise extra due diligence on these accounts, and, in addition to SAMA Account Opening Rules requirements, banks should have procedures and controls in place to implement the following:

1. Dealing only with registered and regulated insurance companies.
2. Performing extra due diligence on the insurance companies and classifying the accounts as High Risk.
3. Verifying and being satisfied with the insurance company's reputation and integrity.
4. Establishing that the insurance company has in place a sound documented due diligence process, including KYC and identification requirements, and activity monitoring for its customers, that is satisfactory to the bank.
5. Establishing that the insurance company has in place written policies, procedures and internal controls to address the risks of its business being used as a vehicle for illegal activities, including the establishment of management controls to prevent the involvement of the insurance company in money laundering and terrorist financing schemes.
6. In the absence of the above requirements, then the bank should not permit the insurance company to open an account.

4.5.9 Introduced & Referred Businesses

It is customary for banks to rely on the procedures undertaken by other banks or introducers (person, entity or a professional intermediary) when business is being referred. In doing so, banks risk placing excessive reliance on the due diligence procedures that they expect the introducers to have performed. Relying on due diligence conducted by an introducer, however reputable, does not in any way remove the ultimate responsibility of the recipient bank to know its customers and their business. In particular, banks should not rely on introducers that are subject to weaker standards than those governing the banks' own KYC procedures or that are unwilling to share copies of due diligence documentation.

1. Introduced Business

Banks that use introducers should carefully assess whether the introducers are reputable and are exercising the necessary due diligence in accordance with the acceptable KYC standards. The ultimate responsibility for knowing customers always lies with the bank. Banks should use the following criteria to determine whether an introducer can be relied upon:

The customer due diligence procedures of the introducer should be as strong as those which the bank would have conducted itself for the customer. The

banks should also ensure that the required due diligence includes that of the introducer.

1. The bank must satisfy itself as to the reliability of the systems put in place by the introducer to verify the identity of the customer.
2. The bank must reach agreement with the introducer that it will be permitted to verify the due diligence undertaken by the introducer at any stage.
3. Banks should obtain and carefully review all relevant identification data and other documentation pertaining to the customer and the introducer.
4. The decision to open the account should not be solely based on the introducer's reputation; rather all KYC process should take place for the introducer as well as the account owner.

2. Referred Business

This means a relationship referred by one branch to another, within one bank or externally from other banks inside or outside the country. In such cases, the branch/bank accepting the relationship should conduct normal KYC process in addition to the referrals received. Such due diligence should include full verification of the customer's identification and information, including beneficial owners, comprising the following steps:

1. Banks must take all reasonable steps to recognize suspicious transactions. This should require banks to have a reasonable understanding of the normal character of the customer's business, and having a reasonable understanding of the commercial basis of the transaction to be undertaken or service to be provided.
2. Where a foreign branch, subsidiary or associate refers business to a bank in Saudi Arabia, in addition to the above procedures, the bank should seek the full business rationale for the referral, and determine whether it complies with Saudi Arabian laws and regulations.
3. If the referred branch determines that it has insufficient information to enable it to accept the referral, the business must be declined and the referring branch, subsidiary or associate notified.

4.5.10 Correspondent Banking Relationships

Correspondent banking is the provision of banking services by one bank (correspondent bank) to another bank (respondent bank) by means of a correspondent account. Through the correspondent account, respondent banks can conduct transactions for themselves and for their customers in jurisdiction where they have no physical presence. These services include cash management, international wire transfers of funds, check collection, and foreign exchange services, which usually involve large amounts and numerous transactions.

Correspondent banking, by its nature, creates an indirect relationship whereby the correspondent bank carries out financial transactions for the respondent bank on behalf of its customers (individuals or entities) without having enough information about the customers or by relying on the information and KYC due diligence provided by the respondent bank. This anomaly, coupled with the fact that the respondent bank may have inadequate AML/CTF standards, poses additional risks in this relationship.

Therefore, banks and money exchangers who maintain correspondent banking relationships should take strict measures to prevent the use of their correspondent accounts for money laundering, terrorist financing and other illegal purposes. Prior to opening any account, banks should fully understand and appropriately document full details of the respondent bank's management and nature of the business. In addition to requirements relating to correspondent banks relationship as stipulated in SAMA Account Opening Rules, the following requirements should apply as minimum standards for opening and maintaining correspondent bank accounts:

1. Banks should not open a correspondent account for or deal with a Shell Bank.
2. Correspondent bank accounts should be opened after senior management approval and after completing and satisfying the KYC due diligence process.
3. Banks should obtain SAMA's approval for opening correspondent bank account in Saudi Riyal.
4. Third parties are prohibited from operating correspondent bank accounts, and local cash deposits should not be allowed. This arrangement, also known as "Payable-Through Accounts" should not be accepted.
5. The correspondent bank should not be under sanctions by the UN or Saudi Arabia.
6. Banks should also determine from publicly available information (e.g., internet) whether the correspondent bank has been subject to any money laundering or terrorist financing investigations or regulatory action.
7. Banks should obtain certification of AML/CTF compliance for all correspondent relationships, which should include the following information:

a. The location, major business activities, and management.

b. That they are under jurisdiction of their central bank or a similar monitory authority and are committed to the FATF recommendations.
c. That they are governed by and committed to AML/CTF and KYC policies and procedures.
d. That they have procedures in place for reporting suspicious transactions.
e. That they are not dealing with any Shell Bank.
f. Any other pertinent information that can reassure the bank that sufficient focus is being directed to combating money laundering and terrorist financing.
g. The certification should be either renewed or confirmed by the correspondent bank every three years.

4.6 Monitoring Customer Activity

4.6.1 Monitoring Process

Article 6 of the Saudi AML Law requires all financial institutions to have in place internal precautionary and supervisory measures to detect and foil any of the offences stated herein, and comply with all instructions issued by the concerned supervisory authorities in this area.

The size of the bank or money exchanger, the AML/CTF risks it faces, number and volume of transactions and the type of activity under scrutiny will impact the degree and nature of monitoring. In applying a risk-based approach to monitoring, banks and money exchangers must recognize that not all transactions, accounts or customers will be monitored in the same way. The degree of monitoring will be based on the perceived risks associated with the customer, the products or services being used by the customer and the location of the customer and the transactions. The principal aim of monitoring in a risk-based system is to respond to institution-wide issues based on each bank's or money exchanger's analysis of its major risks. As a general rule, banks and money exchangers should however ensure that all customer transactions are being monitored.

Risk-based approach monitoring allows banks and money exchangers to create thresholds monetary value below which an activity will not be reviewed. Thresholds used for this purpose should be reviewed on a regular basis to determine capability with the risk levels established. Banks and money exchangers should also assess the adequacy of any systems and processes on a periodic basis.

Banks and money exchangers should consider using an automated monitoring system (especially for those with large volumes of customer transactions) to facilitate the monitoring process through exception reports and alerts identifying unusual transactions or activity for further examination. The appropriateness and sophistication of automated monitoring system will depend on the relevance of the parameters to the nature of business undertaken by each bank or money exchanger.

Certain types of transactions or group of events should alert banks and money exchangers to the possibility that the customer is conducting suspicious activities. For example:

1. Unusual patterns of transactions that do not have apparent or visible economic, lawful or commercial purpose;
2. Events that involve complex transactions;
3. Unusual large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer;
4. Very high account turnover, inconsistent with the size of the balance;
5. Transactions connected with entities or individuals, who are the subject of the local or UN sanctions;
6. Business relationship or transactions with entities or individuals from or in countries which do not sufficiently apply the FATF Recommendations or have weak AML/CTF systems.
7. A customer who provides false or misleading information, refuses to provide relevant information, or refuses to provide his/her identity or whose identity cannot be verified.

All the above may indicate that funds are being laundered through the account. The background and purpose of such transactions should be examined as far as possible and documented in writing, and suspicious transactions should be reported in writing to FIU with a copy to SAMA.

When applying risk-based approach for terrorist financing, the following points should be considered:

1. Transaction amount is not a factor on risk determination.
2. Focus is given for particular individuals, organizations and countries.
3. Before applying risk-based approach, banks and money exchangers should identify a more comprehensive set of indicators of the method and techniques used for terrorist financing, which can then be factored into strategies to assess terrorist financing risk and devise controls to mitigate such risk.

4.6.2 Financial Investigation Process

Banks and money exchangers should have a process in place for the financial investigation and analysis of

unusual customer activity or transactions, which should include the expected frequency, size, volume and origin/ destination of customer funds whether specific to an individual customer, or for a generic customer, type or product type; and the presence of risk factors specific to the bank's or money exchanger's nature of the activity and customer base.

The investigation and analysis of the unusual and higher risk activity and transactions should be conducted by an independent reviewer, and should include the following:

1. Reviewing the identified activity/ transaction in light of the customer risk assessment and the customer due diligence information that it holds;
2. Making further enquiries to obtain additional information required to enable a determination as to whether the activity/ transaction has a rational explanation;
3. Considering the activity/ transaction in the context of any other relationships connected with the customer by referring to the relevant customer due diligence information and making enquiries to reach for appropriate conclusions;
4. Updating customer due diligence information to record the results of the enquiries made;
5. Reviewing the appropriateness of the customer risk assessment in light of the unusual activity and additional customer due diligence information obtained;
6. Considering whether further improvements of the monitoring process is required (staff training, enhancing the monitoring system parameters, strengthening controls for more vulnerable products/ services);
7. Applying increased levels of monitoring to particular relationships;
8. Where the activity or transaction does not have a rational explanation, considering whether the circumstances require a suspicious activity report to be submitted to the bank's or money exchanger's Money Laundering Control Unit (MLCU) or designated Compliance Officer.
9. In case a bank or money exchanger, through its monitoring and investigation process, finds that an activity or transaction of a customer is suspicious, further due diligence should be conducted including re-verifying the customer's information, obtaining additional information from the customer, and re-assessing the relationship.

4.6.3 Transaction Monitoring Threshold

Transaction monitoring threshold of SAR 60,000 or equivalent should be applied for all types of accounts and relationships. This threshold is applicable to a single transaction as well as an aggregate of transactions within a month. Banks and money exchangers, depending on satisfactory customer profiling, can apply product-related threshold limits that are consistent with the profile of the concerned customer.

4.7 Suspicious Transaction

4.7.1 Reporting Suspicious Transactions

The reporting of suspicious transaction or activity is critical to the competent authorities' ability to utilize financial information to combat money laundering, terrorist financing and other financial crimes. The Saudi AML Law and Bylaws and SAMA Rules require banks and money exchangers to file Suspicious Transaction Report (STR) once a suspicion has been formed.

The risk-based approach should be useful in identifying suspicious activity in the following manner:

1. Directing additional resources at those areas a bank or money exchanger has identified as higher risk;
2. The depth of the investigation process could vary depending on the risk identified;
3. Bank and money exchanger will utilize information provided by authorities to inform its approach for identifying suspicious activity;
4. Bank or money exchanger should also periodically assess the adequacy of its system for identifying and reporting suspicious transactions.

The AML Law and Bylaws apply not only to offenders but also to banks or money exchangers and their employees who participate in those transactions, if the employees concerned are aware that the fund is criminally derived. Employees whose suspicions are aroused, but who then deliberately fail to make further inquiries, wishing to remain ignorant or demonstrate "willful blindness", may be considered under Article 2 of the Saudi AML Law to have the requisite knowledge. However, Articles 21 and 25 of the Saudi AML Law relieve the bank or money exchanger, management and employees from any liability that may be caused by performing the duties provided for or by violating the provisions of confidentiality, unless if it is established that they acted in bad faith to hurt the involved person.

Banks and money exchangers reporting policy should mandate employees to do the following:

1. If an employee suspects that a money laundering or terrorist financing transaction is taking place, he/she should immediately report it to the bank's or money exchanger's internal MLCU or designated Compliance Officer. (Refer to Rule 4.7.4 for details).
2. The reporting of suspicious transactions should also include any attempted transactions, that is those transactions which have been identified as suspicious but prevented before processing.
3. Banks and money exchangers should make available, to the appropriate authorities all documents, statements and related transactions where applicable subject to SAMA's approval. Banks and money exchangers must cooperate fully with the local authorities.
4. All documents, reports and information relating to investigated cases, even if not reported to the authorities, should be maintained by the bank and money exchanger for record purposes.
5. It is a criminal offence for bank or money exchanger employees to tip off or assist any customer or individual that they know or suspect of having been involvement in any money laundering or terrorist financing activities. If an employee thinks that a transaction may be related to a criminal activity, this must be immediately reported to the bank's or money exchanger's MLCU/ Compliance Officer.
6. The notifying bank or money exchanger and its employees are free of any blame or charge in respect of any notification made, whether the suspicion is proved to be correct or not, as long as their notification was made in good faith.

4.7.2 Reporting Requirements

Under Article 7 of the AML Law, financial institutions are required to inform, provide relevant information and file Suspicious Transactions Reports (STR) to FIU, comprising a detailed report including all available information and supporting documentation on the parties involved. A copy of the report should also be sent to SAMA. Reporting to FIU shall be done using the STR form adopted by FIU. Banks and money exchangers should follow the reporting process and format as described in the Saudi AML Law and Bylaws, as follows:

1. Names of suspected individuals/ entities, their identifications, addresses and phone numbers.
2. Statement with respect to the suspected transaction/s, the involved parties, how it was discovered and present condition/ status.
3. The exact amount of the suspected transaction/s and related banking accounts.
4. Reasons of suspicion upon which the bank or money exchanger staff had depended/ based on.

Banks and money exchangers should adhere to the following steps for submission of the STRs:

1. Prepare and ensure completion of all the data and filling in of all fields in the reporting form regarding suspected transactions, including any attempted transactions, related to money laundering, indicating the name of the branch and the region, where the suspected account is domiciled;
2. Send the original suspicious report, with the supporting documents, to the FIU;
3. Fax a copy of the above report, and then mail a hard copy, to the Money Laundering Control Unit, Banking Inspection Department, Saudi Arabian Monetary Agency;
4. Retain a copy of the report and its attachments for records and future reference.

4.7.3 Tipping Off

Banks and money exchangers and their directors, officers and employees should not disclose the fact that a customer is being or has been investigated or reported for a suspicious transaction. Banks and money exchangers should exercise extreme caution when performing additional customer due diligence (CDD) because of suspicious transaction, so as not to unintentionally tip off the customer. In case the bank or money exchanger feels the performance of CCD may tip off the customer, it could then decide to discontinue the CDD but to file a suspicious activity report to FIU with a copy to SAMA.

Article 9 of the Saudi AML Law and Bylaws prohibit financial institutions and their employees from alerting customers or other related parties about suspicions of their activities or about their notification to the authorities. Under Article 8 of the Saudi AML Law, notification of suspected money laundering and terrorist financing cases to the authorities does not conflict with the provision of banking secrecy or customer confidentiality under the Saudi banking laws and regulations.

4.7.4 Money Laundering Control Unit (MLCU)

Banks and money exchangers must establish an independent and dedicated function to handle the money laundering control and reporting activities. For small-sized banks and money exchangers, with five branches and less, as a minimum, this function can be handled by the designated Compliance Officer for the

bank or money exchanger. For large banks and money exchangers with more than five branches, an independent and dedicated Money Laundering Control Unit, should be established with adequate staff who should be all Saudis. In both the above situations, the designation of the MLCU staff or Compliance Officer to handle the money laundering control function, should be a Saudi, of senior management position within the bank or money exchanger, knowledgeable of the compliance function and reporting directly to the General Manager or Managing Director of the bank or money exchanger.

The officer-in-charge of the money laundering control function, as an individual or a unit, should have sufficient authority, independence, accountability and resources, and he/she should be granted timely access to customer information (such as identification data, due diligence information, transaction records and other relevant data) to enable him/her to discharge his/her functions effectively.

MLCU, or designated Compliance Officer, will have the following functions and responsibilities:

1. Monitoring of financial banking transactions for the purpose of detecting activities that may involve money laundering and terrorist financing activities.
2. Receiving suspicious transactions relating to money laundering and terrorist finance from branches and various internal departments of the bank or money exchanger, which should entail or augmented with the collection of information, analysis of the data collected, and making necessary decision for taking appropriate action, which should be documented in writing.
3. Reporting to the Saudi Financial Intelligence Unit (SAFIU), and providing a copy to SAMA, when suspicions have been determined, in accordance with established requirements, supported by a detailed technical report on the suspected case, and within the regulatory reporting timeframes.
4. Developing automated programs for controlling money laundering activities and updating the indicators that reflect existence of suspicious money laundering acts in a manner consistent with the development and diversity of the techniques adopted in committing financial crimes
5. Submission of proposals targeting development of internal policies, plans, procedures and controls along with methods for facilitating application of the same. Approval of a state-of-the art automated system in the area of anti-money laundering.
6. Ensuring that staff, in branches and other departments, comply with the instructions and procedures pertaining to accounts monitoring; and ensuring that employees understand the importance of such procedures and instructions as well as the importance of the adopted procedures for suspicious activities and reporting requirements.
7. Supporting of Compliance Department in its task of verifying that the established rules, regulations and requirements are effectively applied in compliance with AML/CTF requirements.
8. Selection of qualified staff to fill the positions in the unit and the development of ongoing training materials to provide them with latest information on money laundering and terrorist financing activities, with the aim of enhancing their knowledge to identify such activities, trends and nature of activities, and how these can avoided and dealt with.
9. Preparation and submission of periodic reports regarding the activities conducted by MLCU/ designated Compliance Officer for money laundering and terrorist financing activities as well as the general status of the bank or money exchanger and its various departments and branches vis-à-vis this matter which need to be supported by statistical data for those activities, and recommendations made for their development/ improvements.
10. Responding to all SAMA's circulars and requests relating to customer accounts statements and blocking, and preparation of the required information in the proper form and timeframe.
11. Maintaining a database comprising all data relating to money laundering and terrorist financing matters in the bank or money exchanger, such as the suspicious cases reported, blocked accounts, etc. and updating of all the old cases in the database.

4.8 Internal Controls

4.8.1 Internal Control Procedures

Under Article 10 of the Saudi AML Law, financial institutions are required to establish and maintain internal control procedures to prevent their institutions from being used for purposes of money laundering and terrorist financing.

In order to have an effective risk-based approach, the risk-based process must be imbedded within the internal controls of the banks or money exchangers. Senior management is ultimately responsible for ensuring that a bank or money exchanger maintains an effective internal control structure, including suspicious activity monitoring and reporting. Strong senior management leadership and engagement in AML/CTF is an important aspect of the application of the risk-based approach. Senior management must

create a culture of compliance, ensuring that all employees adhere to the bank's or money exchanger's policies, procedures and processes designed to limit and control risks.

In addition to other compliance internal controls, the nature and extent of AML/CTF controls will depend upon a number of factors, including:

1. Nature, scale and complexity of a bank's or money exchanger's business.
2. Diversity of a bank's or money exchanger's operations, including geographical diversity.
3. Bank's or money exchanger's customer, product and activity profile and distribution channels used.
4. Volume and size of the transactions.
5. Degree of risk associated with each area of the bank's or money exchanger's operation.
6. Extent to which the bank or money exchanger is dealing directly with the customer or through third parties.

The framework of internal control procedures should:

1. Provide increased focus on a bank's or money exchanger's operations (products, services, customers and geographic locations) that are more vulnerable to abuse by money launderers and other criminals.
2. Provide for regular review of the risk assessment and management processes, taking into account the environment within which the bank or money exchanger operates and the activity in the market place.
3. Provide for an AML/CTF compliance function and designate an individual at management level responsible for managing the compliance function.
4. Ensure that adequate controls are in place before new products are offered.
5. Inform senior management of compliance initiatives, identified compliance deficiencies, corrective action taken, and suspicious activity reports filed.
6. Focus on meeting all regulatory record keeping and reporting requirements, recommendations for AML/CTF compliance and provide for timely updates in response to changes in regulations.
7. Implement risk-based customer due diligence policies, procedures and processes.
8. Provide for adequate controls for higher risk customers, transactions and products, as necessary, such as transaction limits or management approvals.
9. Enable timely identification of reportable transactions and ensure accurate filing of required reports.
10. Include AML/CTF compliance in job descriptions and performance evaluations of appropriate personnel.
11. Provide for appropriate continuous training to be given to all relevant staff.

4.8.2 Assessment of Internal Controls

Banks and money exchangers should establish means of independently and periodically assessing the effectiveness of the internal controls and the adequacy of the overall AML/CTF programs. The assessment should include validating the operation of the risk assessment and management processes and related internal controls, and obtaining appropriate comfort that the adopted risk-based approach reflects the risk profile of the bank or money exchanger.

The internal audit department of the bank or money exchanger, which should be separate from the compliance function, should conduct independent testing to assure the adequacy of the overall compliance function. The results of the testing should be documented and communicated to senior management for appropriate action.

4.9 Staff Training & Hiring

4.9.1 Staff Training & Awareness

Article 10.c of the AML Law and Bylaws mandate all financial institutions to develop training programs to educate their employees and enhance their understanding of KYC procedures, money laundering and terrorist financing risks, trends and preventive methods. As employees become familiar with such activity, they can play an effective role in combating money laundering and terrorist financing through prevention and detection measures.

Banks and money exchangers should therefore provide their employees with appropriate and proportional training, and ongoing awareness, with regard to money laundering and terrorist financing. A bank's or money exchanger's commitment to having successful controls relies on both training and awareness. This requires an institution wide effort to provide all relevant employees with at least general information on AML/CTF laws, regulations and internal policies on compliance.

Applying a risk-based approach to the various methods available for training, however, gives each bank or money exchanger, additional flexibility regarding the frequency, delivery mechanisms and focus of such training. A bank or money exchanger should review its own workforce and available resources and implement

training programs that provide appropriate AML/CTF information, as follows:

1. Tailored to the appropriate staff responsibility (e.g., front-line staff, compliance staff, or customer relations staff, account opening and operations.).
2. At the appropriate level of detail (e.g., complex products, new products and services, trends).
3. At a frequency related to the risk level of the business line involved.
4. All new staff should be educated in the importance of AML/CTF policies while regular refresher training should be provided to staff to ensure that they are reminded of their responsibilities and kept informed of new developments.
5. Testing to assess staff knowledge commensurate with the detail of information provided.

Additionally, banks and money exchangers should make all their staff aware of their responsibilities, personal obligations, liability and penalties under the legislation, should they fail to comply with the relevant requirements, as stated in Articles 2, 3, 9, 17, 18, 21 and 25 of the Saudi AML Law.

4.9.2 Staff Hiring & Appointment of Senior Positions

Banks and money exchangers should put in place adequate background screening procedures to ensure high standards when hiring employees. Banks and money exchangers can develop a risk-based approach on the level of screening based on the function and responsibilities associated with a particular position.

In addition, banks and money exchangers should comply with the provisions stipulated in the SAMA Directive issued in April 2005, relating to Qualification Requirements for Appointment to Senior Positions in Banks, including notifying SAMA for each senior appointment and the annual submission of a list of senior positions.

4.10 Record Keeping & Retention

Banks and money exchangers must keep all records (documents, instructions, transactions, files and reports) relating to their operations in accordance with normal business practices, for ease of reference in their own use, and for use by supervisory/ regulatory and other authorities, and for internal and external auditors. The records should be adequate enough to be able to reconstruct a transaction and offer a complete audit trail of all financial transactions, in particular cash transactions and funds transfer.

Article 5 of the Saudi AML Law requires financial institutions to maintain, for a minimum of ten years following the conclusion of an operation/ transaction or termination of an account/ relationship, all records and documents that explain the financial, commercial and monetary transactions, whether local or foreign, the files of account documentation, related correspondence and copies of the identification documents. Taking into consideration the local law, customer transaction records, such as agreements, checks, etc., should be retained indefinitely.

In specific cases, banks and money exchangers may be instructed by SAMA or other Saudi competent authorities, to maintain any transactions or account records beyond the minimum time period stated below.

Banks and money exchangers should keep and retain these records in the form and for the period as indicated below:

1. Primary Records

Type of Record*Retention Form*Retention Period

a. Customer account opening agreements and related account documents* Original form*Permanently

b. Certified/ attested copies of customer identification documents*Originals of the certified/attested copies*Permanently

c. All customer transaction records and instructions: i. Manual instructions (e.g., checks, transfer applications, etc.) ii. Automated instructions (e.g., internet, phone banking, ATM, incoming wire transfers, etc.)*One of the following: i. Original form ii. Electronic form*Permanently

d. Statements and details of customer accounts and balances*Electronic form*Permanently

2. Secondary/ Non-Financial Records

Type of Record**Retention Form**Retention Period

a. Customer profiles, risk assessments and all other KYC related documents**Original and/or electronic form**Minimum 10 years

b. Investigations, suspicious activity reports, etc.**Original and/or electronic form**Minimum 10 years

c. Automated and manual reports**Original and/or electronic form**Minimum 10 years

d. Reviews, self-assessments, audit reports, etc.**Original and/or electronic form**Minimum 10 years

5. AML / CTF Other Risks

5.1 Product/ Service Risks

Product or service risks are the potential risks inherent in the products or services offered by a bank or money exchanger. Banks and money exchangers should be aware of the associated risks in all the products and

services they offer including the way they are delivered, especially for new or innovative products or services. Banks and money exchangers should develop appropriate risk assessment and controls. The products and services offered by banks and money exchangers, determined as posing potentially higher risks are described below.

5.1.1 Cash

Physical cash is often the ideal and most commonly used method of value transfer for criminal activities, including money laundering and terrorist financing, simply because it is anonymous, untraceable, requires no intermediary, is widely accepted and provides for immediate settlement. While the provision of services to cash-generating business is a particular area of concern, however, some businesses are legitimately cash-based, especially in the retails sector, and so there will often be a high level of cash deposits associated with some of these accounts.

1. Cash Transactions

SAMA has been engaged for many years in the efforts to transform the Saudi economy to a bank-payment based society and has taken significant steps to discourage large cash transactions and encourage the use of banking payment systems and services, such as SARIE, SWIFT, ATM/SPAN, POS, SADAD, Internet banking, credit cards, etc. SAMA Account Opening Rules require banks and money exchangers to accept cash from customers only through an account or relationship, where a full due diligence and KYC process has been established.

Banks and money exchangers should have a process in place to detect cash transactions that could be deemed as suspicious, such as:

1. Large cash deposits, not in line with the customer's type of business or occupation.
2. Numerous cash deposits of small amounts, known as structuring or smurfing, to avoid detection.
3. Cash deposits followed by a transfer (wire transfer, bank check, etc.).
4. Structured cash payments for outstanding credit card balances, with relatively large sums as payments.

2. Cross-Border Transportation of Cash

In accordance with Saudi AML Law Article 14 and related Bylaws, banks and money exchangers should comply with the requirements relating to cross-border transportation of cash coming into or going out of Saudi Arabia for their own use. The cash may be carried by banks and money exchangers or through cash transportation firms by way of cargo, postal parcels, air shipments, etc. Banks and money exchangers or their cash transportation firms should adhere to the requirements by completing a special declaration form for any cash shipment more than SAR 60,000 or equivalent (or equivalent in foreign currencies), in accordance with SAMA Rules for Cash Transportation for Banks and Money Exchangers issued on 29 April 2007.

5.1.2 Wire Transfers

The term wire transfer or funds transfer refers to any transaction carried out on behalf of an originator person (both natural and legal) through a bank or money exchanger by electronic means for the purpose of making an amount of money available to a beneficiary person at another bank or money exchanger. The originator and the beneficiary may be the same person/ entity. The transfer could be a cross-border transfer (to/ from a different country) or a domestic transfer (within the same country).

SAMA Account Opening Rules require banks and money exchangers to accept transfers only from customers having account or other relationship agreement (e.g., express remittance service). Therefore banks and money exchangers should always have adequate information about the originator/ remitter. To enhance the transparency of wire transfers for effective AML/CTF programs, banks and money exchangers should adopt the following measures when executing transfers for their customers:

1. For all outgoing cross-border transfers, ensure to include full and accurate originator information (name, address and account number) on the funds transfers and related messages that are sent, and the information should remain with the transfer or related message in the payment chain.
2. For incoming cross-border transfers, ensure they contain full originator information (name, address and account number) for transfers of SAR 5,000 and above or equivalent and verify if needed. In case the incoming transfer does not contain complete originator information, the bank or money exchanger should hold the transfer and contact the remitting bank for the missing information. Failure to obtain the missing information may be considered as a cause for suspicion and reassessing the relationship with the remitting bank.
3. For domestic transfers (within Saudi Arabia), ensure the remitter's name and account number is included, which should be recorded and retained in the system of remitting bank or money exchanger for prompt retrieval if requested by competent authorities.

4. Retain all physical and system records of all funds transfers in accordance with the prevailing record retention periods.
5. Exercise extra due diligence for funds transferred from or to NCCTs as periodically defined by FATF.
6. Conducting KYC/ due diligence on the remitter/ originator is the responsibility of the remitting bank or money exchanger, whether foreign or local.
7. Conduct a name check of the parties involved in the transfer (originator, beneficiary, intermediary bank) as per requirements in Rule 4.3.5 of this document.
8. Exercise extra the required due diligence when processing transfers relating to PEPs.
9. Not to accept any incoming or outgoing transfers outside Saudi Arabia, for any charity organizations, except with the prior written approval from competent authority through SAMA.
10. When implementing any new electronic fund transfer and payment systems, ensure the systems are designed with capabilities for preventing and detecting money laundering and terrorist financing transactions. Examples of the new electronic payment methods include prepaid cards, electronic purse/stored value cards, mobile payments, internet payment services, etc. Ensure these services are offered only to customers who already have an account or other relationship with the bank or money exchanger.

5.1.3 Alternative Remittances

Alternative remittance system refers to a type of financial service involving the transfer of funds or value from one geographic location to another through informal and unsupervised networks or mechanisms, which traditionally operate outside the regulated conventional financial sector. The very features (efficiency, anonymity and lack of paper trail) which make alternative remittance system attractive to legitimate customers (mainly expatriates remitting money to relatives in home countries), also make the system conducive for the transfer of illicit funds.

Therefore, due to this inherent risk, these systems have proven themselves vulnerable to misuse for money laundering and especially for terrorist financing purposes. Quite often these systems have ties to particular geographic regions and are therefore described using a variety of specific terms, most common being “Door-to-Door”, “Hawala”, or "Hundi". In addition to the vulnerability for misuse, unauthorized or unlicensed alternative remittance services are illegal in Saudi Arabia and banks and licensed money exchangers should endeavor to assist authorities in fighting such unlawful activities.

Persons who offer these illegal services, at a certain point, channel their funds in “blocks” through the banking system by cash deposits and then remit the funds to the beneficiary by a transfer, or communication/ message. Therefore, banks and money exchangers should apply prudent measures to identify and prevent the use of customer accounts for this illegal business. While such suspicious transactions may be difficult to monitor, the application of due diligence process and relevant red flags indicators can help in identifying such transactions. As a minimum, banks and money exchangers should implement the following steps:

1. Have a mechanism in place to monitor customer accounts or relationships for trends of suspicious activities that could indicate dealing or providing alternative remittance service.
2. No account or relationship should be opened or retained if there is any evidence of the account or relationship being used for any type of alternative remittances (e.g., hawala, hundi). Any activities noted under this category should be reported as suspicious activities to FIU with a copy to SAMA.
3. Obtain satisfactory explanation for a customer who maintains several accounts at various locations without reasonable justification.
4. Have a process in place to monitor activity of a customer who receives numerous small deposits to his/her account from various locations, which are not consistent with his/her line of business in accordance with his/her account profile on file. Such account is often used as "collection account" to accumulate funds from various groups and then sent abroad in a single transaction.
5. Track transactions whereby large cash deposits are credited into a customer account and then immediately followed by a telex transfer to another country.
6. The above trends could indicate that the customer is engaged in offering alternative remittance service illegally and, if banks and money exchangers deemed the activities to be suspicious, these should be reported to FIU with a copy to SAMA. The above-stated trends are not exhaustive and banks and money exchangers should implement more controls based on experience and understanding of their customers.

5.1.4 Money Exchanging

Money Exchange is a regulated business in Saudi Arabia and all money exchangers are subject to the

Ministerial Order # 31920 dated 16/2/1402H, which requires all money exchangers to obtain specific license from SAMA. The Ministerial Order prohibits money exchangers from accepting deposits and restricts their activities to purchase and sale of foreign currencies, travelers checks, bank drafts and making remittances inside and outside Saudi Arabia as per the license granted to them by SAMA. The Banking Control Law also prohibits non-banking entities from conducting banking business and, as per authority given, SAMA can impose penalties including revoking of license.

SAMA Account Opening Rules permit banks to open accounts for licensed money exchangers, provided that they have been registered by Ministry of Commerce and licensed by SAMA, specifically indicating that they are allowed to conduct such activity. However, due to the nature of their business, these entities may be engaged in offering remittance service to the community. Therefore, they should be categorized as High Risk for an extra customer due diligence and closer scrutiny.

5.1.5 Electronic Banking

Electronic banking is a broad term encompassing delivery of information, products and services by electronic means (such as telephones/ mobiles, personal computers, automated teller machines, points of sales, and automated clearing houses). Electronic banking provides opportunities for banks to offer a variety of their banking products and services in a faster, more convenient and cheaper way.

The number of banks providing banking services through internet is growing considerably, with increasing range of services becoming available, including savings and deposit account services, credit cards, transfers, bill paying services, shares trading, etc. Therefore, electronic banking is vulnerable to money laundering and terrorist financing because of its user anonymity (usage and funding), rapid transaction speed, and its wide geographic availability.

To prevent these risks, banks and money exchangers should be required to have policies in place or take such measures as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes. banks and money exchangers are not allowed to offer banking products and services through electronic banking payment methods (internet/ online banking, telephone, automated teller machine, mobile, or any new electronic payment method) to customers unless they maintain a bank account or other relationship with the bank, in which case the banks and money exchangers will have electronic records of the customers including identification and other personal information.

5.1.6 International Trade

International trade, which deals in the movement of goods and services, can be used either as a cover for the movement of illicit funds or as the money laundering mechanism itself. Criminals will utilize normal trade-related products and services offered by banks relating to import and export operations, such as letters of credit, guarantees, documentary bills for collection, trade financing services, etc., to legitimize the proceeds of their money laundering activities or to provide funding for terrorist organizations, with a relatively low risk of detection. The techniques used basically are: misrepresentation of the price (over-, under- and multi-invoicing of goods/ services), quantity (over- and under-shipments of goods/ services), or quality of imports or exports (falsely described goods/ services).

Banks should watch out for the following examples of red flag indicators that are commonly used to identify trade-based money laundering activities:

1. Discrepancies between the description of the goods on the invoice and bill of lading.
2. The size of the shipment or the type of goods appears inconsistent with the customer's regular business activities.
3. The letter of credit amount is unusually large or sudden surge in number of letters of credit issuance that appears to deviate from the customer's normal business activity.
4. The type of goods being shipped is designated as high risk or involves a high-risk jurisdiction.
5. The transaction involves receipt of payment (especially cash) from third parties with no apparent connection with the transaction.
6. The transaction involves the use of repeatedly amended or frequently extended letter of credit.
7. The transaction involves the use of front (or shell) companies.

5.2 Country/ Geographic Risks

Country or geographic risks can be defined as risks posed by countries that are subject to sanctions by United Nations (UN) or by other credible sources (e.g., FATF-NCCTs) due to one factor or a combination of factors, as determined by UN or FATF, such as lack of appropriate AML/CTF laws, regulations and other measures; providing funding or support for terrorist

activities; or having significant levels of financial criminal activities.

Banks and money exchangers should exercise additional due diligence and give special attention to business relations and transactions with persons, including companies and banks that are located in or whose geographical spheres of business activities are in jurisdictions that do not adequately apply FATF recommendations.

Whenever necessary, SAMA will issue instructions to banks and money exchangers about certain countries and on how transactions relating to these countries should be treated.

5.3 Risk Variables

A bank's or money exchanger's risk-based approach methodology may take into account risk variables specific to a particular customer or transaction. These variables may increase or decrease the perceived risk posed by a particular customer or transaction and may include:

1. The purpose of an account or relationship.
2. The level of assets to be deposited in relation to the customer's profile.
3. The level of regulatory oversight to which a customer is subject.
4. The regularity or duration of the relationship.
5. The familiarity with a country and regulatory structure.

END OF POLICY DOCUMENT

6. Glossary

Account: "Account" should be taken to include, in addition to a bank account, any other similar banking relationships (such as bank account, credit card, express remittance service, etc.) between the bank or money exchanger and its customer.

Anonymous, Fictitious Name or Numbered Account: Anonymous, Fictitious Name or Numbered Account is generally a bank account for which the customer's name does not appear on the bank's records/ systems, documents and statements. Instead, a unique number or code-name is recorded. The customer's identify is known only to a small number of the bank's officials. While such accounts are offered by some banks in the world for a legitimate purpose, such as providing confidentiality and additional protection for private matters, they can also be misused to hide the proceeds of financial crimes.

Beneficial Owner: The natural person who ultimately owns or controls a customer and/ or the person on whose behalf a transaction is being conducted. It also includes a person who exercises ultimate effective control over a legal person or arrangement.

Competent Authority: All administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including SAMA and SAFIU.

Extra Due Diligence (EDD): This is an additional due diligence process needed for all High Risk accounts/ relationships and where the bank/ME deems it necessary. EDD is needed for PEPs, private banking customers, correspondent banks, charity organizations, and for other types of customers categorized as high risk by the bank/ME.

Financial Action Task Force (FATF): Financial Action Task Force, the main ruling international body for overseeing AML-CTF efforts. Saudi Arabia is a member of this organization through its membership of the GCC.

Financial Intelligence Unit (FIU): The UN Convention adopted this definition, stating: "Each state shall consider the establishment of a financial intelligence unit to serve as a national center for the collection, analysis and dissemination of information regarding potential money laundering." Based on the Saudi AML Law of 2003, the Saudi Financial Intelligence Unit was established under the authority of the Ministry of Interior. This is the authority that receives and analyzes suspicious activity reports from all financial & non-financial institutions.

Intermediary: A professional intermediary is a firm or person (such as an accountant, banker, broker, lawyer or similar professional) who manages an account or transacts on behalf of a client.

Money Exchanger (ME): A natural or legal person who provides a money/ currency changing service and/ or providing a money/ value transfer/ remittance service. The person must be registered by Ministry of Commerce and licensed by SAMA. These entities are subject to SAMA regulations as per authority given through the Banking Control Law, the AML Law (Bylaw 1.1) and the Ministerial Order # 31920.

Nominee: A person or firm (registered owner) into whose name securities or other assets are transferred and held under a custodial agreement in order to facilitate transactions, while leaving the customer as the actual owner (beneficial owner). A "nominee account" is a type of account in which a stockbroker holds shares belonging to clients, making buying and selling those shares easier.

Non-Cooperative Countries & Territories (NCCT): FATF publishes reports on countries which do not

cooperate adequately in the fight against money laundering, known as Non-Cooperative Countries & Territories. The list is maintained and updated by FATF and may be consulted on the FATF website. Banks/MEs should give special attention to business relations and transactions with customers from countries included in the NCCT list, and exercise extra due diligence.

Payable-Through Account: This is a demand deposit account maintained at a local bank by a foreign bank or corporation, whereby the foreign bank channels deposits and checks of its customers (usually individuals or businesses located outside the country) into the account. The foreign customers have signing authority over the account and can thereby conduct normal international banking activities. This makes it impossible to implement KYC policy and monitoring of suspicious activity process for the customers using the account

Shell Bank: Shell bank means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.

Source of Funds: Source of funds is the activity which generates the funds for a relationship, e.g., a customer's occupation or business activities.

Source of Wealth: Source of wealth is different from source of funds, and describes the activities which have generated the total net worth of a person both within and outside of a relationship, that is those activities which have generated a customer's funds and property.

Subsidiaries: This refers to majority owned subsidiaries of a bank or money exchanger, inside or outside the country.

Suspicious Transaction: A suspicious transaction is one in respect of which a banks/ME has reason to believe that some type of wrongdoing or illegal activity may be involved. Suspicious transactions must be reported to the appropriate authorities through Suspicious Transaction Report (STR). The notifying bank/ME and its employees are free of any blame or charge in respect of any notification made, whether the suspicion is proved to be correct or not, as long as their notification was made in good faith.

Trustee: A person (an individual or entity) who holds and administers the assets in a trust fund separate from the trustee's own assets, for the benefit of another person/s (the beneficiary/ies). The trustee invests and disposes of the assets in accordance with the settlor’s trust agreement, taking into account of any letter of wishes. There may also be a protector, who may have power to veto the trustees’ proposals or remove them, and/or a custodian trustee, who holds the assets to the order of the managing trustees.

Unusual Transaction: An activity or transaction that is inconsistent with or deviates from the expected pattern of activity within a particular customer, or with the normal business activities for the type of product or service offered. Unusual activity or transaction should alert banks to the possibility of suspicious transactions.

ANNEX 6: THE BANKING CONTROL LAW (1966)

BANKING CONTROL LAW
ISSUED BY ROYAL DECREE
No. MIS Dated 22.2.1386
ROYAL DECREE
NO. MI 5
Date: 22.2.1386 (11.6.1966)

With the help of God Almighty, We, Faysal Ibn Abdul Aziz AI Saud, King of the Kingdom of Saudi Arabia, In view of Article 19 of the Council of Ministers' Charter issued by Royal Decree No.38 dated 22.10.1377 A.H. and having reviewed Council of Ministers' Decision No.179 dated 5.2.1386, ordain the following: First: Approving Banking Control Law in the Attached text. Second: The Deputy Premier and the Minister of Finance and National Economy shall execute our present Decree. Faysal

BANKING CONTROL LAW

Article 1

In this Law the following expressions shall have the definitions specified in this Article:

a. "Bank" means any natural or juristic person practicing basically any of the banking business in the Kingdom.

b. "Banking Business" means the business of receiving money on current or fixed deposit account, opening of current accounts, opening of letters of credit, issuance of letters of guarantee, payment and collection of cheques, payment orders, promissory notes and similar other papers of value, discounting of bills, bills of exchange and other commercial papers, foreign exchange transactions and other banking business.

c. "National bank" means a bank the head office and branches of which are situated in the Kingdom.

d. "Foreign Bank" means a bank with branches in the Kingdom and its head office outside it.

e. "Agency" means the Saudi Arabian Monetary Agency.

f. "Invested Capital," means the capital assigned by a foreign bank for the capital use of its branches in the Kingdom.

Article 2

No person, natural or juristic, unlicensed in accordance with the provisions of this Law, shall carryon basically any of the banking business. However,

a. Juristic persons licensed in accordance with another law or special decree to carry on banking business may practice such business within the limits of their intended purposes.

b. Licensed moneychangers may practice basically exchange of currency in the form of notes and coins, but no other banking business.

Article 3

All applications, for the grant of licenses to carryon banking business in the Kingdom, shall be addressed to the Agency which will study the applications after obtaining all the necessary information and submit its recommendations to the Minister of Finance and National Economy.

The license for a National Bank shall stipulate the following:

1. It shall be a Saudi Joint Stock Company.
2. The paid-up capital shall not be less than Rls. 2.5 million and all subscriptions towards share capital shall be payable in cash.
3. The founders and members of the board of directors shall be persons of good reputation.
4. The memorandum and articles of association shall be acceptable to the Minister of Finance and National Economy.

In the case of a Foreign Bank wishing to set up a branch or branches in the Kingdom, the grant of a license shall be subject to such conditions as the Council of Ministers may stipulate upon the recommendation of the Minister of Finance and National Economy. The license shall in all cases be issued by the Minister of Finance and National Economy after the approval of the Council of Ministers.

Article 4

As an exception to the provisions of the previous Article, the licenses or authorizations previously issued to the persons carrying on banking business in the Kingdom and effective at the time of promulgation of this Law shall continue to be recognized.

The Agency may, however, call such documents and information from these persons, as it may deem necessary.

The Agency with the approval of the Council of Ministers may call upon them to comply with all or any of the provisions of Article 3 of this Law within such period as it may fix.

Article 5

Any person not authorized basically to carryon banking business in the Kingdom is not allowed to use the word "Bank", or its synonyms, or any similar expression in any language on his papers or printed

matter, or in his commercial address, or his name or in his advertisements.

Article 6

The deposit liabilities of a bank shall not exceed fifteen times its reserves and paid-up or invested capital. If the deposit liabilities exceed this limit, the bank must within one month of the date of submission of the statement referred to in paragraph 1 of Article 15, either increases its capital and reserves to the prescribed limit or deposit fifty percent of the excess with the Agency.

Article 7

Every bank shall maintain with the Agency at all times a statutory deposit of a sum not less than fifteen percent of its deposit liabilities. The Agency may, if it deems it to be in the public interest, vary the aforesaid percentage provided that it shall not be reduced below 10 percent nor increased to more than 17.5 percent. The Agency may, however, vary these two limits with the approval of the Minister of Finance and National Economy.

In addition to the statutory deposit provided for in the previous paragraph, every bank shall maintain a liquid reserve of not less than 15 percent of its deposit liabilities. Such reserve shall be in cash, gold or assets, which can be converted into cash within a period not exceeding 30 days. The Agency may, if deemed necessary, increase the aforesaid percentage up to twenty percent.

Article 8

No bank shall grant a loan or extend a credit facility, or give a guarantee or incur any other financial liability with respect to any natural or juristic person for amounts aggregating more than 25 percent of the Bank's reserves and paid-up or invested capital. The Agency may, in the public interest, and subject to such conditions as it may impose, increase this percentage up to 50 percent.

The provisions of the above paragraph do not apply to transactions between banks or between head offices and their branches or between these branches.

Article 9

No bank shall undertake the following transactions:

1. Granting a loan or extending credit facilities, or issuing a guarantee or incurring any other financial liability on the security of its own shares.

2. Granting, without security, a loan or credit facilities, or issuing a guarantee or incurring any other financial liability in respect of:

a. Member of its Board of Directors or its Auditors.

b. Establishments not taking the form of joint-stock companies in which any of its Directors or Auditors is a partner or is a manager or has a direct financial interest.

c. Persons or establishments not taking the form of joint stock companies in cases where any of the Bank's directors or Auditors is a Guarantor.

3. Granting, without security, a loan or a credit facility or giving a guarantee or incurring any other financial liability in favor of any of its officials or employees for amounts exceeding four months salary of any such concerned person.

Any bank director or auditor or manager who contravenes paras 2 and 3 of this Article, shall be considered as having resigned his position.

Article 10

No bank shall undertake any of the following activities:

1. To engage, whether for its own account or on a commission basis, in the wholesale or retail trade including the import or export trade.

2. To have any direct interest, whether as a stock-holder, partner, owner, or otherwise, in any commercial, industrial, agricultural or other undertaking exceeding the limits referred to in para 4 of this Article, except when such interest results from the satisfaction of debts due to the bank, provided that all such interests shall be disposed of within a period of two years or within any such longer period as may be determined in consultation with the Agency.

3. To purchase, without the approval of the Agency, stocks and shares of any bank conducting its business in the Kingdom.

4. To own stocks of any other joint-stock company incorporated in the Kingdom, in excess of ten percent of the paid up capital of such a company provided that the nominal value of these shares shall not exceed twenty percent of the bank's paid-up capital and reserves; the above limits may, when necessary, be increased by the Agency.

5. To acquire or lease real estate except in so far as may be necessary for the purpose of conducting its banking business, housing of its employees or for their recreation or in satisfaction of debts due to the Bank.

In cases where a bank acquires real estate in satisfaction of debts due to it and such real estate is not necessary for the Bank's own banking business or housing of its employees or for their recreation, it shall dispose of it within three years of its acquisition or, in exceptional and justifiable circumstances, within such period or periods as may be approved by the Agency

and subject to such conditions as it may deem fit to prescribe.
As an exception to the provisions of para 5 of this Article, the bank may, in special and justifiable circumstances and with the approval of the agency, acquire real estate, the value of which shall not exceed 20 percent of its paid-up capital and reserves.

Article 11
Banks are precluded from undertaking any of the following operations except after the written approval of the Agency and according to the conditions it prescribes:
a. Altering the composition of their paid-up or invested capital.
b. Entering into any scheme of amalgamation or participation in the business of another bank or another establishment carrying on banking business.
c. Acquiring shares in a company established outside the Kingdom.
d. Ceasing to carryon banking business. In such a case, the Agency must, before agreeing to this cessation, ascertain that the Bank has made necessary arrangements to safeguard the rights of the depositors.
e. Opening branches or other offices in the Kingdom and also opening of branches or other offices by national banks outside the Kingdom. Before granting the written license provided for under this paragraph, the Agency should get the approval of the Minister of Finance and National Economy.

Article 12
No person shall be a director of more than one bank.
No person in the following cases shall be elected as a director or shall become a manager of any bank without prior written approval of the Agency:
a. If he occupied a similar position in a banking concern that was wound up, even if the liquidation had been made before the promulgation of this Law.
Such approval shall not be given by the Agency until it becomes clear that the person concerned was not responsible for that liquidation.
b. If he was removed from a similar post in any banking establishment, even if such removal was before the promulgation of this Law. The approval of the Agency shall in this case be based on acceptable reasons.
Any director or manager of a bank, who is adjudicated bankrupt or convicted of a moral offense, shall be considered as having resigned his post.

Article 13
Every bank shall, before declaring distribution of any profits, transfer a sum equal to not less than 25 percent of its net profits, to the statutory reserve, until the amount of that reserve equals as a minimum of the paid-up capital. (Amended Clause*) "No bank shall pay dividends or remit any part of its profits abroad, until its aggregate foundation expenditures and losses incurred have completely been written off, and after deducting not less than 10% of the value of capitalized expenditures until all these expenditures have been completely written off. (Amended in accordance with Royal Decree No. MI2 dated 6.1.1391 AB.)
Any action taken to declare or pay dividends in contravention to the provisions of this Article shall be considered null and void.

Article 14
Every bank shall appoint annually two auditors from amongst the approved list of auditors registered with the Ministry of Commerce and Industry. The Auditors shall submit a report on the Balance sheet and profit and loss account. This report shall include whether in the auditor's opinion the Bank's balance sheet duly and correctly represents its financial position and the extent of their satisfaction with any explanations or information they may have requested from the bank's manager or other staff.
With regards to banks taking the form of a company, the report referred to in the above paragraph shall be read together with the annual report of the Bank management in the General Meeting, which must be held within the six months following the end of the bank's financial year. The bank management should send copies of these two reports to the Agency.
The provisions of the first para of this Article shall apply to foreign banks in respect of their branches operating in the Kingdom. They should send a copy of the Auditor's report to the Agency.

Article 15
Every bank shall furnish the Agency by the end of the following month with a consolidated monthly statement of its financial position relating to the previous month, which shall be true and correct, and be in the form prescribed by the Agency. Every bank shall also furnish the Monetary Agency within six months of the close of
its financial year with a copy of its annual balance sheet and profit and loss accounts certified by its auditors in the form prescribed by the Agency.

Article 16
The Monetary Agency may, with the approval of the Minister of Finance and National economy, issue general rules regarding the following matters:
1. The maximum limits of total loans that can be extended by a bank or banks.
2. The prohibition or limitation of specified categories of loans or other transactions.
3. Fixing the terms and conditions, which banks, should take into consideration when carrying out certain types of transactions for their customers.
4. The cash margins to be obtained by banks against specified categories of credits or guarantees.
5. The minimum ratio to be observed between the limits for loans and the collateral for such loans.
6. Fixing the assets to be maintained by each bank within the Kingdom. Such assets should not fall below a certain percentage of the Bank's deposit liabilities, which shall be fixed by the Agency from time to time.
The Agency may, from time to time, issue decisions concerning the following:
1. Definition of the expression "deposit liabilities" referred to in this Law.
2. Determination of bank holidays and bank business hours.

Article 17
The Agency may, at any time, request any bank to supply it, within a time limit it will specify and in the manner it will prescribe, with any information that it deems necessary for ensuring the realization of the purposes of this Law.

Article 18
The Agency may, with the approval of the "Minister of Finance and National Economy conduct an inspection of the books and accounts of any bank, either by the Agency's own staff or by outside auditors assigned by it. The examination of the bank's books and accounts should take place in the bank's premises. In such a case the bank staff must produce all the required books and records of accounts and other documents in their custody or within their authority and must furnish any information they have relating to the bank.

Article 19
Any person, who comes into possession of information during the performance of his duties in the implementation of this Law, is not allowed to disclose such information or to make use of it in any manner.

Article 20
The Agency shall periodically publish combined statements of the principal data contained in the returns mentioned in Article 15.

Article 21
The Minister of Finance and National Economy, in exceptional circumstances, and with the prior approval of the Council of Ministers, may exempt any bank from any provision of this Law or from the regulations issued in execution thereof for a limited period and subject to such other conditions as may be laid down in each case.

Article 22
If the Agency finds that a bank has failed to comply with the provisions of this Law, or with the provisions of any regulations issued under this Law, or if a Bank adopts a policy that might seriously affect its solvency or liquidity, it may, with the approval of the Minister of Finance and National Economy, take one or more of the following measures:
a. Appoint one or more advisers to advise the bank in the conduct of its business.
b. Order the suspension or removal of any director or officer of the bank.
c. Limit or suspend the granting of credits or the acceptance of deposits.
d. Require the bank to take such other steps, as it may consider necessary.
If the Agency finds that a bank persistently contravenes the provisions of this Law or the decisions or regulations made there under, it may call upon such a bank to submit its reasons for the contravention, accompanied by its proposals to rectify the position within a stated period. If the Agency is of the opinion that such proposals are not sufficient for their purpose or if the bank fails to implement an agreed or prescribed course of action within the stated period, the Minister of Finance and National Economy may, subject to the approval of the Council of Ministers, revoke the license of the said bank.

Article 23
1. Any person who contravenes the provisions of para 1 of Article 2, Article 5 and items a, band c of para 1 of Article 11, Article 12 and Article 18, shall be liable to imprisonment for a term not exceeding two years and to a fine not exceeding Rls 5,000 for every day the offense continues or to either of these penalties.
2. Any person who contravenes the provisions of Article 19 shall be liable to imprisonment for a term

not exceeding two years and to a fine not exceeding Rls 20,000 or to either of these penalties.
3. Any person who contravenes the provisions of Articles 8, 9 and 10 shall be liable to imprisonment for a term not exceeding six months and to a fine not exceeding Rls 10,000 or to either of these penalties.
4. Any person who contravenes the provisions of articles 7, 14 and 15 shall be liable to a fine not exceeding Rls 500 for every day the contravention continues.
5. Any person who contravenes any other provision of this Law or the regulations and decisions issued in execution thereof shall be liable to a fine not exceeding Rls 5,000.
6. In the event that offenses punishable according to paras 2,3 and 5 of this Article are committed by the same person for one purpose and provided that such offenses are inter-related as to object and timing, they are to be considered as one offense punishable by one penalty.
In imposing the penalties contained in this Article it is to be observed that should an offense be punishable by more than one penalty, the offender shall be subjected to the severest.

Article 24
The Chairman, the Managing Director, the Directors, head office Manager and Branch manager shall be responsible, each within his own jurisdiction, for any contravention of this Law or the decisions and rules issued for its execution.

Article 25
The Minister of Finance and National Economy shall appoint a committee of three persons from outside the Agency and specify the conditions and measures to be observed in adjudging contraventions punishable under this Law at the request of the Agency.

Article 26
The Deputy Premier and the Minister of Finance shall put this Law into effect and it shall come into force from the date of its publication.

ANNEX 7: RULES FOR ENFORCING THE BANKING CONTROL LAW (1986)

Ministerial Decision *NO.3/2149* dated 14.10.1406 H
Ministerial Decision No.3/2149 dated 14.10.1406 H.
The Minister of Finance and National Economy, In accordance with the powers entrusted to him, In compliance with Article 26 of The Banking Control Law issued under Royal decree no. M/S dated 22.2.1386(11 .6.1966), Having reviewed the Memo of His Excellency the Governor of the Saudi Arabian Monetary Agency (SAMA) No. 4111MZIMA dated 13.6.1406H. proposing draft rules for enforcing the provisions of 'The Banking Control Law", Having reviewed Ministerial Decision NO.31920 dated 162.1402 H, concerning "Regulations for Money Changing Business", and Having reviewed Ministerial Decision No,31959 dated 26.4,1404 H, setting rules for the formation of the committee prescribed under Article 25 of "The Banking Control Law" to adjudge contraventions punishable under said Law, Decides the following ;

1. Approval of the rules for enforcing the provisions of "The Banking Control Law" as per the following procedure:

Firstly:
In implementation of Article 16 of "The Banking Control Law", banks shall comply with the following:
1. Non-contravention of the rules set forth by SAMA concerning the limits on loans and credit, which a bank may extend.
2. Non-contravention of the rules prescribed by SAMA concerning the extension of certain types of loans and other transactions, such as, but not necessarily exclusive of:
a. Notifying SAMA, prior to undertaking or commitment. of any loan application submitted by a non-resident entity.
b. Obtaining prior written approval of SAMA before initiating any procedure for extending any loan to a non-resident entity.
c. Obtaining the prior written approval of SAMA before inviting foreign banks to participate in any syndicated loan facilities in Saudi Riyals.
d. Obtaining the prior written approval of SAMA before participation in any syndicated loan facilities in Saudi Riyals arranged outside the Kingdom for both resident and non-resident entities.
e. Obtaining the prior written approval of SAMA before participating in any syndicated loan facilities arranged in foreign currencies for non-residents.
f. Obtaining the prior written approval of SAMA before the acquisition of, or subscription for, any securities in Saudi Riyal abroad.
g. Obtaining the prior written approval of SAMA before the acquisition of or subscription for any securities in foreign currencies abroad, with the exception of bank ownership of treasury bills and negotiable certificates of deposits.
h. Obtaining the prior written approval of SAMA before issuing and/or participation in the issue of any securities inside or outside the Kingdom.
i. Reporting to SAMA before introducing any new activities inside the Kingdom, which may entail financial obligations on the Bank.
3. Non-contravention of any of the guidelines and rules set forth by SAMA for banks for carrying on certain types of transactions for their customers such as but not necessarily exclusive of:
a. Adherence to the tariff schedule for banking services.
b. Informing government authorities of foreign guarantees issued by banks other than those included in the approved list which was supplied to the banks; and of breaches of any of the terms that should be complied with in such guarantees, in keeping with Circular NO.II/M112407 dated 5.8.1396 H of the Ministry of Finance and National Economy and any circulars that might be issued thereafter.
c. Refraining from conducting, or mediation in conducting any transaction, which might involve circumvention of the provisions of "The Banking Control Law" inside and outside the Kingdom.
d. Refraining from implementing any scheme for soliciting deposits, with the exception of current accounts and fixed-term deposits, before reporting to SAMA.
e. Refraining from carrying on any banking business with any person who is not licensed to conduct such business in accordance with the regulations in force, including money changers who are not licensed by SAMA in conformity with the Decision NO.31920 dated 1621402 H of the Minister of Finance and National Economy
4. Non-contravention of rules issued by SAMA concerning cash margins, which should be maintained against certain types of letters of credit or guarantees.
5. Non-contravention of instructions on the minimum limit of collateral between tl1e amount of loan and assets offered to secure it, which should be observed by banks as, prescribed by SAMA.

6. Non-contravention of instructions issued by SAMA on earmarking assets to be maintained by each bank within the Kingdom and their ratio to deposits liabilities.
7. Non-contravention of instructions issued by SAMA concerning bank holidays and bank business hours
8. Non-breach of provisions of The Banking Control Law and related executive rules which prohibit banks from helping or covering up others in carrying on banking or commercial business which they are not allowed to undertake, or circumvent the terms and rules of the Banking Control Law. It is also forbidden for any bank employee to request or obtain a reward for extending, or recommending the extension of credit facilities from the bank.

Secondly:
In pursuance of the provisions of Article 12 of The Banking Control Law, every bank is to observe the following:
1. No person shall be appointed a member of the Board of Directors of more than one bank. Any person who is nominated as a member of the Board of Directors of any bank shall disclose his membership in the Board of any other bank.
2. None of the following actions or practices shall be performed without prior written approval of SAMA:
a. Election of any person as a member of the Board of Directors of any bank if he had occupied a similar position in a banking concern which was liquidated, or if he had been previously removed from a similar post in any banking establishment, even if the liquidation had been made before coming into force of the " Banking Control Law" whether the banking concern was located inside or outside the Kingdom. Any person who is nominated as a member of the Board of Directors shall disclose such information.
b. Appointment of any person as a manager of a bank if he had occupied a similar position in any banking concern that was liquidated, or if had been previously removed from a similar position in any banking concern even if the liquidation or removal had occurred before coming into force of the Banking Control Law whether this banking concern was located inside or outside the Kingdom. Every person nominated, or applying for this position shall disclose such information.
3. Submission of all particulars and information requested by SAMA about persons occupying or nominated to occupy leading positions in the bank.

Thirdly:
In accordance with Article 17 of the "Banking Control Law", every bank shall observe the following.
1. Submission of the following information to SAMA in the manner it will prescribe and in accordance with instructions it will issue.
A, Monthly Statements
(A.1) A Statement of Conditions.
(A.2) Banks having branches and banking units abroad shall also submit:
-A consolidated Statement of Conditions of the bank, including its branches and units inside and outside the Kingdom,
-A separate Statement of Conditions of each branch or unit abroad,
(A.3) A statement of foreign assets and liabilities.
(A.4) A statement of banks' purchases and sales of foreign exchange.
(A.5) A statement of imports financing statistics.
B. Quarterly Statements
(B.I) Profit and loss Account Statement.
(B.2) Banks having branches and banking units abroad shall also submit a Profit and Loss Account statement for each branch or unit separately.
(B.3) A statement of deposits of government departments and agencies.
(B.4) A statement of geographiC breakdown of foreign assets.
(B.5) Quarterly balance sheet statements of the bank and its operating activities that should be published in daily newspapers four times during the financial year, (as per the rules regulating share trading transactions, before their publication)
C. Bi-annual Statements
(C.I) A statement of Classification of bank credit by economic sectors.
(C.2) A statement of maturity analysis.
(C.3) A statement of Loans and advances granted to non-residents and foreign investments
(C 4) A stalement of doubtful loans and advances.
D. Annual Statements
(D.I) Bank's annual balance sheet and clOSing statements
(D.2) Bank's detailed auditors' report on the bank's balance sheet.
(D.3) Annual report of the bank's board of Directors. Banks with branches and banking units abroad shall submit separate Balance sheet for each branch or unit, along with the detailed auditors' report.
E. Any statements related to the bank's branches and units abroad in accordance with instructions issued by SAMA in this respect.

F. A copy of the minutes report of every General Meeting of the Shareholders or the meeting of the partners, within one month from the date on which the meeting was held.
2. Requesting banks' external auditors to directly submit to SAMA any data explanations or Information requested by it on the banks' activities within the scope of their business.

Fourthly:
In pursuance of the provisions of Article 18 of the "Banking Control Law" the banks shall be fully committed to cooperate with the inspection team designated by SAMA for inspecting the bank activities. To this end, none of the bank's staff shall exercise any of the following acts or practices:
a. Obstructing the team from examining the bank's books, accounts and other documents, which the team desires to have access to for the perfom1ance of its duty
b. Refraining from producing available infom1ation and explanations requested by the team, or its deliberate concealment.
c. Withholding from the team on the commencement of its inspection breaches in the bank's activities, or concealing same deliberately.
d. Non-compliance with the recommendations and instructions issued by the team to the bank as a result of its inspection.

Fifthly:
In Implementation of Article 22 of the "Banking Control Law", if SAMA finds that a bank has failed to comply with the provisions of the Banking Control Law or its executive rules, or if a bank adopts a policy that might seriously affect its solvency or liquidity, it may take one or more of the following measures:
1. Enforce the penalties prescribed under Article 23 of The Banking Control Law.
2. Suspension or removal of any of the bank's staff who deliberately produced incorrect data. or stated inaccurate information or events.
3 Drawing the attention of the bank to the contraventions in Its business, and requesting It to rectify the situation within a time limit specified by SAMA, either in writing or through calling the bank's chairman of the Board or Directors or the chief executive officer or the general manager. If the bank fails to comply with SAMA's instructions, it may take some or all the measures indicated hereinafter against the bank.
4. Informing the chairman of the bank's Board of Directors through SAMA's representative or any other means of the necessity to invite the bank's Board of Directors to convene a meeting within a time period specified by SAMA to look into the bank's contraventions and to take necessary measures for their removal. This meeting will be attended by one or more representatives from SAMA.
5. The bank shall comply with any measures that SAMA deems necessary for the rectifying of the situation.
6. Appointment of one or more advisers by SAMA to advise the bank on the conduct of its business
7 Appointment by SAMA of a member as an observer In the bank's Board or Directors for a time period specified by SAMA. The member shall be entitled to participate in the discussions held at the meetings of the Board and record his opinion with respect to the decisions taken by the Board during such meetings
8. Taking any other measures that SAMA may deem necessary on the approval of the Minister of Finance and National economy.
2. This decision shall be notified to whom it may concern for implementation and it shall come in force from the date of its issue.
Minister of Finance and National Economy
Mohammad Abal Khail

ANNEX 8: IN DEPTH DESCRIPTION OF ML AND TF IN SHARI'AH (RELATED TO SECTION 1)

Explanation provided by KSA

Even if the term "money laundering" is not mentioned in the Shari'ah, the Islam has used terms with a meaning broader than money laundering, such as "the prohibited illegal funds" or the "prohibited profit" or the "illicit profit". The world became aware of ML as a behavioral product. Pursuers of this behavior seek to give prohibited money a lawful or legal capacity. In the 20th century, Islam has indicated its stance toward money in general and prohibited unlawful money in particular. Indeed, Islam permitted what is lawful, called for it and showed its ways, while it prohibited unpermissive profit, criminalized it and established ways for preventing it on the individual and state levels. Upon considering the forms and objectives of ML, we find that it is a cooperation in committing sins and rancor: mostly, the money of the ML results from prohibited acts such as drugs trafficking, theft and illicit activities. Cooperating with the money launderers means helping them in concealing the sources of their funds and harming the communities. The Almighty Allah said: "Help ye one another in righteousness and piety, but help ye not one another in sin and rancor" (Al-Maida: 2). It also means disobedience to the person charged with authority who has to be obeyed except when it involves disobedience to God. The Islamic or non-Islamic countries have enacted laws prohibiting ML. The person charged with authority should be obeyed when he does not involve disobedience to God. The Almighty said: "O ye who believe! obey Allah, and obey the Messenger, and those charged with authority among you." (An-Nisaa: 59). Oubada bin Al-Samet narrated saying: "We have pledged allegiance to the Messenger of Allah (PBUH) to listen and obey in ease and in hardship and that we do not dispute the matter (authority) with its people and that we stand for or speak the truth wherever we were and that in the service of Allah we would fear the blame of no one." The establishers of these laws took into consideration drawing the interest and averting the causes of corruption whether of soul or wealth. Forbidding ML aims at achieving the public interest and ensuring a safe life for people, which is no doubt a legal requirement and prescribed by the Shari'ah, and is a practical part of the general rules of the Shari'ah which ensures the humans' safety and their money. Eating up illicit money: what the money launderers benefit from their crime, is eating up illicit money. Abdulrahman bin Samrah – may Allah be pleased with him – said: The Prophet (PBUH) said:"….Oh Abdulrahman, Verily Allah forbade paradise for the flesh that grew on illicit gains, for hell is his abode." Al-Hakim said: this is a true tradition. The criminalization of ML crime is deduced from the Shari'ah from the saying of the Almighty: "And do not eat up your property among yourselves for vanities, nor use it as bait for the judges with intent that ye may eat up wrongfully and knowingly a little of (other) people's property." (Al-Baqara: 188). The verse is explicit in prohibiting obtaining and gaining money illicitly, such as bribery and theft. The Almighty said: "O ye who believe! eat not up your property among yourselves in vanities: but let there be amongst you traffic and trade by mutual good-will". (An-Nisaa: 29). There is a general legislation in this verse that prohibits dealing falsely with and manipulating the people's. It permits dealing in money among people in specific ways like trading. ML is different than trading since its dealers do not seek to earn money by permissible means, but justify their money by impersonating falsely the status of legal trade and dealing. The Almighty said: "He allows them as lawful what is good (and pure) and prohibits them from what is bad". (Al-A'raf: 157). No doubt ML is a prohibited and evil profit. In his Farewell Speech, the Prophet (PBUH) said: "O people, your blood, your wealth and your honor are sacred until the Day when you meet your Lord, as sacred as this day of yours in this month of yours in this land of yours. You will meet your Lord and He will question you about your deeds. I have conveyed (the message)." This indicates the sacredness of the Muslim's money and the prohibition of taking it illicitly. In general, this includes all financial and economic crimes, such as the ML crime. The Prophet (PBUH) said: "there will be a time when people will not care about the source of money, whether from a permissible or impermissible source".

Accordingly, Islam generally prevents persons from acquiring and collecting illicitly earned money. This is done on two levels: *i)* by explicitly prohibiting illicit money altogether and, *ii)* by identifying and prohibiting

specific venues for illicit acquisition of money. The first level is addressed in the Qur'an, which prohibits obtaining any person's money illicitly. The Qur'an reads, "And eat up not one another's property unjustly (in any illegal way e.g. stealing, robbing, deceiving, etc.), nor give bribery to the rulers (judges before presenting your cases) that you may knowingly eat up a part of the property of others sinfully" (2:188). On the second level, some specific ways of acquiring money are prohibited. Examples include the prohibition of liquor, which include the prohibition of its production, usage, carriage, selling, gaining its proceeds, and purchase. In Sunnah, the prophet explains that "He who prohibited it has prohibited its price." The same applies to theft, armed robbery, usury, prostitutions, etc.

The Islamic Shari'ah criminalizes terrorism as an antisocial crime, on which the most severe punishments should be imposed. Pursuant to the provisions of the Shari'ah, TF is considered a way leading to terrorism. It helps in committing sins and rancor: the terrorist financer is mostly a supporter for the doer of the criminal act, whether this act is committed or not, as cooperating with the terrorists means helping them in harming the communities. The Almighty said: "Help ye one another in righteousness and piety, but help ye not one another in sin and rancor" (Al-Maida: 2). It is also a disobedience to the ruler in charge of authority. The person in charge of authority should be obeyed when it does not involve disobedience to the God. The Almighty said: "O ye who believe! obey Allah, and obey the Messenger, and those charged with authority among you." (An-Nisaa: 59). Oubada bin Al-Samet narrated saying: "We have pledged allegiance to the Messenger of Allah (PBUH) to listen and obey in ease and in hardship and that we do not dispute the matter (authority) with its people and that we stand for or speak the truth wherever we were and that in the service of Allah we would fear the blame of no one". Therefore, the most severe punishments shall be enforced on TF and terrorism. There is a difference between the perpetrator of the terrorist act and TF in the provisions of the Shari'ah in terms of describing the crime or the punishment that could be imposed.

ANNEX 9: MLA STATISTICS

Statistics on the number of MLA requests received by KSA			
Request by	**Type of Request**	**Country**	**Result**
IINTERPOL	Requesting a copy of the investigations of the drugs case	Syria	Completed
CIGP	Requesting the examination of the investigations of Riyadh assaults	Switzerland	Sent to the General Investigation Authorities
Public Rights	Hearing and investigation request	Paris	The French Interpol has already been informed of the case
MOFA	ML	Turkey	Completed
Public Security	ML	Jordan	Completed
MOF	Request of investigating individuals	UAE	Completed
INTERPOL	Requesting copies of investigations of an ML case	Syria	Completed
INTERPOL	Investigating a drugs case	Syria	Completed
INTERPOL	ML	London	Completed
MOFA	Investigating a drugs case	Turkey	Completed
Prosecution Authority	Legal Assistance (Request for obtaining pictorial evidence)	Australia	In process
MOFA	Legal Assistance (Request for identifying two bodies through DNA)	Russia	In process
Public Security	ML	France	Completed
Security Affairs	Investigation request	Switzerland	In process

ANNEX 10: LIST OF PREDICATE OFFENCES (PROVIDED AND TRANSLATED BY THE AUTHORITIES OF KSA)

OFFENCE	TEXT EXTRACTED FROM THE QURAN	TEXT EXTRACTED FROM THE SUNNAH OF THE PROPHET	TEXT EXTRACTED FROM THE LAW
Being part of an organized criminal group and blackmailing	Allah Says: "The recompense of those who wage war against Allah and His Messenger and do mischief in the land is only that they shall be killed or crucified or their hands and their feet be cut off on the opposite sides, or be exiled from the land. That is their disgrace in this world, and a great torment is theirs in the Hereafter". (Al-Ma'idah 33). Allah Says: "Help you one another in virtue, righteousness and piety; but do not help one another in sin and transgression. And fear Allah. Verily, Allah is Severe in punishment". (Al-Ma'idah 2) Allah Says: "And eat up not one another's property unjustly, nor give bribery to the rulers that you may knowingly eat up a part of the property of others sinfully". (Al-Baqara 188)	The Prophet (PBUH) said: "O people! Your blood, your properties, and your honor are sacred to one another like the sanctity of this day of yours, in this (sacred) town (Mecca) of yours, in this month of yours" And: It is not permissible to take money from a Muslim unless he is fully content.	The Kingdom imposes the following penalty on any person who takes part in an organized criminal group: Article 17 of the Anti-Money Laundering Law stipulates that the perpetrator of a money-laundering offense shall be subject to a jail penalty not exceeding 15 years and a fine of no more than SR 7,000,000 if the offence is committed through an organized gang. Article 37 of the Anti-Narcotic Drugs and Psychotropic Substances Law. Vienna Convention of 1988, the Palermo Convention. A number of conventions with some countries, including: 1- Security Cooperation Agreement with Iran, approved by virtue of Decree M/31 dated 6/7/1422 H. 2- Security Cooperation Agreement with Sudan, approved by virtue Decree M/5 dated 15/1/1427 H. 3- Security Cooperation Agreement with Senegal, approved by virtue of Decree M/2 dated 24/1/1419 H. 4- The Memorandum of Understanding with Italy approved by virtue of Decree M/12, dated 10/9/1417 H. 5- The Memorandum of Understanding with Britain approved by King Abdullah by virtue of cable No. 5/b/6737 dated 1/5/1410 H.
Terrorism, including financing of terrorism	Allah Says: "The recompense of those who wage war against Allah and His Messenger and do mischief in the land is only that they shall be killed or crucified or their hands and their feet be cut off on the opposite sides, or be		Article 1 of the Anti-Money Laundering Law contains the definition of a criminal activity, which is any activity sanctioned by Sharia or law including financing of terrorism and terrorist acts. And all treaties and conventions signed between the Kingdom and other countries condemn terrorism and terrorist acts, and shall be treated as the Law, since the approval thereof is issued in form of royal decrees and shall be considered as binding to the Kingdom according to the Basic Law of Governance, Articles (70) and (81) thereof.

OFFENCE	TEXT EXTRACTED FROM THE QURAN	TEXT EXTRACTED FROM THE SUNNAH OF THE PROPHET	TEXT EXTRACTED FROM THE LAW
	exiled from the land. That is their disgrace in this world, and a great torment is theirs in the Hereafter". (Al-Ma'idah 33). Allah Says: "Help you one another in virtue, righteousness and piety; but do not help one another in sin and transgression. And fear Allah. Verily, Allah is Severe in punishment". (Al-Ma'idah 2)		
Human trafficking and smuggling of migrants.	Allah Says: "And force not your maids to whoredom if they desire chasistity, in order that you gain in the goods of this worldly life. And if anyone compels them, then after such compulsion, Allah is oft-forgiving, Most Merciful". (Al-Nour 33). Allah Says: "And indeed We have honoured the Children of Adam, and We have carried them on land and sea, and have provided them with lawful good things, and have preferred them above many of those whom We have created with a marked preference". (Al-Isra' 70)	The Prophet (PBUH) said: "O people! Your blood, your properties, and your honor are sacred to one another like the sanctity of this day of yours, in this (sacred) town (Mecca) of yours, in this month of yours" And: I am the enemy of three kinds of people: the one who makes a promise in My name then does not honor his promise, the one who sells a free person and keeps his value for himself, and the one who employs someone and does not pay him.	United Nations Convention Against Transnational Organized Crime (Palermo)
Sexual exploitation, including the sexual exploitation of	Allah Says: "And transgress not, Lo! Allah loveth not transgressors" (Al-Ma'idah 87).	The Prophet (PBUH) said: " No people among whom adultery and usury become openly practiced unless they have	

OFFENCE	TEXT EXTRACTED FROM THE QURAN	TEXT EXTRACTED FROM THE SUNNAH OF THE PROPHET	TEXT EXTRACTED FROM THE LAW
children.	Allah Says: "And come not near unto adultery. Lo! it is an abomination and an evil way". (Al-Isra' 32)	earned the punishment of Allah". And: "O people! Your blood, your properties, and your honor are sacred to one another like the sanctity of this day of yours, in this (sacred) town (Mecca) of yours, in this month of yours"	
Narcotic Drugs and Psychotropic Substances illegal trafficking	Allah Says: " O ye who believe! Intoxicants and gambling and idols and divining arrows are only an infamy of Satan's handiwork. Avoid it in order that ye may succeed". (Al-Ma'idah 90). Allah Says: "Prohibits them as unlawful". (Al-A'raf 157).	The Prophet (PBUH) said: "All drinks that intoxicate are unlawful (to drink)." And: Narcotic Drugs and intoxicants are forbidden among my people.	Article 3 of the Anti- Narcotic Drugs and Psychotropic Substances Law, issued by virtue of Royal Decree number M/39, dated 8/7/1426 H., specifies the criminal acts, whether through smuggling, importing, production, manufacturing, transforming, extracting, use, distribution, or cultivating, or by taking part in all of the above mentioned acts.
Illicit trade in weapons	Illicit trade in weapons is a violation of the directives of the ruling authority. Allah Says: " O ye who believe! Obey Allah, and obey the messenger and those of you who are in authority". (An-Nisa' 59). Allah Says: "Help you one another in virtue, righteousness and piety; but do not help one another in sin and transgression. And fear Allah. Verily, Allah is Severe in punishment". (Al-Ma'idah 2)		The Weapons and Ammunitions Law clarifies a number of pertinent offences in the following articles: Article 34: There shall be imposed a jail penalty of up to thirty years and a fine of up to 300,000 Riyals on any person, proved to have committed the following: a- Smuggling of war weapons and firearms, or related ammunitions or parts, into the kingdom for the purpose of disturbing its national security. b- Using , manufacturing, assembling, selling, purchasing, or holding war weapons and firearms, or related ammunitions or parts thereof for the purpose mentioned in paragraph (a) hereof. Article 35: There shall be imposed a jail penalty of up to twenty years and a fine of up to 200,000 Riyals, or any of the above, on any person, proved to have committed the following:

OFFENCE	TEXT EXTRACTED FROM THE QURAN	TEXT EXTRACTED FROM THE SUNNAH OF THE PROPHET	TEXT EXTRACTED FROM THE LAW
			a- Smuggling of weapons of war, or related parts or ammunitions, into the Kingdom for the purpose of trafficking. b- Manufacturing of weapons of war, or ammunitions thereof or spare parts, for the purpose set forth in paragraph (a) hereof. Article 36: There shall be imposed a jail penalty of up to fifteen years and a fine of up to 150,000 Riyals, or any of the above, on any person, proved to have held, owned, sold or purchased a weapon of war or any related ammunitions. Article 37: There shall be imposed a jail penalty of up to ten years and a fine of up to 100,000 Riyals, or any of the above, on any person, proved to have manufactured firearms or any related parts or ammunitions, or proved to have smuggled the same into the Kingdom for the purpose of trafficking. Article 38: There shall be imposed a jail penalty of up to five years and a fine of up to 30,000 Riyals, or any of the above, on any person, proved to have committed the following: a- Smuggling of hunting weapons, or related parts or ammunitions, into the Kingdom for the purpose of trafficking. b- Smuggling of firearms, or parts thereof or ammunitions, into the Kingdom for personal use. c- Manufacturing of hunting weapons, or related spare parts. d- Amending of the mechanism of hunting weapons, training weapons, or antiquated weapons in such a way so as to make them more dangerous. Article 39: There shall be imposed a jail penalty of up to two years and a fine of up to 7,000 Riyals, or any of the above, on any person, proved to have purchased a firearm or ammunition without license or proved to have sold any firearm or ammunition. Article 40: There shall be imposed a jail penalty of up to eighteen months and a fine of up to 6,000

OFFENCE	TEXT EXTRACTED FROM THE QURAN	TEXT EXTRACTED FROM THE SUNNAH OF THE PROPHET	TEXT EXTRACTED FROM THE LAW
			Riyals, or any of the above, on any person, proved to have held a firearm or ammunition without license. Article 41: There shall be imposed a jail penalty of up to one year and a fine of up to 5,000 Riyals, or any of the above, on any person, proved to have committed the following: 1- Using the licensed firearm by holding and owning the same for a purpose other than for which it was licensed. 2- Using a firearm for hunting, even though it was licensed. 3- Owning a hunting weapon or ammunition without license. 4- Allowing others to use the licensed firearm, or letting others use the firearm as a result of negligence. 5- Transporting or helping transport non-licensed weapons and ammunitions. 6- Opening a place for training on hunting weapons or training without license. 7- Working in the repair of weapons without license. 8- Repairing non-licensed weapons. 9- Manufacturing the ammunitions of hunting weapons. 10- Smuggling training weapons, by wholesale, into the Kingdom. 11- Smuggling hunting weapons or related ammunitions into the Kingdom for personal use. 12- Smuggling antiquated weapons for the purpose of trafficking. 13- Violating any of the licensing conditions in terms of importation, sale, holding, or repair. Article 42: There shall be imposed a jail penalty of up to six months and a fine of up to 3,000 Riyals, or any of the above, on any person, proved to have information about non-licensed weapons trafficking or smuggling operations, and has not notified the competent authorities of the same. Article 43: There shall be imposed a penalty of up to 2,000 Riyals on any person: a- Whose importation, sale, purchase, repair or training license validity has expired, and has

OFFENCE	TEXT EXTRACTED FROM THE QURAN	TEXT EXTRACTED FROM THE SUNNAH OF THE PROPHET	TEXT EXTRACTED FROM THE LAW
			continued practicing the licensed activity without submitting a license renewal application within three months from the expiry date thereof. b- Who cancels the holding or owning license granted to him, and does not dispose of the weapon, or notify the competent authorities of the same within three months from the date of cancellation. c- Who smuggles training weapons for personal use. d- Who is aware of the losing, stealing, or deterioration of his weapon, and does not notify the competent authorities of the same. e- Who violates any other provision of the present law or pertinent regulations and does not fall under the penalties stated therein. Article 44: There shall be imposed a penalty of up to 1,000 Riyals on any person who holds his licensed firearm at the places where and at times during which the holding of weapons is forbidden. A list of such places and times is specified in the implementing regulations. Article 45: There shall be imposed a penalty of up to 1,000 Riyals on any person, proved to have his firearm stolen or have lost the same as a result of negligence; the person shall be also forbidden from obtaining a new license for any weapon for a period of two years from the date of penalty enforcement. Article 46: There shall be imposed a minimum penalty of 100 Riyals for each year of delay and shall not exceed 500 Riyals as a maximum on any person: a- Whose weapon holding or owning license the validity of which is over, and who does not submit a renewal application thereof within three months from the expiry date thereof. b- Who gets, by legacy or will, a licensed weapon and does not notify the competent authorities of the same within three months of the occurrence of the situation. Article 47: Any person proved to have disposed of weapons and ammunitions allowed to cross the Kingdom, through selling or offering the same inside the Kingdom, shall be subject to the

OFFENCE	TEXT EXTRACTED FROM THE QURAN	TEXT EXTRACTED FROM THE SUNNAH OF THE PROPHET	TEXT EXTRACTED FROM THE LAW
			penalties imposed on smugglers of weapons based on their kinds. Article 48: There shall be imposed the prescribed penalty on any person, proved to have taken part in committing of any of the violations indicated herein. Article 49: Penalties – excluding imprisonment – provided for herein shall be imposed on institutions, companies or any entity proved to have violated any of the provisions set forth in the present law.
Illegal trading in stolen goods and other goods	Allah Says: "As for the thief, both male and female, cut off their hands. It is the reward of their own deeds, an exemplary punishment from Allah. Allah is Mighty, Wise". (Al-Ma'idah 38). Since stealing is forbidden, then trading in anything stolen is considered as forbidden according to Sharia.	The Prophet (PBUH) said: "O people! Your blood, your properties, and your honor are sacred to one another.	The penalty imposed on such kinds of offences is stipulated by the Sharia; accordingly, there is no necessity to promulgate a specific law.
Corruption and bribery	Allah Says: "Those who break Allâh's Covenant after ratifying it, and sever what Allâh has ordered to be joined, and do mischief on earth, it is they who are the losers. Allah Says: "We will add torment to the torment because they used to spread corruption" Allah Says: " And when it is said unto them: Make not mischief in the earth, they say: We are peacemakers only" and " Are not they indeed the mischief-makers? But they perceive not". (Al-Baqara 11-12).	The Prophet (PBUH) said: Curse of Allah on bribers, bribed and bribees.	The Anti-Bribery Law issued by virtue of Royal Decree No. M/36, dated 26/12/1413 H, consists of 23 articles, and it was published in Umm al-Qura newspaper, Jeddah, issue 3414, dated 3/3/1413 AH. It aims at addressing all aspects of bribery and power abuse, and imposing penalties on the aforementioned offence and all related types. Article 1 of the above mentioned Law provided for the following: "Any civil servant who asks for himself or for others, accepts or takes a gift for accomplishing any of his work duties, even if the aforementioned duty is legal, shall be considered as a bribe taker, and shall be subject to imprisonment and a penalty of up to one million Riyals, or any of the above; and the intention of the employee of not executing the work he promised shall not be taken into consideration in the existence of the offence.

OFFENCE	TEXT EXTRACTED FROM THE QURAN	TEXT EXTRACTED FROM THE SUNNAH OF THE PROPHET	TEXT EXTRACTED FROM THE LAW
	Allah Says: " O ye who believe! Betray not Allah and His messenger, nor knowingly betray your trusts". (Al-Anfal 27)		
Fraud	Allah Says: "The way (of blame) is only against those who oppress mankind, and wrongfully rebel in the earth. For such there is a painful doom". (Ash-Shura 42)	The Prophet (PBUH) said: Who cheats us shall not be considered one of us. The Prophet (PBUH) said: Who deceives Muslims is not of them.	Article 1 of the Anti-Commercial Fraud Law provides for the following: "There shall be imposed a penalty of 5,000 to 100,000 Riyals, or the closing of the store of one week minimum and 90 days maximum, or both, on any person who cheats or attempts to cheat or dupe, in any way whatsoever, in any of the following matters: a- The good itself, its nature, type, kind, elements or main features. b- The source of the good. c- The amount of the good, whether in terms of weight, measure, gauge, number, capacity or caliber, or the using of any method or way to falsify the same. d- The description, advertising, or presentation of the good in a way showing false or cheating information.
Currency counterfeit	Considered a form of transgression on property, protected by the Sharia through the protection of the five fundamentals.		The Anti-Forgery Law issued by virtue of Royal Decree No. 12, dated 1379 H. and the penalty article of Royal Decree No M/38, dated 23/10/1421 H., provide for a jail penalty of 5 years minimum and 25 years maximum, and a fine of 30000 Riyals minimum and 500,000 Riyals maximum.
Product forgery and Pirating	Allah Says: "And transgress not, Lo! Allah loveth not transgressors" (Al-Ma'idah 87). Allah Says: "And eat up not one another's property unjustly " (Al-Baqara 188).	The Prophet (PBUH) said: Who cheats us shall not be considered one of us. The Prophet (PBUH) said: It is not permissible to take money from a Muslim unless he is fully content.	Law against Computer Crimes, M/79, dated 7/3/1428 AH. Copyright Protection Law, M/41, dated 2/7/1424 AH. Paris Convention for the Protection of Industrial Property and Berne Convention for the Protection of Literary and Artistic Works, joined by virtue of Decree M/180, dated 4/7/1424 H.
Environment crimes	Allah Says: "Work not confusion in the earth after the fair ordering (thereof), and call on Him in fear and hope". (Al-A'raf 56)	The Prophet (PBUH) said: Do not kill a woman or infants or elderly people, and do not burn palm trees or uproot trees or	The General Law of Environment provides for criminating some acts pursuant to the following articles: Article 13: Any person who starts practicing any service or production activities or others shall abide by taking necessary measures to ensure the following: 1- The non-pollution of the surface, ground or coastal water by solid or liquid waste, whether

OFFENCE	TEXT EXTRACTED FROM THE QURAN	TEXT EXTRACTED FROM THE SUNNAH OF THE PROPHET	TEXT EXTRACTED FROM THE LAW
		destroy houses.	directly or indirectly. 2- Protecting and avoiding the deterioration and pollution of the soil and the land. 3- Reducing noise, especially when operating machines, equipment, warning machines and loudspeakers, and never exceeding the limits of the authorized environmental standards stipulated in the executive regulations. Article 14: 1- It is forbidden to allow the entry of dangerous, toxic or radioactive waste into the KSA, including its territorial waters or the exclusive economic zone. 2- Any person in charge of producing, transporting, storing, recycling or processing, or disposing of toxic, dangerous or radioactive materials shall abide by the procedures and controls set forth in the executive regulations. 3- It is forbidden that ships or others have their harmful pollutants or any dangerous, toxic or radioactive waste thrown in the territorial waters or the exclusive economic zone.
Killing and causing serious body injuries	Allah Says: "And do not kill anyone whose killing Allah has forbidden, except for a just cause ". (Al-Isra' 33). Allah Says: "And whoever kills a believer intentionally, his recompense is Hell to abide therein; and the Wrath and the Curse of Allâh are upon him, and a great punishment is prepared for him ". (An-Nisa' 93). Allah Says: "Life for life, eye for eye, nose for nose, ear for ear, tooth for tooth, and wounds equal for equal". (Al-Ma'idah 48).	The Prophet (PBUH) said: "Whoever kills someone with whom we have a treaty, he would not find the smell of Paradise, which a walker can smell when he is forty years away." The Prophet (PBUH) said: The believer will stay on the right religious track as long as he did not commit any forbidden act of killing. The Prophet (PBUH) said: "O people! Your blood and your properties, are sacred to one another".	The penalty imposed on such kinds of offences is stipulated by the Sharia; accordingly, there is no necessity to promulgate a specific law.

OFFENCE	TEXT EXTRACTED FROM THE QURAN	TEXT EXTRACTED FROM THE SUNNAH OF THE PROPHET	TEXT EXTRACTED FROM THE LAW
Kidnapping, chaining, and taking hostages illegally	This act is a transgression against faithful innocent people, and transgression against innocent people is not permissible. Allah Says: "And transgress not. Verily, Allah does not like the transgressors" (Al-Ma'idah 87). And Allah says "The recompense of those who wage war against Allâh and His Messenger and do mischief in the land is only that they shall be killed or crucified or their hands and their feet be cut off from opposite sides, or be exiled from the land. That is their disgrace in this world, and a great torment is theirs in the Hereafter. (Al-Ma'idah 33).		The International Convention opposing the taking of hostages, joined by the Kingdom, by virtue of Royal Decree No. M/21, dated 15/7/1410 AH.
Robbery and burglary	Allah Says: "As for the thief, both male and female, cut off their hands. It is the reward of their own deeds, an exemplary punishment from Allah. Allah is Mighty, Wise." (Al-Ma'idah 38).	The Prophet (PBUH) said: Curse of Allah on the thief, the thief who steals an egg shall have his hand cut off, and the thief who steals the rope shall have his hand cut off. The Prophet (PBUH) said: "No thief who steals is a believer so long as he commits theft"	The penalty imposed on such kinds of offences is stipulated by the Shari'ah; accordingly, there is no necessity to promulgate a specific law.
Smuggling	Allah Says: " O ye who believe! Obey Allah, and obey the messenger and those of you who are in authority" (An-Nisa' 59) And: " Help ye one another in		Article (142) of the Unified Customs Law provides for the following: "Smuggling is the act of entry or attempted entry into the country, or getting out or attempted getting out of goods from the country in a way violating the applicable laws, without paying all or part of the custom duties, or by breaching the restriction or banning rules stipulated in the present law and other laws.

OFFENCE	TEXT EXTRACTED FROM THE QURAN	TEXT EXTRACTED FROM THE SUNNAH OF THE PROPHET	TEXT EXTRACTED FROM THE LAW
	righteousness and piety, but help ye not one another in sin and rancour" (Al-Ma'idah 2)		
Blackmailing	Blackmailing is criminated by the Shari'ah, whether it was related to money or people, for any abuse of the five fundamentals, namely "the soul, the religion, the honor, the mind, the money" shall be considered as an offence. Allah Says: "And transgress not. Verily, Allah does not like the transgressors" (Al-Ma'idah 87). Allah Says: "And eat up not one another's property unjustly "(Al-Baqara 188).	The Prophet (PBUH) said: "O people! Your blood, your properties, and your honor are sacred to one another like the sanctity of this day of yours, in this (sacred) town (Mecca) of yours, in this month of yours" The Prophet (PBUH) said: It is not permissible to take money of a Muslim unless he is fully content.	
Counterfeit	Allah Says: Avoid dirt from idolaters and avoid false statements.	The Prophet (PBUH) said: Shall I inform you of the biggest of the great sins?" We said, "Yes, O Allah's Apostle" He said, "To join partners in worship with Allah: to be undutiful to one's parents." The Prophet sat up after he had been reclining and added, "And I warn you against giving forged statement and a false witness; I warn you against giving a forged statement and a false witness." The Prophet kept on repeating that warning	Article (5) of the Anti-Forgery Law, No. 114, dated 26/11/1380 H., stipulates the following: There shall be imposed a jail penalty of one to five years on any employee who has committed, during his work time, any counterfeit act by issuing a document or writing a paper that has no original, or copied intentionally from the original, or has signed, sealed or put his fingerprint on the same; or has gotten rid of an official document or proving documents, whether partially or completely; or has counterfeited an academic certificate or a public or private service certificate; or has missigned in blank, or has proven the accuracy of facts, statements and testimonies, or noted statements and information other than the ones said by the concerned, or has changed or falsified official papers, records and documents by scratching, striking off, or mentioning untrue and incorrect names, or has changed the numbers and the official records through changing, removal or falsification.

OFFENCE	TEXT EXTRACTED FROM THE QURAN	TEXT EXTRACTED FROM THE SUNNAH OF THE PROPHET	TEXT EXTRACTED FROM THE LAW
		till we wished that he would stop.	
Pirating	Allah Says "The recompense of those who wage war against Allah and His Messenger and do mischief in the land is only that they shall be killed or crucified or their hands and their feet be cut off on the opposite sides, or be exiled from the land. That is their disgrace in this world, and a great torment is theirs in the Hereafter". (Al-Ma'idah 33).		The Kingdom applies pertinent treaties and conventions according to Articles (70) and (81) of the Governance Law.
Insider trading and markets manipulation	Allah Says: "And eat up not one another's property unjustly " (Al-Baqara 188).	The Prophet (PBUH) said: "O people! Your blood, your properties, and your honor are sacred to one another like the sanctity of this day of yours, in this (sacred) town (Mecca) of yours, in this month of yours"	Capital Market Law, Royal Decree number M/30, dated 2/6/1424 AH. Article 49: a- Any person shall be considered in violation of this Law if he intentionally does any act or involves in any action which creates a false or misleading impression of the market, the prices or the value of any security for the purpose of creating that impression or thereby encouraging others to buy, sell or subscribe for such security or to refrain from doing so or to induce them to exercise, or refrain from exercising any rights conferred by such security. b- The Authority shall set out rules determining the acts and practices that constitute violations of paragraph (a) of this article. The rules shall define acts and rules excepted from the application of the terms of paragraph (a) of this article. The powers of the Authority provided for in this paragraph shall include the power to set forth the rules, define the circumstances and procedures aiming at stabilizing the prices of securities offered to the public, and the manner in which and the period during which these actions must be taken. c- The following acts and practices shall be among those which shall be considered types of fraud that are prohibited by paragraph (a) of this article above: 1- To perform any act or practice aiming at creating a false or misleading impression of an active trading in a security as contrary to the reality. These acts and practices shall include, but not be limited to the following: a- Concluding securities transactions which do not involve a true transfer of ownership

OFFENCE	TEXT EXTRACTED FROM THE QURAN	TEXT EXTRACTED FROM THE SUNNAH OF THE PROPHET	TEXT EXTRACTED FROM THE LAW
			thereof. b- Entering a buy order or orders of a particular security with prior knowledge that a similar order or orders of the same size, price and timing for the sale of the same security has been or will be entered by a party or different parties. c- Entering a sale order or orders of a particular security with prior knowledge that a similar order or orders of the same size, price and timing for the purchase of the same security has been or will be entered by a party or different parties. 2- To affect, individually or with others, the price of a particular security or securities traded on the Exchange through executing a series of transactions in such security or securities creating actual or apparent active trading or causing an increase or decrease in the prices of such securities, for the purpose of attracting third parties to buy or sell securities as the case may be. 3- To affect, individually or with others, through executing any series of transactions such as buying or selling, or buying and selling a security traded on the Exchange for the purpose of pegging or stabilizing the price of such security in violation of the rules set forth by the Authority for the safety of the market and the protection of investors. Article 50: a- Any person who obtains, through family, business or contractual relation, insider information (hereinafter an "insider") is prohibited from directly or indirectly trading in the security related to such information, or to disclose such information to another person with the expectation that such person would trade in the aforementioned security. Insider information means information obtained by the insider and which is not available to the public, and has not been disclosed, and such information is of the type that a normal person would realize that in view of the nature and content of this information, its release and availability would have a material effect on the price or the value of security related to such information, and the insider knows that such information is not generally available and that, if available, it would have a material effect on the price or value of such security. b- No person may purchase or sell a security based on information obtained from an insider while knowing that such person, by disclosing such insider information related to the security, has violated paragraph (a) of this article. c- The Authority has the power of establishing the rules for specifying and defining the terms

OFFENCE	TEXT EXTRACTED FROM THE QURAN	TEXT EXTRACTED FROM THE SUNNAH OF THE PROPHET	TEXT EXTRACTED FROM THE LAW
			provided for under paragraphs (a) and (b) above, and such acts or practices which the Authority deems appropriate to exclude from their application, as may be required for the safety of the market and the protection of investors. Article 57: a- Any person who violates Article 49 of the present Law or any of the regulations or the rules issued by the Authority pursuant to the said Article by engaging in an act or transaction for the purpose of intentionally manipulating the price of a security, or participating in such act or transaction, or is responsible for a person who executes such act or transaction, shall be liable for damages to any person who purchases or sells the security, the price of which has been adversely affected significantly by such a manipulation, for the amount such person's purchase or sale price was so affected. b- The due damages under this article from any defendant, and the rights of indemnity and contribution among the persons responsible shall be estimated in a manner that is consistent with the provisions of paragraph (e) of Article 55 hereof. c- In addition to the penalties and financial compensation provided for under this Law, the Committee may, based on a claim filed by the Authority, sentence the persons who violate Articles 49 and 50 to up to five years' imprisonment. Article 59: a- If it appears to the Authority that any person has involved, is involving, or is about to involve in acts or practices that violate any of the provisions set forth herein, or in the regulations or rules issued by the Authority, or the regulations of the Exchange, it shall have the right to bring a legal action against him before the Committee to get an order for the appropriate sanction. The sanctions include the following: 1- Warning the person concerned. 2- Obliging the person concerned to cease or refrain from carrying out the act in question in the suit. 3- Obliging the person concerned to take necessary steps to avert the violation, or to take necessary corrective steps to address the results of the violation. 4- Indemnifying the persons who have suffered damages as a consequence of a violation that has occurred, or obliging the violator to pay to the Authority's account the gains realized

OFFENCE	TEXT EXTRACTED FROM THE QURAN	TEXT EXTRACTED FROM THE SUNNAH OF THE PROPHET	TEXT EXTRACTED FROM THE LAW
			as a consequence of such violation. 5- Suspending the trading in the security. 6- Barring the violating person from acting as a broker, portfolio manager or investment advisor for a period of time as necessary for the safety of the market and the protection of investors. 7- Issuing a property writ of attachment and execution. 8- Travel ban. 9- Barring from working with companies, the securities of which are traded on the Exchange. b- The Authority may, in addition to taking the actions provided for under paragraph (a) above, request the Committee to impose a fine on the persons responsible for any intentional violation of the provisions of this Law, pertinent implementing regulations, the rules of the Authority and the regulations of the Exchange. As an alternative to the foregoing, the Board may impose a certain fine on any person responsible for any violation of the provisions of this Law, pertinent implementing regulations, the rules of the Authority and the regulations of the Exchange. The fine that the Committee or the Board may impose shall not be less than SR 10,000 and shall not exceed SR 100,000 for each violation committed by the defendant. Art. 49: Offence of Markets Manipulation. Art. 50: Trading Based on Insider Information.