FATF

MENA FATF
مينا فاتف
GAFIMOAN

Anti-money laundering and counter-terrorist financing measures

Kingdom of Saudi Arabia

Mutual Evaluation Report

September 2018

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CTF) standard.

For more information about the FATF, please visit the website: **www.fatf-gafi.org.**

For more information about MENAFATF, please visit the website: **www.menafatf.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

This assessment was adopted at the joint FATF-MENAFATF Plenary meeting in June 2018.

Citing reference:

FATF-MENAFATF (2018), *Anti-money laundering and counter-terrorist financing measures – Saudi-Arabia,*
Fourth Round Mutual Evaluation Report, FATF, Paris
http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-saudi-arabia-2018.html

Photo Credit - Cover: © Saudi Arabian Monetary Authority (SAMA).

Table of contents

Executive Summary

1. This report provides a summary of the anti-money laundering and countering the financing of terrorism (AML/CFT) measures in place in the Kingdom of Saudi Arabia at the date of the on-site visit (8-23 November 2017). It analyses the level of compliance with the FATF 40 Recommendations, the level of effectiveness of its AML/CFT system, and makes recommendations on how the system could be strengthened.

Key Findings

- Inter-agency policy coordination and cooperation is a significant strength of the Saudi system. Saudi Arabia has developed a good understanding of its ML and TF risks through its national risk assessments, using a robust process and a wide range of information. Saudi authorities have introduced a number of measures to address specific risks identified prior to the recent NRAs.
- The FIU is not conducting sophisticated financial analysis to effectively support investigations, in particular those into more complex cases of ML. The analysis provided by the FIU is straightforward and single-layered, based mainly on organising and compiling information from available databases. Nevertheless, a wide variety of information is available and competent authorities regularly use financial intelligence in the course of their investigations.
- Saudi Arabia is not effectively investigating and prosecuting individuals involved in larger scale or professional ML activity. Investigations are often reactive, and tend to be straightforward, unsophisticated, and single-layered. Prosecutions are mostly for the self-laundering offence, with individuals convicted when they are unable to prove the source of funds. ML investigations have significantly increased in recent years, but remain too low.
- Saudi Arabia is not effectively confiscating the proceeds of crime. Authorities are not routinely attempting to trace and confiscate the instrumentalities and proceeds of crime, and have not been able to repatriate any criminal proceeds from another country over the period 2013-16, despite the large majority of proceeds generated in Saudi Arabia are estimated to leave the country. The amounts of

proceeds of crime seized and confiscated domestically within Saudi Arabia have been increasing, but are still low.

- Saudi Arabia has demonstrated an ability to respond to the dynamic terrorism threat it faces in country. Saudi Arabian authorities have the training, experience and willingness to pursue terrorist financing investigations in conjunction with and alongside terrorism cases. Financial investigations are routinely carried out, and TF cases are generally identified during terrorism-related investigations conducted by Mabaheth, leading to an exceptional number of investigations and convictions.
- Saudi Arabia has an established legal framework and co-ordination process for implementing UN targeted financial sanctions (TFS) on terrorism without delay, and regularly makes use of TFS domestically. However, Saudi Arabia makes far greater use of financial restrictions imposed on a person through criminal procedures and watch-list mechanisms, which lack legal safeguards and are not publicly available. On proliferation financing, the mechanisms in place to implement TFS and prevent sanctions evasion are weak.
- Saudi Arabia conducts comparatively intensive supervision of the higher-risk sectors in accordance with a risk-based approach, and has done a great deal of outreach with regulated entities to communicate their new obligations. These efforts have resulted in a significant improvement in compliance with the AML/CFT requirements.
- AML/CFT preventive measures in the financial sector are strong and well established. Major FIs including banks, securities and financing companies, have a solid understanding of the ML/TF risks they face, and a good level of implementation of the risk-based approach; although the level of implementation is not so strong among smaller DNFBPs, and STR reporting remains a concern for all sectors.
- Saudi Arabia can and does respond to incoming requests for mutual legal assistance, but does not effectively seek international co-operation from other countries to pursue money laundering and the proceeds of crime. On terrorist financing, Mabaheth clearly does prioritise international co-operation, both inbound and outbound, and provided good examples of using international law enforcement co-operation.

Risks and General Situation

2. Saudi Arabia faces a high and diverse risk of terrorism financing, linked to terrorism committed both within Saudi Arabia, and to countries experiencing conflicts within the region. The risk of terrorism and terrorist financing within Saudi Arabia is linked to the presence of cells of Al Qaeda, ISIS, affiliates, and other groups. The number of foreign fighters is high, with estimates of over 3,000 departures between January 2000 and February 2018. Saudi Arabia also faces a high risk of terrorist acts carried out in Saudi Arabian territory.

3. The economy of the Kingdom is dominated by petroleum activities: Saudi Arabia is the largest exporter of petroleum, and the sector accounts for 45% of GDP.

Saudi Arabia is generally seen as a conservative country and an unattractive location for laundering international proceeds because of its relatively small financial and commercial sectors, limitations on direct foreign investment and participation in the corporate sector, and restrictions on access by foreigners to the financial and non-financial markets. The financial sector and DNFBP sectors in Saudi Arabia are relatively small, and primarily serve domestic customers. The remittances sector is an exception: over a third of the resident population in Saudi Arabia was born outside the Kingdom, which has the second highest total outflows of remittances in the world after the US, approximately $38.8bn for the year to April 2017.

4. The overall proceeds of crime generated in Saudi Arabia are estimated to be approximately USD 12 - 32 billion; based on IMF and UNODC research on the proceeds of crime as a proportion of GDP.[1] This range is consistent with Saudi Arabia's risk profile and the Saudi NRA for ML. Saudi authorities estimate the main proceeds-generating crimes in Saudi Arabia to be illicit trafficking in narcotics, corruption, and counterfeiting and piracy of products. Between 70 and 80 per cent of domestic proceeds of crime are estimated to flow out of the Kingdom, while the balance remains in the country.

Overall level of Effectiveness and Technical Compliance

5. Saudi Arabia's AML/CFT framework has undergone fundamental changes since 2010. In late 2017, Saudi Arabia passed comprehensive revisions of its Anti Money Laundering Law (AMLL) and Law on Terrorism Crimes and Financing (LTCF). The new laws were adopted on 24 October 2017 (AMLL) and 1 November 2017 (LTCF), immediately before the on-site visit. Saudi Arabia's National Risk Assessments were adopted in August 2017, and a national Strategy and accompanying Action Plan were adopted in the same period. Further changes to the administrative system were in progress in November 2017, during the on-site visit (including structural changes at the Public Prosecution, and the move of the FIU from the Ministry of Interior to a new ministry, the State Security Presidency). The revised laws address deficiencies identified in the 2010 Mutual Evaluation, implement new requirements added to the revised FATF Recommendations in 2012, address the conclusions of the NRAs, and correct deficiencies identified in the first draft of the TC analysis prepared for the current evaluation. In terms of technical compliance, the results of the new laws have been very positive: Saudi Arabia has brought its' legal system into line with the up-to-date FATF Recommendations, and has successfully addressed almost all of the deficiencies which were present previously.

6. In terms of effectiveness, Saudi Arabia achieves substantial results on risk understanding and mitigation; on combating terrorist financing (through both law enforcement and administrative measures); and on supervision. Serious problems affect the investigation of money laundering; the confiscation of the proceeds of crime, international co-operation, and proliferation financing.

---

1 The UNODC estimates that all criminal proceeds, excluding tax evasion, amounts to 2.3 to 5.5 per cent of global GDP. This figure is consistent with the 2 to 5 per cent range previously produced by the International Monetary Fund to estimate the scale of money-laundering. See http://www.unodc.org/unodc/en/press/releases/2011/October/unodc-estimates-that-criminals-may-have-laundered-usdollar-1.6-trillion-in-2009.html.

7. The new laws, regulations, and institutional/administrative framework mean that the AML/CFT framework which is the basis for the effectiveness assessment is significantly different from the framework assessed in the technical compliance annex. It has not been possible to assess the effectiveness with which Saudi Arabia is implementing the obligations which were introduced for the first time in November 2017, and in many places the effectiveness analysis highlights deficiencies or gaps which have already been addressed through the new laws, or provides recommended actions which ask Saudi Authorities to implement the new laws or continue new policies. As a result, much of the analysis in the main report on effectiveness is based on activities under the old laws and regulations while the TC annex reflects the new laws and regulations.

National AML/CFT Policies and Co-ordination (Chapter 2: IO1; R.1, R.2, R.33)

8. Saudi Arabia has a solid understanding of its ML and TF risks, based on a robust risk assessment process and a wide range of information. Saudi authorities have produced two parallel National Risk Assessments (NRAs) of ML and TF risks. The ML risk assessment identifies the main proceeds-generating offences, and laundering methods - primarily through transfers to other countries through cash, FIs, and trade-based laundering. Authorities also identify banks, money remitters, and dealers in precious metal and stones (DPMS) as the highest risk sectors. Some elements of the ML risk assessment are not fully developed, including the laundering of proceeds after they have been moved out of Saudi Arabia and the potential for more sophisticated forms of money laundering within Saudi Arabia.

9. Saudi Arabia has a very good understanding of its TF risks. The TF NRA considered the risks associated with countries, sources of funds, transportation methods, routes, and entry points. The assessment looked specifically at the financing associated with FTFs, terrorists and groups within Saudi Arabia and in other countries. The assessment benefited from analysis of more than 1,700 TF investigations undertaken by Saudi authorities since 2013, providing a uniquely rich pool of information as a basis for the analysis.

10. Inter-agency policy co-ordination and co-operation is a significant strength of the Saudi system. Saudi Arabia has a strong and well-established institutional framework for co-ordination, based on the Anti Money Laundering Permanent Committee and the Permanent Committee for Counter Terrorism.

11. Saudi authorities have introduced a number of measures to address risks identified prior to the recent NRAs. These include specific measures to mitigate ML and TF risks to NPOs and the remittances sector; to reduce the use of cash and the risks associated with the Hajj and Umar pilgrimages; and to combat corruption. Saudi Arabia has been quick to reflect the results of the risk assessments in its legal framework, passing comprehensive new AML and CFT laws in October and November 2017. However, authorities had not yet had sufficient time prior to this assessment to fully reflect their findings in national policies or in the objectives or practices of individual agencies.

Legal system and Operational Issues (Chapter 3: IOs 6-8, R.3, R.4, R.29-32)

12. Saudi Arabia has devoted significant resources to support financial investigation, distributed across the FIU and other law enforcement agencies. The

analysis provided by the FIU is straightforward and single-layered, based mainly on organising and compiling information from available databases and reporting entities. This is the result of a number of factors, including inadequate IT systems. As a result, the SAFIU is not conducting sophisticated financial analysis to effectively support investigations, in particular those into more complex cases of ML. The FIU has access to a wide range of databases, but analysts have to manually search each of them, and the FIU can only retrieve additional information from some reporting entities indirectly, via the supervisor. Specialised IT tools are not available: the main trigger that initiates investigation is the presence of a criminal record, rather than the detection of financial red flags or patterns of activity. Decisions not to follow-up on STRs are not always based on an appropriate methodology, with some STRs archived on the basis of the low value of transactions, although the outcome of the NRA will be used as means to help decide which STRs to archive. The relatively low proportion of staff devoted to analysis at the SAFIU, the long time taken to process STRs, the low level of reporting from non-bank sectors, the fact that STR reporting and dissemination is done on paper, and weaknesses in international co-operation all contribute to the weakness of the FIU.

13. Outside the SAFIU, law enforcement authorities and other competent authorities across Saudi Arabia do regularly use financial intelligence and other relevant information as part of their investigations into money laundering, predicate offences, and terrorist financing, and collaborate well. Law enforcement agencies have access to a wide range of databases, and in some cases conduct financial analysis. Trends are understood to some extent.

14. Saudi Arabia has a legal framework that provides it with an adequate basis to investigate and prosecute ML activities, and displays a number of positive elements: ML investigations have significantly increased in recent years; financial investigations are often conducted alongside the investigation of proceeds-generating offences; and awareness-raising activities have been organised by the Public Prosecution in order to encourage a consistent approach among all LEAs and OCAs. As a result of recent awareness raising and strengthened co-ordination, Saudi Arabia has increased the number of ML offences being investigated.

15. Despite these recent changes, Saudi Arabia is not effectively investigating and prosecuting individuals involved in larger scale or professional ML activity. LEAs and OCAs are not conducting a sufficient number of investigations into ML activity (whether triggered by investigations into proceeds generating predicate offences, or following the receipt of STRs from the SAFIU). Investigations are often reactive rather than proactive, and tend to be straightforward, unsophisticated, and single-layered. Prosecutions are mostly for the self-laundering offence, with individuals convicted when they are unable to prove the source of funds. This is reflected in the low number of prosecutions being sought and convictions being handed down for 3rd party money laundering. Saudi Arabia has also not demonstrated that it is pursuing cases relating to the 70-80% of proceeds which leave the jurisdiction.

16. Saudi Arabia is not effectively confiscating the proceeds of crime relative to its risks. Authorities are not routinely attempting to trace and confiscate the instrumentalities and proceeds of crime, although they are doing so in some cases. In cases where the criminal funds are located outside Saudi Arabia, the authorities have not been able to repatriate any criminal proceeds over the period 2013-16. The

amounts of proceeds of crime seized and confiscated domestically within Saudi Arabia have been increasing, but are still low and are not consistent with the country's risk profile. Deficiencies in Saudi Arabia's ability to effectively investigate and prosecute ML activity are limiting the ability of Saudi Arabia to trace and confiscate criminal proceeds. The failure to conduct co-ordinated investigations with other countries is also significantly limiting the confiscation of criminals' assets, given a large proportion of the proceeds of crime are estimated to leave the country.

17. Saudi Arabia has broad legal powers for confiscating the proceeds and instrumentalities of crime under Shari'ah. The confiscation of the objects of crime (principally narcotics) does appear as a priority. However, the identification and confiscation of proceeds is not achieved even to a relatively comparable extent.

18. At its borders, Saudi Arabia is detecting a large amount of non-declared and falsely declared cash, as well as non-declared and falsely declared gold, precious metals and stones. Saudi Arabia has also taken measures to respond to the heightened risk associated with the large numbers of individuals entering and exiting the country every year, implementing measures to limit the amounts of cash brought into the country by individuals on pilgrimage. The amounts confiscated at the border that are suspected of being related to ML, TF or a predicate offence appear relatively low, although the new powers in the 2017 AMLL may help Saudi Arabia confiscate larger quantities of currency and BNI at the border linked to ML, TF or a predicate offence

Terrorist Financing and Financing of Proliferation (Chapter 4 – IO.9-11; R.5-8)

19. Saudi Arabia has demonstrated an ability to respond to the dynamic terrorism threat it faces in country. Saudi Arabian authorities have demonstrated that they have the training, experience and willingness to pursue TF investigations in conjunction with and alongside terrorism cases. Financial investigations are routinely carried out in connection with most terrorism cases, and TF cases are generally identified during terrorism-related investigations conducted by Mabaheth. A range of investigative techniques are used to find evidence of TF activity, including preventative terrorist financing measures (mainly pertaining to FTFs), phone interceptions and social media scrutiny. The authorities have successfully identified, investigated and prosecuted a large number of TF cases within the Kingdom - including over 1,700 TF investigations, resulting in over 1100 convictions.

20. However there are some areas for improvement: there are no, or very few, convictions for "standalone" terrorist financing, that are independent from the prosecution of other terrorist-related offences, or of persons who are financing terrorism but who are not otherwise involved in the commission of terrorist act or affiliated with these terrorist groups. This includes TF cases in relation to funds raised in the Saudi Arabia for support of individuals affiliated with terrorist entities outside the Kingdom, particularly outside the Middle-East region, which remains a risk.

21. Saudi Arabia's overall strategy for fighting terrorist financing mainly focuses on using law enforcement measures to disrupt terrorist threats directed at the Kingdom and its immediate vicinity. While this is an understandable priority, the almost exclusive focus of authorities on domestic TF offences means the authorities are not prioritising disruption of TF support for threats outside the Kingdom. They are also not taking full advantage of TFS to enhance the disruptive impact of their law enforcement actions both in Saudi Arabia and beyond their borders. Saudi authorities

are particularly focused on domestic TF offences at the expense of international TF networks, which has an effect on their approach to both Immediate Outcome 9 and Immediate Outcome 10.

22. Saudi Arabia has an established legal framework and co-ordination process for implementing targeted financial sanctions (TFS) without delay under the relevant United Nations Security Council Resolutions (UNSCRs). Saudi Arabia has co-sponsored designations to the 1267 UN Committee and has partaken in de-listing and exemption requests, but has not proactively nominated individuals or entities to the UN for designation.

23. Domestically, Saudi Arabia has made significant use of designations under the UNSCR 1373 system, up through 2016 accepting 41 designation requests from foreign countries and, designating 150 individuals on its own motion. However, Saudi Arabia's 1373 designations are not public which hinders effective implementation: the largest number of freezes - - comes from financial restrictions imposed on a person through criminal procedures and watch-list mechanisms (possibly more than 3000 persons alone), which do not provide for legal processes (such as de-listing or exemption) required in the FATF standards. Even though these domestic designations are largely communicated to FIs and DNFBPs, there is no publicly available list of designees or guidance regarding implementing obligations, which hinders effective and consistent implementation.

24. Saudi Arabia's NPO sector is very small in number and tightly regulated. NPOs utilise the financial sector for virtually all their transactions, are under tight control for fundraising activities, and have highly restricted access to international transfers. In addition to these measures, Saudi Arabia has taken steps to raise awareness of TF abuse risks within the sector and the public at large. These measures have had the effect of drastically reducing the risk of terrorist financing abuse in the sector. However, NPOs continue to be treated by FIs/DNFBPs as high-risk clients for terrorist financing. In 2017 Saudi Arabia began analysing information derived from compliance visits of NPOs to implement a risk-based approach, although this is based primarily on financial integrity, and this system has not yet led to any reduction in the intensity of restrictions on lower-risk NPOs.

25. While Saudi Arabia has taken significant steps to limit its exposure to Iran and DPRK financial activity by cutting economic, financial and trade relations, the mechanisms in place to prevent sanctions evasion are weak. Saudi Arabia has an interagency framework and co-ordination mechanism that oversees the implementation of targeted financial sanctions related to proliferation financing. This technical system was enhanced with the issuance of new Implementing Regulations in November 2017. Under the system up until November 2017, implementation without delay of TFS for PF was not demonstrated. Saudi Arabia has not frozen any assets or blocked any transactions as a result of TFS related to PF, and there are no examples of inter-agency co-ordination related to proliferation financing. There are also significant delays in implementing and communicating new TFS relating to PF within both public and private sectors.

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

26. AML/CFT preventive measures in Saudi Arabia are strong and well established. The new AMLL and CTFL adopted in November 2017 further

strengthened the legal basis for AML/CFT preventive measures in Saudi Arabia; these Laws were however introduced too soon before the on-site visit to assess the level of effectiveness and implementation of the new elements within the FIs and DNFBPs.

27. Major FIs including banks, securities and financing companies, have a solid understanding of the ML/TF risks they face, and a good level of implementation of the risk-based approach thanks to the supervision and outreach efforts made by the authorities, as well as the risk assessments conducted at institutional level. They apply AML/CFT preventive measures including CDD, record keeping and identification of beneficial ownerships. However, STRs are not submitted in a timely way, and the low number of terrorist financing-related STRs reported is a major concern.

28. Money exchangers and other DNFBPs (in particular real estate agents and accountants) do not fully understand their ML/TF risks and apply mitigating measures under a risk-based approach. The awareness and implementation of AML/CFT obligations among reporting institutions has increased significantly thanks to supervisory measures in the last two years, but some sectors are still at the beginning stage and need more efforts to understand the ML/TF risks and AML/CFT obligations. Implementation of the risk-based approach remains weak among class A and class B money exchangers. Reporting of STRs is a major concern, with a low level of reporting from DNFBPs, including the higher risk sectors.

Supervision (Chapter 6 - IO3; R.26-28, R. 34-35)

29. The system in place for supervision of FIs achieves a substantial level of effectiveness: financial supervisors have a good understanding of the ML/TF risks, a sound model for risk-based supervision, and good communication and relations with their sectors. Saudi Arabia conducts comparatively intensive supervision of the higher-risk sectors in accordance with a risk-based approach, and since 2016 has done a great deal of outreach and engagement with regulated entities to communicate their new obligations and supervision arrangements, which appears to have been successful. All these efforts have resulted in a significant improvement in compliance with the AML/ CFT requirements.

30. AML/CFT obligations were applied to DNFBPs comparatively recently. For DNFBPs, outreach programmes/campaigns started in 2016, and AML/CFT focussed supervision started in early 2017. These arrangements are being further elaborated and enhanced for some DNFBPs and have to be further applied to all the obligations introduced in new laws. While the pace and intensity of recent activity is impressive, it is too early to reach a conclusion about its effectiveness.

Legal Persons and Arrangements ((Chapter 7 – IO5 R. 24-25)

31. Saudi Arabia has a system for regulating and monitoring legal persons and arrangements which is helpful in maintaining transparency and also in identifying beneficial owners. The Company Register maintained by MOCI provides the updated and accurate details of the legal ownership of commercial entities. Designated Courts have such records in respect of Waqfs and conduct verification. However, prior to November 2017, Joint-Stock Companies and Limited Partnerships did not have to report shareholder information to the Company Register.

32. Saudi Arabia applies controls on foreign ownership of companies, among other measures, that mitigate the risk of misuse of legal persons and arrangements by foreigners to some extent. Foreign legal persons who want to invest in Saudi Arabia must obtain a licence from SAGIA, who grants it after conducting verification on the ownership and control structure and the financial standing of the foreign investors.

33. Access to beneficial ownership information is also primarily through the Company Registry (and SAGIA). Around 83% of the corporate entities have only natural persons as shareholders, which allows for the matching of the legal owners themselves with the beneficial owners. Banks and other reporting entities also hold beneficial ownership information and maintain the necessary records when a legal person/arrangement has a customer relationship with them. However, the accuracy of and extent to which the information is up-to-date is not always ensured as some weaknesses still exist in banks' ongoing CDD procedures. The understanding of authorities of the risks of misuse of legal entities and arrangements does not yet seem to be sufficiently well-developed. Further, it is also not clear whether current and reliable BO information is available and accessible to competent authorities in respect Joint-stock Companies

International Cooperation (Chapter 8 - IO2; R. 36-40)

34. Saudi Arabia does not effectively seek international co-operation from other countries to pursue money laundering and the proceeds of crime. The number of outgoing requests remains low despite a recent significant increase. Several authorities have shown examples of co-operation with foreign counterparts to disrupt criminal activities, but this is limited to identifying targets in Saudi Arabia, or disrupting the physical production of drugs in other countries, not exposing their wider networks in other countries or identifying financing. Saudi authorities do not follow the money outside the borders of the kingdom, and as a result they do not exploit opportunities to investigate and disrupt transnational criminal networks involved in the supply of narcotics to a lesser extent, corruption and in money laundering, or to confiscate the proceeds of crime.

35. Saudi Arabia can and does respond to incoming requests for mutual legal assistance (but there appear to be delays in some cases). The outcome of international co-operation provided to other countries was not clear, in terms of investigations carried out on behalf of other countries and / or assets confiscated and repatriated.

36. On terrorist financing, Mabaheth clearly does prioritise international co-operation, both inbound and outbound, and provided good examples of using international law enforcement co-operation with their counterparts, especially in the conflict zones, to disrupt the threat of terrorist networks. Mabaheth relies primarily on intelligence co-operation (rather than MLA) which is effectively used to identify and disrupt terrorist threats and intercept FTFs. The use of such mechanisms may mean missing the opportunity to use criminal justice tools and powers to uncover and disrupt further elements of terrorist networks, either in Saudi Arabia or overseas. Saudi Arabia also makes significant contributions through its leading role in global and regional alliances against terrorism and its financing.

Priority Actions

37. The prioritised recommended actions for the Kingdom of Saudi Arabia, based on these findings, are:

- Saudi Arabia should prioritize the investigation of professional enablers and facilitators of ML, with a view to increasing proactive ML investigations. All investigations of major proceeds-generating crimes should include a parallel financial investigation to identify associated money laundering activity and its facilitators, and to trace and confiscate the proceeds. Saudi Arabia should improve the level of capacity, awareness and understanding of the investigative and legal tools available, and consider establishing specialised units.
- Saudi Arabia should actively seek MLA and other forms of co-operation, so that their investigations prioritise following the money and disrupting criminal networks and facilitators inside and outside Saudi Arabia's borders. Saudi Arabian authorities should pursue joint investigations with foreign jurisdictions, and should establish the capacity, expertise, and agreements needed to work with other countries to identify foreign money launderers, and to seize, repatriate and confiscate the proceeds of crime that have left the country.
- Saudi Arabia should establish a system that ensures full implementation of proliferation-related TFS by FIs and DNFBPs without delay, and address the remaining technical gaps.
- National co-ordination bodies should actively monitor the implementation of the new laws, regulations, and administrative arrangements to ensure they are well-understood and effectively implemented, and should take prompt action to address any emerging weaknesses in the context of the National Strategy and Action Plan.
- The FIU should comprehensively update its systems and processes: installing dedicated analytic tools capable of sophisticated analysis and systems for secure electronic filing of STRs and dissemination to authorities. It should establish powers and channels to access additional information from all reporting entities directly, and review its staffing and internal processes for handling cases. Enhanced and more frequent training should be provided to SAFIU analysts and LEA and OCA investigators, drawing on international best practice.
- Saudi authorities should provide more information and guidance on TF risks and typologies to raise awareness among FIs and DNFBPs, especially the high-risk sectors, and enable them to better identify TF suspicious activities, and ensure timely reporting of STRs by all reporting entities. The information and guidance should focus on high risk methods and techniques for ML and TF
- Saudi Arabia should conduct a more thorough assessment of the ML/TF risks related to the misuse of legal entities/legal arrangements, and the use of straw-men, and take appropriate and proportionate mitigation measures.
- With a goal of enhancing the impact of targeted financial sanctions to the greatest extent, Saudi Arabia should reduce reliance on financial restrictions based on watch-lists in favour of a consolidated and comprehensive list of 1373 domestic designations, which should be publicly available.

Effectiveness & Technical Compliance Ratings

Effectiveness Ratings (High, Substantial, Moderate, Low)

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

Technical Compliance Ratings (Technical Compliance Ratings (C - compliant, LC – largely compliant, PC – partially compliant, NC – non compliant)

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

MUTUAL EVALUATION REPORT

Preface

This report summarises the AML/CFT measures in place as at the date of the on-site visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the AML/CFT system, and recommends how the system could be strengthened.

This evaluation was based on the 2012 FATF Recommendations, and was prepared using the 2013 Methodology. The evaluation was based on information provided by the country, and information obtained by the evaluation team during its on-site visit to the country from 8 to 23 November 2017.

The evaluation was conducted by an assessment team consisting of:

- Ms. Rand Gharndoke, Anti Money Laundering & Counter Terrorist Financing Unit, Jordan (legal expert);
- Mr. Amr S. Rashed, Egyptian Money Laundering and Terrorist Financing Combating Unit, Egypt (law enforcement expert);
- Ms. Kate Eyerman, Department of the Treasury, United States (legal expert);
- Mr. Thomas Mathew, Reserve Bank of India, India (financial expert)
- Mr. Qipeng Xu, People's Bank of China, China (financial expert)
- Mr. Alastair Bland, Canada Revenue Agency, Canada (law enforcement expert);
- Mr. Tom Neylan, Mr. Neil Everitt, and Mr. Francesco Positano, FATF Secretariat;
- Mr. Sofiene Marouane and Ms. Shatha Ismaeel, MENAFATF Secretariat;

The report was reviewed by:

- Mr. Anders Worren (Ministry of Justice and Public Security, Norway);
- Mr. Nicola Muccioli (Agenzia Di Informazione Finanziaria, San Marino);
- Mr. Charles Nugent-Young (Department of Home Affairs, Australia); and
- Mr. Abdelrahman Al-Akhras (Financial Follow-up Unit, Palestinian Authority).

The Kingdom of Saudi Arabia previously underwent a FATF Mutual Evaluation in 2010, conducted according to the 2004 FATF Methodology. The 2010 evaluation has been published and is available at the FATF website.

That Mutual Evaluation concluded that the country was compliant with 4 Recommendations; largely compliant with 26; partially compliant with 15; and non-compliant with 4. The Kingdom of Saudi Arabia was rated compliant or largely compliant with 8 of the 16 Core and Key Recommendations.

The Kingdom of Saudi Arabia was placed in regular follow-up by MENAFATF immediately following adoption of its 3rd round Mutual Evaluation Report. Saudi Arabia was removed from the follow-up process in June 2014 on the basis that progress with all the Core and Key recommendations was equivalent to a rating of largely compliant.

CHAPTER 1. ML/TF RISKS AND CONTEXT

38. Saudi Arabia is the 5th largest country in Asia covering an area of 2 149 690 square kilometres, with extensive sea borders, and borders with eight other countries (Kuwait, Iraq, Jordan, Yemen, Oman, Bahrain, the United Arab Emirates and Qatar), two of which are currently suffering political instability (Yemen and Iraq). Saudi Arabia has a population of around 32 million (2016).[2] Over a third of the resident population was born outside Saudi Arabia, with the largest proportion comprising Asian expatriates. Recently, the number of foreigners increased with the arrival of refugees from Syria and Yemen.[3] Saudi Arabia receives a significant number of visitors, with more than 10 million visitors over the course of year and 2 million at specific points in the calendar for pilgrimages.

ML/TF Risks and Scoping of Higher Risk Issues

Overview of ML/TF Risks

39. The overall proceeds of crime generated in Saudi Arabia are estimated to be approximately USD 12 – 32 billion; based on IMF and UNODC research on the proceeds of crime as a proportion of GDP.[4] This range is broadly consistent with Saudi Arabia's risk profile and with the Saudi NRA for ML. The NRA for ML estimates the crimes which generate the largest share of proceeds are: illicit trafficking in narcotic drugs and psychotropic substances (31%), corruption (22%), counterfeiting and piracy of products (21%), and customs smuggling (8%). Smuggling and production of alcoholic drinks, fraud, human trafficking and tax evasion, in addition to other crimes, make up the remaining limited sources of proceeds.

40. The ML risk assessment estimates that about 71% of these proceeds are associated with organised criminal groups,[5] with 53% associated with transnational groups and 47% domestic groups. It considers that between 70 and 80 percent of domestic proceeds of crime flow out of the Kingdom, while the balance remains in the

2 The General Authority for Statistics, Kingdom of Saudi Arabia. https://www.stats.gov.sa/en/5305

3 NRA

4 The UNODC estimates that all criminal proceeds, excluding tax evasion, amounts to 2.3 to 5.5 per cent of global GDP. This figure is consistent with the 2 to 5 per cent range previously produced by the International Monetary Fund to estimate the scale of money-laundering. See http://www.unodc.org/unodc/en/press/releases/2011/October/unodc-estimates-that-criminals-may-have-laundered-usdollar-1.6-trillion-in-2009.html.

5 According to the IMF methodology, this includes any crime involving three persons or more, not necessarily limited to crimes committed by larger organisations.

1

country. Neighbouring countries are estimated to be the most significant destinations for foreign proceeds.

41. The NRA does not provide an estimate of how much of these proceeds are returned to the Kingdom after being laundered in another country, or of the inflows of proceeds of foreign crimes being laundered in the Kingdom. Nevertheless, Saudi Arabia is considered an unattractive location for laundering international proceeds because of its relatively small financial and commercial sectors, and limitations on direct foreign investment, and restrictions in access by foreigners to the financial and non-financial markets. These factors significantly reduce the risks of inflow of criminal proceeds into or through the Kingdom.

42. Saudi Arabia faces a high and diverse risk of terrorism financing, linked to terrorism committed both within and outside Saudi Arabia. Saudi Arabia also faces a high risk of terrorist acts carried out in Saudi Arabia, as can be seen by previous incidents on Saudi Arabian territory. The risk of terrorism and terrorist financing within Saudi Arabia is linked to the presence of cells of Al Qaeda, ISIL, affiliated groups, and other groups identified by Saudi Arabia. The number of foreign fighters is high, with estimates of over 3000 departures between January 2000 and February 2018. The risk of financing of terrorist groups abroad is linked to Saudi foreign fighters who travel, or attempt to travel, to conflict zones and to individuals who may raise funds and move assets from Saudi Arabia. The risk of fund-raising of terrorism through NPOs has been significantly mitigated over the last decade.

43. The international political situation, the lack of stability in the region, the presence of terrorist groups neighbouring Saudi Arabia and the presence of terrorist cells within the Kingdom have all been identified in Saudi Arabia's National Risk Assessment (NRA) on terrorist financing as reasons for assessing the likelihood of terrorist financing as high, with certain risks believed to be on the increase. The NRA examined the risks in three areas:

- Raising funds inside the Kingdom and transferring them outside for the support of external terrorist groups, purchase of weapons to be smuggled back into the Kingdom and for the purpose of facilitating the travel of foreign terrorist fighters.
- Raising funds inside the Kingdom for the purpose of carrying out attacks inside Saudi Arabia;
- Funds coming from outside the Kingdom for the purpose of carrying out attacks inside Saudi Arabia or as a transit point for another country.

44. Among the vulnerabilities are the presence of some foreign communities, the calls by individuals to raise non-official contributions domestically and internationally for humanitarian purposes, and the use of social media. In general, Saudi Arabia has taken significant steps to reduce and mitigate the outlined risks, as discussed in IOs 1, 9, and 10.

45. Saudi Arabia does not have any direct economic or financial relationships with Iran given the geopolitical relationship between the two countries. There is also very little economic exposure with DPRK. Saudi Arabia faces proliferation financing risks given its geographic proximity to Iran and trade relations with nearby countries that may trade with Iran.

Country's Risk Assessment & Scoping of Higher Risk Issues

46. Saudi authorities' understanding of the country's ML/TF risks is primarily based on two National Risk Assessments of ML and TF risks. Work on these assessments started in late 2015 and both assessments were completed in April 2017, and formally endorsed in August 2017. The assessments of ML and TF followed the same process and timetable, and both used the IMF risk assessment methodology. They were conducted under the auspices of the different bodies responsible for policies on ML and TF: the NRA for ML was prepared by the Anti-Money Laundering Permanent Committee (AMLPC). The NRA for TF was prepared by the Permanent Committee for Counter Terrorism (PCCT). These NRAs are the first time Saudi authorities have formally assessed their ML and TF risks. There are, however, risk-based policies on specific issues which pre-date 2017, in particular on the NPO sector, the supervisory engagement, money remitters, the Hajj and Umrah pilgrimages, and the use of cash. Both NRAs are classified but have been shared with relevant authorities and the private sector through workshops, although they have not been published. Members of the Mutual Evaluation team had an opportunity to review the NRAs and the 2017-2019 ML/TF action plan during the onsite visit.

47. In deciding what issues to prioritise for increased focus, the assessors reviewed material provided by Saudi Arabia on national ML/TF risks (as outlined above), and information from reliable third-party sources. The following list of issues was identified for additional focus:

Terrorist Financing:

- ***Foreign Terrorist Fighters (FTFs):*** There are a number of politically unstable regions that either border Saudi Arabia (Yemen, Iraq) or are located relatively close to it (Syria, the Horn of Africa). Terrorist organisations such as ISIL, Al-Shabaab and Al-Qaeda are active in these regions. Combined with the extensive land and sea borders around Saudi Arabia, the authorities determined that there is a risk of FTFs crossing Saudi Arabia's borders. It has been estimated that over 3,000 FTFs of Saudi Arabian nationality have become FTFs since 2000. The NRA identifies the exploitation of social media and information technology as a tool to finance or recruit terrorist fighters. While ISIL has not publicly claimed to focus its attacks on Saudi Arabia, several claimed attacks have taken place, including attacks on Mosques, and a series of attacks, including in July 2016, killing a number of government and security personnel. Mabaheth, the competent authority responsible for investigating terrorism and TF, has identified terrorist cells affiliated to ISIL operating in Saudi Arabia.
- ***Non-profit organisations:*** NPOs are an important sector in Saudi Arabia due to the large volume of charitable donations by Saudi residents. Saudi Arabia has recognised the risks that may in the past have been associated with the NPO sector and over the last decade has developed and implemented stringent safeguards and preventive measures for NPOs. NPOs in Saudi Arabia are also actively supervised. In combination, these steps have resulted in the risks being significantly mitigated. The Ministry of Labour and Social Development (MLSD) is the competent authority responsible for supervising NPOs. The NRA assigns a low residual risk rating to the NPO sector due in large part to the very strict measures imposed on the whole sector and the awareness-raising outreach efforts of the government since 2005.

1

- ***TF investigations, prosecutions, and sanctions:*** In addition to terrorist groups that are designated by the UN, Saudi Arabia prosecutes other groups for terrorism and terrorist financing. In line with the risks identified by the NRA, the investigation and prosecution of terrorism and terrorist financing offences is prioritised by Saudi authorities, and such cases are handled by a dedicated court - the Specialised Criminal Court. The assessment focused in particular on the investigation and prosecution of terrorist financing cases by Saudi authorities. Given the trans-national nature of TF and terrorist activity in Saudi Arabia (including on the large amount of remittances flowing out of the country), the assessment also particularly focused on how Saudi Arabia collaborates with international partners in this field.

Money Laundering:

- Cross-border cash movements and remittances: Saudi Arabia has long borders, including with countries undergoing conflict, and a very large number of individuals travel to Saudi Arabia each year. Saudi Arabia also has the second highest total outflows of remittances in the world. Saudi Arabian authorities have estimated that 70 to 80% of the proceeds of crime generated in Saudi Arabia flow out of the country and approximately 54% of domestic proceeds are generated in cash. The NRAs identify money remitters as having a high-level of risk for ML and TF. The assessment looked at how Saudi authorities prevent illicit cross-border flows, in the form of cash movements or through MVTS operators. It focused particularly on operational measures by law enforcement authorities to detect and disrupt illicit cash movements, as well as on steps to promote the use of non-cash channels.
- Corruption: Saudi Arabia's NRAs identify corruption as one of the most significant proceeds-generating crimes, and a serious concern for Saudi authorities. The assessment looked at how authorities investigate the laundering of the proceeds of corruption, and their activities to identify and recover these assets.

Materiality

48. Saudi Arabia is the largest economy in the Middle East (excluding Turkey) with a GDP of approximately USD 646bn. It has the fifth highest GDP per capita in the region, of USD 20 000 (2016)[6], and the 42nd highest in the world. The most important cities are Makkah and Madinah (holy cities), Riyadh (capital), Dammam and Jeddah (economic centres). The Kingdom is divided into 13 provinces or mintaqat.

49. Modern Saudi Arabia was established on 23 September 1932 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. A pilgrimage to Makkah, or hajj is a sacred journey, which has a precise time in the year that changes every year according to the Hijri Calendar. All Muslims are required to make Hajj once in their lifetime at least if they can afford to do so. During the hajj up to 2 million pilgrims enter the country. Umrah is another religious journey to Makkah and can be conducted at different times of the year.

50. The economy of the Kingdom is dominated by petroleum related activities; the Kingdom has 15.6% of the world's proven oil reserves and ranks as the largest

6 See https://data.worldbank.org/indicator/NY.GDP.PCAP.CD

exporter of petroleum. The petroleum sector accounts for roughly 63% of budget revenues, 43% of GDP, and 77% of export earnings. Only about 39% of GDP is generated by the private sector (which is partly publicly owned). Saudi Arabia is generally seen as a conservative country with relatively low crime rates.

51. Saudi Arabia has the second highest total outflows of remittances in the world after the US, approximately USD 38.8bn for the year to April 2017[7], representing 5-6% GDP and an average of USD 1 000 per capita per year, reflecting the large community of non-Saudi nationals living and working in Saudi Arabia.

Structural Elements

52. Saudi Arabia has the structural elements necessary for an effective AML/CFT system, including political and institutional stability, the rule of law, and high-level commitment to AML/CFT. Nevertheless, there are distinct features of the Saudi legal system that affect the implementation of AML/CFT measures. These are noted in the analysis of IO.9 below.

Background and Other Contextual Factors

AML/CFT strategy

53. Saudi Arabia has a national strategy for AML/CFT, and adopted an associated National Action Plan in October 2017. The national strategy sets out high-level strategic objectives to improve the Kingdom's effectiveness in different areas of AML/CFT policy and operations (e.g. to enhance capacity to detect crimes). The Action Plan sets out more specific actions, with corresponding indicators and timetables. At the time of the on-site visit, Saudi Authorities reflected the results of the NRAs in the high-level National Strategy (though to a very limited extent since the strategy is very high-level), and has adopted an Action Plan - which is more detailed and able to reflect the specific findings of the NRAs.

Legal & institutional framework

54. Saudi Arabia is an absolute monarchy. The King, currently His Custodian of the Two Holy Mosques King Salman 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).

55. The legislative branch is known as 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. Citizens have access to high officials (usually at a majlis; a public audience) and the right to petition them directly.

56. 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

[7] See http://www.worldbank.org/en/topic/migrationremittancesdiasporaissues/brief/migration-remittances-data

1

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.

57. 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 as the Constitution of the Kingdom, and provides for the application of Islamic Law (Shari'ah).

Shari'ah

58. Shari'ah is the body of Islamic religious law. Shari'ah is a form of law like civil law and common law and serves as the legal framework within which all aspects of life are regulated in the Kingdom. Shari'ah is also a religious obligation that binds the rulers of the Islamic state and requires them to implement Shari'ah. 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. While those man-made elements within Shari'ah are subject to change over time and place, the Qur'an's provisions are permanent, irrevocable and unchangeable.

59. If Shari'ah is silent on any given issue, 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, and the statutes of the King are Shari'ah-based and may 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 areas of criminal law, which means that the criminal statute deals with specificities, such as AML provisions, rather than generalities. The Kingdom also 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.

60. ML and TF are criminalised in the Kingdom based on statutory provisions outlined in detail under Recommendations 3 and 5 of the Technical Compliance Annex respectively. Shari'ah law generally prevents persons from acquiring and collecting illicitly originated money. This is done on two levels: i) by explicitly prohibiting illicit funds altogether and, ii) by identifying and prohibiting specific avenues for the illicit acquisition of funds. The first level is addressed in the Qur'an, which prohibits obtaining any person's money illicitly. On the second level, certain specific ways of acquiring funds are prohibited. An example includes the prohibition of liquor, which includes the prohibition of its production, usage, carriage, selling, gaining its proceeds, and purchase. The same applies to theft, armed robbery, usury, prostitution, etc. 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. 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 co-operating with the terrorists means helping them in harming society. The most severe penalties for terrorism offences under Shari'ah can therefore also be applicable to TF.

AML/CFT Institutions:

Co-ordination Bodies

61. *Permanent Committee on Combating Money Laundering (AMLPC):* The AMLPC was established by Cabinet's Resolution in May 1999. It is based at SAMA headquarters in Riyadh and chaired and supervised by the Governor of SAMA. The AMLPC is responsible for all AML related policy co-ordination, including ensuring implementation of the FATF Standards. The Committee heads the Saudi delegation to FATF, MENFATF and other international bodies. The Committee employs a vice-chairman and full time secretarial staff.

62. *Permanent Committee on Combating Terrorism* (PCCT): The PCCT was formed in December 2001 and has an oversight and co-ordination role for efforts in Saudi Arabia to combat TF. It is responsible for all CFT related policy co-ordination, including ensuring implementation of the FATF Standards. The Committee heads the Saudi delegation or participate as a member in all international, regional and local meetings with regards CT and TF such as (UN, GCTF, FATF, MENAFATF, International Coalition Against ISIL, etc.).

63. *The Permanent Committee for Legal Assistance Requests (PCLAR)* at the Ministry of Interior. It is presided over by the MOI undersecretary and is formed by representatives from 10 governmental authorities. Its role is to process requests from foreign states for international co-operation or mutual legal assistance.

64. *Chapter VII Committee*, headquartered within the Ministry of Foreign Affairs to oversee the implementation of UNSCRs in accordance with the UN Chapter VII Committee. It has implementing regulations. These regulations detail the whole regime to implement targeted financial sanctions related to proliferation financing.

Law enforcement bodies

65. *Saudi Arabia Financial Intelligence Unit* (SAFIU): The Saudi Arabia Financial Intelligence Unit I (also termed the General Directorate of Financial Intelligence) is a law enforcement body reporting to the State Security Presidency. All the law enforcement bodies may be requested by the SAFIU for information or may investigate cases pertaining to their field of expertise and authority at the request of the SAFIU. Also the SAFIU has the authority to request the PP to execute seizures.

66. *Public Prosecution (PP)*: The Public Prosecution is the body responsible for investigation and prosecution of crimes in Saudi Arabia, including ML/TF cases under the AML and CFT laws. In cases where other law enforcement bodies investigate cases, the PP is the supervisory body.

67. *Directorate of General Security (GSD):* Saudi Arabia's regular police force. It is the law enforcement body responsible for combating all predicate offences that are not the responsibility of other bodies, such as the General Intelligence Directorate.

68. *The General Intelligence Directorate (GID) or Mabaheth*: The General Intelligence Directorate or Mabaheth is the law enforcement body under the State Security Presidency, responsible for investigating terrorism, TF and bribery cases. It also investigates reports from the SAFIU on ML associated with bribery, and TF.

69. *The General Directorate of Narcotics Control* (GDNC)*:* The General Directorate of Narcotics Control 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.

70. *Saudi Customs*: Saudi Customs is responsible for checking and clearing all travellers and goods that enter or leave the Kingdom. It has specific powers to enforce its laws. It is part of the Ministry of Finance.

Financial supervisory bodies

71. *Saudi Arabian Monetary Authority (SAMA)*: SAMA is the monetary authority/central bank of Saudi Arabia. It is the supervisory and regulatory body for all FIs in the Kingdom, except for the securities sector. As SAMA chairs the AMLPC, it is also the leading authority for AML matters. H.E. the Governor of SAMA has a cabinet rank.

72. *Capital Market Authority (CMA)*: CMA, established under the Capital Market Law, promulgated by Royal Decree No. (M/30) dated 31/7/2003, is the supervisory and regulatory body for the securities sector, which includes the Saudi Stock Exchange (Tadawul), the Securities Depository Centre Company (Edaa), and the FIs that are licenced by the CMA to carry on securities business (the Authorised Persons), on all matters, including AML/CFT. CMA's status is similar to that of a Ministry.

Non-Financial supervisory bodies

73. *The Ministry of Commerce and Investment (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.

74. *The Ministry of Justice (MOJ)* supervises the judicial system in Saudi Arabia. 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 law firms.

75. *The Ministry of Labour and Social Development (MLSD)* is responsible for licensing, registration and supervision of general charities (which can be charitable societies or special charity institutions.

Other Control Authorities (OCAs)

76. The OCAs, which are not law enforcement authorities per se, but in identifying ML in the performance of their functions, are responsible for collecting evidence on ML and referring the file to the PP. The OCAs include Saudi Customs (in relation to customs violations); SAMA (in relation to breaches of the Banking Control Law, Finance and Insurance Laws); CMA (in relation to breaches of the CMA Law); the Ministry of Justice (in relation to violations of the Law of Lawyers); the Ministry of Commerce and Investment (in relation to breaches of the Commercial Fraud Law and the Concealment Law); and, the Food and Drug Authority (in relation to violations of the Food and Drugs Authority Law).

Financial sector and DNFBPs

77. Commercial banks represent the largest part of the financial sector. Saudi incorporated banks dominate the domestic banking market. They offer Sharia compliant products. The banking sector is concentrated around a few banks, some of which are part owned by government entities, in some cases banks own part of other companies that offer insurance, finance, and securities services (through separate legal entities), and some have ties to major international banks. More recently, the regulator has taken steps to increase the number of foreign banks operating in Saudi Arabia. As of 2017, SAMA has granted licences to 12 foreign banks. SAMA has taken major steps to enhance the prudential oversight of banks, with banks – the core of the Saudi financial system – liquid and resilient to economic shock.[8]

78. Capital Market activities in Saudi Arabia are still developing, and are relatively young compared to the banking sector. There is one licensed stock exchange, with the stock market opened up directly to non-resident foreign investors in 2015 which have been restricted only for Qualified Foreign Investors (QFI) in addition to the Swap Agreements Framework and investing through investment funds. Beforehand, non-resident foreign investors were only able to receive the economic benefits of securities listed on the Saudi Stock Exchange (Tadawul) via purchasing swaps agreements or invest through investment funds. The stock exchange facilitates electronic trading in listed securities, including shares and sukuk and bond markets. There are several hundred regulated collective investment funds, operated by less than one hundred fund managers. There are only 89 authorised persons engaged in regulated securities activities.

79. The insurance sector in Saudi Arabia consists mainly of non-life insurance. Only 3% of the market consists of life insurance. The sector is supervised by SAMA.

80. The finance companies sector is the youngest financial sector in Saudi Arabia. This sector provides financial leasing, real estate and consumer financing, Productive asset financing, SME's Financing, Credit Card Financing. SAMA is the supervisory authority for this sector.

81. Money exchangers and remitters are considered part of the banking sector, but are separately licensed and supervised. There are two types of money exchangers in Saudi Arabia: type A and type B. The type A license allows business to offer money transfer and exchange services, and the type B license that only allows for exchanging money. Supervision is undertaken by SAMA.

82. 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. There are more than ten thousands real estate agents active in the Kingdom. All real estate businesses are subject to related requirements of the AMLL/ CFTL.

83. There are more than two thousand dealers in precious metals and stones in the Kingdom, licensed for general purposes by the MOCI. All companies dealing in precious metals and stones are subject to related requirements of the AMLL/CFTL.

8 IMF (2017), Financial System Stability Assessment of Saudi Arabia

84. There are more than 4000 lawyers in the Kingdom, licensed for general purposes by the Ministry of Justice (MOJ). All lawyers are subject to related requirements of the AMLL/CFTL.

85. There are more than two hundred accountants in the Kingdom. Saudi Organisation of Certified Public Accounts (SOCPA) under MOCI has the responsibility of regulating and supervising. Registration with the Ministry is compulsory. All accountants are subject to related requirements of the AMLL/CFTL.

86. Although notaries exist in Saudi Arabia, these are employees of the Ministry of Justice, and therefore considered not to be notaries as defined by the FATF.

87. Gambling is illegal in Saudi Arabia and contrary to Sharia principles, and therefore, there are no casinos.

Preventive Measures

Table 1. **Overview of Financial Sector and Designated Non-Financial Businesses and Professions**

Sector	No. of Entities	Remarks
Banks (including local banks and foreign bank branches).	24	12 local banks and 14 foreign bank branches(2 not yet operating)
Insurance companies offering life insurance services	24	The number of insurance companies (34), of these 24 provide protection and/or saving insurance (corporate & 7 provide individual protection and or saving insurance)
Life insurance brokers	40	Brokers mainly provide services with respect to protection insurance for corporate.
Money Exchange Institutions (CLASS A)	4	Currency exchange services, as well as money transfer services. The entities are well-established companies with single owners or family businesses.
Money Exchange Institutions (CLASS B)	69	Only currency exchange services; the entities all have Saudi ownership.
Securities Services	89	Saudi bank affiliated AP (12 APs); Local AP (21 APs); Regional affiliated AP (22 APs); International affiliated AP (14APs); Arranging & advising AP (19 APs); (5) APs have not yet commenced
Finance companies	34	Only financial leasing, real estate and consumer financing, Productive asset financing, SME's Financing, Credit Card Financing
Lawyers	4 246	Most lawyers are sole practitioners or belong to small firms.
Accountants	220	There are 180firms. Each firm will have one or more accountants.
Real estate agents	1 2712	The vast majority are very simple firms and managed by the owner himself with no other employees.
DPMS	2 838	

Table 2. **Financial Sector in Saudi Arabia as of December 2016**

Sector	Assets (SAR)	% of FS Assets	% of NGDP
Banks	2 228 795 391 000	94.7%	92.9%
Financing companies	38 800 000 000	1.6%	1.6%
Securities	27 274 116 000	1.2%	1.2%
Insurance	55 725 888 000	2.4%	2.3%
Money Exchangers	696 005 000	0.0%	0.0%
Total	**2 351 291 400 000**		

Financial Institutions

88. All financial activities conducted by FIs as identified by the FATF standards and definitions are present in Saudi Arabia. Saudi Arabia has a legal and regulatory framework that governs the financial sector obligations vis-à-vis AML/CFT. The newly adopted AMLL and CFTL have been passed that in combination provide for a comprehensive overarching legislative framework for preventive measures that applies equally to FIs and DNFBPs. The laws are supplemented by more detailed Regulations.

Designated Non-Financial Businesses and Professions (DNFBPs)

89. Most of the FATF's Designated Non-Financial Businesses and Professions (DNFBPs) exist in Saudi Arabia: real estate agents, dealers in precious metals, dealers in precious stones, lawyers and legal advisers, and accountants. 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.

90. The provisions of the AMLL/CFTL Regulations, and in particular those dealing with the preventive measures and the monitoring of their implementation, apply equally to FIs and to the DNFBPs. The AML/CFT provisions designed for FIs, notably on CDD and reporting, are to be applied by DNFBPs to all their clients/ activities/ dealings. The Ministry of Commerce and Investment (MOCI) and the Ministry of Justice (MOJ) both had 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.

Legal persons and arrangements

91. The following commercial legal entities can be established in Saudi Arabia:(i) unlimited liability company; (ii) joint stock company; (iii) limited liability company and (iv) limited partnership company. In addition there are many commercial enterprises which do not have separate legal personality (e.g. silent partnerships).

92. Saudi society does not generally utilise legal persons for private asset management purposes but sets up legal persons almost exclusively to operate viable businesses and to directly conduct legitimate trade and commerce. The vast majority of Saudi Arabia companies have actual business activities. Shell companies utilised purely to manage assets do not exist. Approximately 17% of Saudi companies have a

1

corporate shareholder or corporate director. Most legal entities are owned and controlled exclusively by natural persons, which typically are the same persons controlling the legal entity's business activities and registered as shareholders and/or directors in the Company Registry.

93. Foreign ownership or control of Saudi legal persons is subject to tight regulations and oversight. Foreign individuals – resident or non-resident – may not be shareholders or directors of a Saudi legal person. Foreign legal persons may hold shares of a domestic legal person only after receiving approval from Saudi Arabia General Investment Authority (SAGIA) based on a stringent application and screening process. As of 2017, 4 174 foreign legal persons had received approval by SAGIA to invest in Saudi Arabia, of which about 20% were listed companies. About 3% of Saudi legal entities have a foreign element in their ownership or control structure.

94. Due to the limitations on foreign ownership and control, authorities consider that Saudi legal entities are not generally used when setting up transnational, multi-layered corporate structures. Given the controls, there is a possibility that in some instances strawmen may be used for registration purposes to obscure ownership by non-authorised persons. The limited use of corporate directors and shareholders in Saudi legal entities suggests that corporate vehicles are not widely used in themselves as a tool to obscure ownership or control rights.

95. Saudi Arabia has measures in place to ensure the transparency of legal persons and arrangements, as set out in the analysis of IO.5. All legal persons, (as well as commercial operations without legal personality but with capital above SAR 100 000 (EUR 27,700)) are required to be established/registered at the MOCI; a public notary is involved in the establishment process; foreign corporate directors or shareholders have to undergo a comprehensive screening and approval process before they may own or control a share of a Saudi legal entity; and annual financial disclosures by Saudi companies allow for the identification of CDD and beneficial ownership information maintained at FIs and DNFBPs. For all those legal entities that have capital requirements, the law requires that the capital share be deposited into a Saudi bank account. This necessitates that the legal entity undergoes the CDD process at the institutional level and provides beneficial ownership to the financial institution as part of the account opening process.

96. The following non-profit legal entities can be established in Saudi Arabia: (i) general charities (which can be charitable societies or special charity institutions, and are registered, licensed and supervised by the Ministry of Labor and Social Development (MLSD) and (ii) educational charities (which run Qur'an schools and or promote religion, and which are licensed and supervised by the Ministry of Islamic Affairs). At the time of the on-site these responsibilities were in the process of being consolidated within the MLSD.

97. Saudi Arabia has private waqfs, which are legal arrangements provided for in Islamic law. Waqfs are similar to common law trusts, but limited to specific purposes, and created through a judge who supervises the particular waqf.

Table 3. **Supervisory arrangements**

Types of sector	Supervisor
Banks (*includingRemittances Sector*)	SAMA
Insurance Companies	SAMA
Finance Companies	SAMA
Money Exchangers	SAMA
Securities Companies	CMA
Dealers in precious metals and stones	MOCI
Real estate agents	MOCI
Lawyers	MOJ
Accountants	MOCI

International co-operation

98. Saudi Arabia engages in international co-operation through a wide range of global, regional, and bilateral treaties and arrangements. It is a party to relevant international conventions including the Merida, Vienna, and Palermo conventions and the International Convention for the Suppression of the Financing of Terrorism. Relevant authorities take part in sector-focused global arrangements including Interpol, the Egmont Group, Financial standard-setting bodies (BCBS, IOSCO, IAIS). Saudi Arabia is a member of the Gulf Cooperation Council and the associated regional arrangements for international co-operation. Saudi Arabia also plays a prominent role in regional and global co-operation to combat ISIL and terrorist financing, e.g. the Counter-ISIL Financing Group.

CHAPTER 2. NATIONAL AML/CFT POLICIES AND CO-ORDINATION

Key Findings and Recommended Actions

Key Findings

- Based on its national risk assessments, Saudi Arabia has a good understanding of its ML risks and a very good understanding of its TF risks. The NRAs benefited from wide participation by authorities, good access to information and a sophisticated analytic approach.
- However, the NRAs were completed very recently, and authorities have not yet had time to fully reflect their findings in national policies or in the objectives of individual agencies.
- Saudi Arabia had a sound understanding of key ML/TF risks before conducting the NRAs, and has taken extensive steps to mitigate those risks (e.g. within the remittance sector and the special measures for Hajj and Umrah pilgrims).
- Saudi Arabia does nevertheless reflect important ML/TF risks in its national policies, although not on the basis of a formal assessment of these risks.
- Co-operation and co-ordination between Saudi authorities is backed by a strong institutional framework in the form of the AMLPC and PCCT, both of which have sufficient resources and political support to perform their jobs well.

Recommended Actions

- Saudi authorities should continue to implement the National Action Plan for AML/CFT on the basis of the NRAs, and fully reflect the findings in the objectives of individual agencies.
- Saudi authorities should improve the data available for the next revision of the ML risk assessment, specifically to improve the comparability of information from different agencies (as noted in R33), and to enable better estimates of proceeds of crime flowing to and from other countries, as well as extending the scope of the NRA to provide more in-depth assessment for financing terrorist groups in more distant regions, based on availability of a wider range of cases (noted in IO7 and IO9).
- Ensure that FIs and DNFBPs have a proper understanding of ML/TF risks, as a basis for applying simplified CDD measures.

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

Immediate Outcome 1 (Risk, Policy and Co-ordination)

Country's understanding of its ML/TF risks

100. Saudi authorities' understanding of the country's ML/TF risks is primarily based on two National Risk Assessments of ML and TF risks. Work on these assessments started in late 2015, and both assessments were completed in April 2017, and formally endorsed in August 2017 by the AMLPC and the PCCT. The assessments of ML and TF followed the same process and timetable, and both used the IMF risk assessment methodology, but were conducted under the auspices of the different bodies responsible for policies on ML and TF. The NRA for ML was prepared by the Anti Money Laundering Permanent Committee (AMLPC). The NRA for TF was prepared by the Permanent Committee for Counter Terrorism (PCCT). This exercise was the first time Saudi authorities have formally assessed their ML and TF risks, though there are risk-based policies on specific issues which pre-date 2017, in particular on the NPO sector, supervisory engagement, money remitters, the hajj and Umrah, and the use of cash. Both NRAs are classified but have been shared with relevant authorities (and the private sector through workshops and meetings), and have not yet been published or provided to the assessment team. Nevertheless, members of the assessment team were able to review the NRAs and the 2017-2019 ML/TF Action Plan during the on-site visit.

National Risk Assessment for Money Laundering

101. In general, Saudi Arabia has a good understanding of its ML risks. The ML NRA identifies four main proceeds-generating crimes: illicit trafficking in narcotic drugs and psychotropic substances (31%); corruption (22%), counterfeiting and piracy of products (21%), and customs smuggling (8%). About 71% of proceeds of crime are associated with organised criminal groups (considered to be any crime involving three persons or more, not necessarily by larger organisations). The main method used to launder money were transfers to other countries (authorities estimate that roughly 70-80% of proceeds flow out of the country) through, cash, FIs, and trade-based ML. Authorities also identify exploitation of FIs as a method, with banks, money remitters, and dealers in precious metal and stones (DPMS) assessed as having the highest risks.

102. The risks identified in the NRAs are reasonable, and largely consistent with the cases and other material provided to the assessment team, though some elements are not fully developed, including the laundering of proceeds after they have been moved out of Saudi Arabia (and their eventual repatriation), and the potential for more sophisticated forms of money laundering within Saudi Arabia. The difficulties with ML investigation in Saudi Arabia (noted in the analysis of IO7) mean that the risks identified by the NRA are not all supported by case studies based on the outcomes of successful investigations. More effective investigation of ML would in turn support a more granular risk assessment.

103. The NRA was prepared by the AMLPC through a dedicated subcommittee on risk assessment, including 26 members from all relevant agencies, and was based on the IMF's risk assessment methodology, adapted to reflect Saudi Arabia's administration and situation. The NRA used a wide range of information including statistical data and reports from all relevant agencies; academic studies of

vulnerabilities; outcomes of criminal investigations; reports from international organisations, strategic analysis by the FIU, and self-assessments of vulnerabilities, with bilateral meetings and workshops used to gather and understand the information. The assessment used diverse quantitative and qualitative data in order to avoid confirmation bias, coding qualitative responses in order to reflect them in the analysis. The NRA team made good use of such data as is available, but identified some areas for improvement, such as the deficiencies noted with R.33 where data is unavailable, or where different agencies gather data based on different and incompatible classifications.

National Risk Assessment for Terrorist Financing

104. Saudi Arabia has a very good understanding of its terrorism and TF risks. The TF NRA considered the risks associated with countries, sources of funds, transportation methods, routes, and entry points; and evaluated the particular TF risks posed by FTFs. The NRA identified the main terrorist threats as emanating from Al Qaida (particularly in Yemen) and ISIL/Daesh (in Yemen, Iraq, and Syria), with terrorists associated with both groups operating in Saudi Arabia. The NRA looked specifically at the financing associated with FTFs, as well as terrorists and groups within Saudi Arabia and in other countries, and included self-financing activity, as well as third parties within Saudi Arabia and both inbound and outbound cross-border financing. Particular vulnerabilities include migrant and diaspora communities associated with unstable or conflict countries. The conclusions of the NRA are reasonable, and consistent with international assessments of the terrorist and TF threats in Saudi Arabia and neighbouring countries.

105. The main sources of information used to develop to the TF NRA were the results of TF investigations. Saudi Arabia has conducted more than 1,700 terrorist financing investigations since 2013, resulting in 1,133 convictions. These peaked in 2014, at the height of ISIL's recruitment of FTFs. This exceptionally large number of cases (530 cases) gives Saudi Arabia a uniquely rich pool of information to use as the basis for a detailed evaluation of its TF risks, trends, and methods. This has been supplemented by other sources of information on vulnerabilities and methods, as well as the ML NRA. All relevant agencies participated in the development of the TF NRA, either directly through the PCCT or through workshops and discussions.

106. The reliance on a rich pool of TF cases does leave one gap. As noted in the analysis of IO.9, the TF cases available reflect the nature of the current and recent TF threats to Saudi Arabia, with a large number of cases relating to FTFs and to terrorist groups active in the Kingdom and neighbouring countries, and few cases relating to financing of terrorist groups operating in more distant regions. This has historically been a major concern and the TF NRA should address this potential threat more directly, despite the greater challenges of obtaining reliable evidence in the absence of numerous cases.

Table 4. **Statistics on TF investigations and convictions**

2013	206	619	373
2014	128	797	583
2015	101	161	105
2016	76	123	72
Total	**511**	**1 700**	**1 133**

National policies to address identified ML/TF risks

107. There has not yet been sufficient time for the results of the NRAs to be properly reflected in national policies. Nevertheless, Saudi authorities previously introduced a number of measures to address risks identified prior to and outside the NRA process. It was clear during the onsite that there is a very strong political commitment to conduct all the necessary improvements to the AML/CFT system in Saudi Arabia in order to address ML/TF risks, as illustrated by the speed with which legislation was passed.

108. Following completion of the NRAs in April 2017, Saudi Arabia passed comprehensive revisions of the AMLL and the LTCF. The laws were adopted on 24 October 2017 (AMLL) and 1 November 2017 (LTCF), immediately before the on-site visit, and took effect immediately. Revisions were also recently made to the NPO law (in March 2016). While many of the changes made in these revised laws and regulations were to address deficiencies identified in the 2010 FATF Mutual Evaluation of Saudi Arabia, or to implement new requirements added to the revised FATF Recommendations in 2012, a range of these changes also aimed to specifically address the conclusions of the NRAs. For example:

- The NPO law granted the MLSD a wider range of supervisory sanctions to address violations by NPOs of the registration and disclosures requirements;
- The process for incoming and outgoing mutual legal assistance in relation to asset tracing and recovery was further refined; and
- Asset recovery provisions in both AML and CFT laws were also broadened to permit prosecution in absentia and non-conviction based confiscation provisions were introduced in certain cases.

109. The AML and CFT Laws harmonise the preventive measures obligations for all FIs and DNFBPs. Previously these obligations were addressed in sectoral regulations, which created some inconsistencies amongst sector specific obligations. While the technical aspects of the preventive measures obligations in the new AML and CFT Laws were also aligned with the new FATF requirements, the driving force behind moving those obligations from sector specific regulations to an overarching legal framework were the findings during the NRA process with regards to the need for harmonisation of the legal obligations.

110. Saudi Arabia has a national strategy for AML/CFT, and an associated National Action Plan. The national strategy sets out high-level strategic objectives to improve the Kingdom's effectiveness in different areas of AML/CFT policy and operations (e.g.

to raise capacity to discover crimes). The action plan sets out more specific actions, with indicators and a timetable associated with each. At the time of the on-site visit, Saudi authorities had reflected the results of the NRAs in the high-level National Strategy and adopted a National Action Plan which is more detailed and able to reflect the specific findings of the NRAs.

111. Saudi Arabia has implemented several significant policies to address ML/TF risks which were identified prior to the NRA process, and show that given sufficient time, Saudi Arabia can and does adapt national policies which have the effect of mitigating ML/TF risks (although this may not be their primary purpose). The most significant examples include:

- *Controls on NPOs* - Following 2003, Saudi authorities applied very tight restrictions on the activities of NPOs, and established an intensive regime of oversight and inspection, in order to mitigate the risk that they could be misused. This is discussed in more detail in IO 10.
- *Remittances Sector* - Illegal or unlicensed MVTS operators, as well as poor AML/CFT controls by legal operators - have been considered a risk in Saudi Arabia for a number of years. Since April 2011, Saudi authorities have developed a remittance service framework to reduce and eventually eliminate the demand for illegal (or stand-alone) MVTS operators, and to ensure the implementation of adequate CDD and preventive measures by licensed MVTS operators. This includes a requirement for international MVTS providers to operate through a partnership with one of seven Saudi-licensed banks; the creation of over 730 remittance centres across Saudi Arabia through which these services can be accessed. Saudi Authorities have stopped issuing licenses for stand-alone MVTS operators, and the few remaining operators (using grandfathered licenses as class-A money exchanges) are subject to intensive supervision, as set out in the analysis of IO.3.
- *Cash* - The use of cash has been identified as an important enabler of ML and TF, and one of SAMA's policy objectives is to reduce the use of cash in Saudi society by encouraging the wider availability and acceptance of cashless payments, and expanding the diversity of products and payment systems offered by the financial sector. A key element of this strategy has been to require electronic payment of wages and salaries, in combination with ensuring all workers have access to accounts and payment cards.
- *Corruption* - Saudi Arabia's Anti-Corruption Commission – NAZAHA - recently took a number of measures aimed at reducing and mitigating the risks of these crimes, including the launch of an electronic monitoring program for public tenders, in addition to enhancing the detection and investigation capacity in financial and administrative corruption. Nazaha has developed a service which allows employees and beneficiaries to evaluate the services provided to them by the government entities. Furthermore, a supreme committee headed by Crown Prince Mohammed bin Salman was recently established to identify offenses, crimes, persons and entities involved in cases of public corruption and to take precautionary measures until cases are referred to the investigating authorities or judicial bodies. High profile cases have also been initiated recently, involving seizures of bank accounts and significant amount of funds that are suspected to be related to corruption offenses

- *Hajj and Umrah* – Special measures have been put in place to control the funds of pilgrims coming to the Kingdom for the Hajj and Umrah. Hajj and Umrah offices are required to open bank accounts in the Kingdom which are active only for the duration of the Hajj and Umrah (there are Hajj and Umrah offices in all countries where there are large numbers of residents travelling to Saudi Arabia for Hajj or Umrah). Transfers into the account are permitted only from the country in which the Hajj and Umrah office operates, and disbursements from the account are made only through bank checks in the name of the Hajj and Umrah office. Hajj and Umrah offices must provide to the authorities in the Kingdom all the names and identification documents, hotel in Saudi Arabia, transportation arrangements etc. of persons authorized under such accounts. Hajj and Umrah pilgrims are also inspected on arrival to ensure they are not carrying cash, with additional scrutiny for high-risk persons. According to statistical data, the volume of cash carried through the Saudi ports during Hajj and Umrah periods has decreased by more than 99% during the last three years.

Exemptions, enhanced and simplified measures

112. Before the introduction of the new AML law in October 2017, Saudi Arabia did not allow any FIs and DNFBPs to apply any exemptions or simplified measures in relation to the FATF recommendations. Enhanced measures based on established ML/TF risks are applied to some sectors, as noted above. The ML and TF NRAs have not yet been used as the basis for any further simplified or enhanced due diligence measures. The recently-revised AMLL and LTCF were drafted in accordance with the results of ML/TF NRAs and their implementing regulations set out that enhanced CDD should be applied on the basis of risks but does not set out specific cases or indicators which require enhanced measures.

113. Financial institutions and DNFBPs are required under the new AML Law to take enhanced due diligence measures to manage and mitigate higher risks when these are identified in their risk assessments, or in situations set out by authorities. Authorities require enhanced measures in situations set out in the FATF Recommendations, but no specific measures to mitigate risks identified through the NRA process have yet been put in place. The new AML Law and its Implementing Regulation allow simplified measures are to be applied where lower risk has been identified and there is no suspicion of ML. Simplified measures should be proportionate to the risk. However, the new laws were not being implemented in practise at the time of the on-site visit.

Objectives and activities of competent authorities

114. The results of the NRAs are not yet included in the objectives of individual competent authorities or reflected in their activities. At the time of the on-site visit, Saudi authorities were preparing a National Action Plan for AML/CFT, which when completed will set out actions for each relevant agency, to be reflected in their objectives. Nevertheless, outside the context of the NRA, the objectives and activities of some agencies reflect the ML/TF risks.

115. Following the adoption of the national risk assessments on ML and TF, the AMLPC and PCCT identified eight strategic objectives to reduce the risk of ML/TF as follows: -

- Enhancing local and international co-operation and co-ordination in the area of combating ML/TF,
- Enhancing capacities to discover the crime and analysis, investigation, litigation, provisional seizure and confiscation in cases of ML/TF;
- Ensure the existence of understanding and assessment of ML/TF risks within the entities subject to supervision;
- Enhancement of capacity building and training programs in the area of combating ML/TF; knowledge of beneficiary ownership and technology in the area of ML/TF.
- Raising the level of awareness of combating ML/TF; and
- Reduction of reliance on cash and curbing financial remittances through informal systems.
- Enhancing the identification of the Beneficial Owner.
- Enhancing the technical systems in the area of Ml and TF.

116. Financial supervisors (SAMA and CMA) have been quick to take steps to implement the findings of the ML/TF NRAs in their supervisory risk models and in the conduct of supervision. Both supervisors issued rules to implement CTF Law provisions and disseminated those rules to the financial entities subject to their supervision.

National co-ordination and co-operation

117. National co-ordination and co-operation on the development of policy is a significant strength of the Saudi system. Saudi Arabia has a strong and well-established institutional framework for co-ordination, with two main pillars: the AMLPC and the PCCT. Permanent Committees are a normal feature of the Saudi administrative system where co-ordination is required. The AMLPC and PCCT were set up as co-ordination bodies and have since played a major role on policy and operational co-operation in the areas of AML/CFT. The PCCT and AMLPC also co-ordinate with each other to ensure that the approach reflected in national AML policies harmonises and is consistent with that taken in the area of CFT, in particular when it comes to supervisory and financial issues.

118. Both committees include all relevant authorities (with scope to involve non-members as needed) and have clear mandates and procedures set out in Royal decrees. There is a significant overlap in the membership of the AMLPC and PCCT. Both committees have permanent staff which acts as a secretariat and can follow up on agreed actions. The secretariats of both committees are strongly backed by engagement and commitment at ministerial level. Both Committees meet at least on a monthly basis to discuss ongoing AML/CFT issues and policies in addition to ad-hoc meetings when needed. The first main output of both committees was conducting the ML and TF NRAs. All the members of AMLPC and PCCT contributed to the drafting of the AMLL and CTTFL and their implementing regulations respectively, through dedicated subgroups.

119. In addition to the AMLPC and PCCT, Saudi Arabia has two other relevant co-ordination bodies: the *Chapter VII Committee*, within the Ministry of Foreign Affairs, which is responsible for co-operation and co-ordination on the development and

implementation of national policies and activities to combat the financing of proliferation of weapons of mass destruction. Some members of the AMLPC are also members of the Chapter VII and the two Committees co-ordinate on a regular basis (e.g. to finalise procedures for implementing TFS). Saudi Arabia has also formed the *Permanent Committee of the Mutual Legal Assistance*, which acts as a central authority for handling mutual legal assistance requests received from foreign countries or made by Saudi Arabia to foreign countries on all offences. This Committee includes relevant law enforcement agencies and also co-operates with the AMLPC and the PCCT.

120. The analysis of IOs 6, 7 and 8 indicates that there may be some weaknesses in operational co-ordination between different prosecution and law enforcement authorities regarding individual cases, as well as dispersed or overlapping responsibilities (e.g. for financial investigation). These appear to affect authorities' ability to successfully pursue investigations upstream within criminal networks and to recover the proceeds of crime.

Private sector's awareness of risks

121. A Risk-based approach was introduced in 2009 for the securities sector, and in 2012 for most FIs, which are required to periodically conduct risk assessments and put in place mitigating measures. Financing and insurance companies (and many DNFBPs) were required to implement these measures from 2016, when supervisors introduced full risk-based supervision. The level of awareness generally reflects the length of time for which risk-based approach measures have been required: banks and APs have a good understanding of their risks, while others have varying levels of understanding as set out in the analysis of IO.4, with many DNFBPs' understanding of the risks beginning with the dissemination of the results of the NRA.

Overall conclusions on IO.1

122. Saudi Arabia has a good understanding of its ML and TF risks, based on a robust risk assessment process and a wide range of information. It also has strong and well-established mechanisms for national policy co-operation and co-ordination. Gaps remain in some areas. Some result from the focus of LEAs on ML and TF offences (as discussed in the analysis of IO7 and IO9), and could be addressed when the NRAs are updated. Others result from the very recent completion of the NRAs, the National Strategy and Action Plan, the AML law and the CFT law. Given sufficient time, the actions already taken will address most of these gaps.

123. **Saudi Arabia is rated as having a Substantial level of effectiveness for IO.1.**

CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

Key Findings and Recommended Actions

Key Findings

Immediate Outcome 6

- The SAFIU is well resourced overall, has an adequate legal basis to be able to perform its functions, and has access to a wide range of financial, administrative and law enforcement information.
- LEAs and other competent authorities across Saudi Arabia regularly use financial intelligence and other relevant information as part of their investigations into money laundering, predicate offences, and terrorist financing, and collaborate well. Trends are understood to some extent.
- The analysis provided by the SAFIU to LEAs and OCAs is straightforward and single-layered. STRs are not always archived appropriately, with some STRs archived on the basis of the low value of transactions. A lack of international co-operation, the use of only non-specialised IT tools, the large proportion of STRs disseminated and the low proportion of staff devoted to analysis at the SAFIU all contribute to the weaknesses. A new specialized IT tool that began to be implemented during the on-site visit may help to rectify some of the shortcomings.
- The STRs received by the SAFIU by categories of reporting entity do not appear consistent with the risk profile of the country. There are low numbers of STRs submitted by DNFBPs, while dealers in precious metals and stones are considered high risk.
- Outreach by the SAFIU and by SAMA has led to an increase in the number of STRs submitted by the banking sector, with an increasing number of STRs disseminated to LEAs. The time taken to process STRs within the SAFIU, the need for the SAFIU to retrieve additional information from reporting entities (in some cases via the supervisor), and the relatively limited number of STRs submitted by non-bank FIs and DNFBPs has had an adverse effect on the value and timeliness of financial intelligence disseminated to LEAs and OCAs.
- Paper filing of STRs by reporting entities puts the confidentiality of STR information at risk, although at the time of the on-site visit, a pilot project had been introduced to enable electronic reporting (see 3rd Key Finding above). Exchanges of information between the SAFIU and LEAs and OCAs

takes place via sealed envelopes which also poses a risk to the confidentiality of information.

Immediate Outcome 7

- Saudi Arabia has a legal framework that provides it with an adequate basis to investigate and prosecute ML activities.
- A Money Laundering Cases Procedure Manual has been developed which broadly serves as a national policy for the identification and investigation of money laundering cases. The manual illustrates the measures that the Kingdom has taken to ensure the different competent authorities recognize the importance of money laundering investigations while recognizing the value of financial intelligence and the need for consistent co-ordination between the relevant intelligence, investigative and prosecution agencies.
- As a result of recent awareness raising and strengthened co-ordination, Saudi Arabia has increased the number of ML offences being investigated from 295 in 2014 to 842 in 2016. Despite this, the number of investigations pursued is still not consistent with the risks the country faces.
- Saudi Arabia is not effectively investigating and prosecuting individuals involved in larger scale or professional ML activity. Investigations are often reactive rather than proactive, and tend to be straightforward and single-layered. Prosecutions are mostly for the self-laundering offence where Saudi Arabia is convicting individuals when they are unable to prove the source of funds.
- According to the Saudi Arabian National Money Laundering Risk Assessment, approximately 70 to 80% of the proceeds of crime generated in the Kingdom are estimated to leave the jurisdiction. However, Saudi Arabia has not demonstrated that it is pursuing cases pertaining to these proceeds and has not demonstrated it is conducting co-ordinated investigations with other countries to purse these proceeds.

Immediate Outcome 8

- Saudi Arabia's broad legal powers for confiscating the proceeds and instrumentalities of crime provided for under Shari'ah appear adequate. The new 2017 AML law provides more specific provisions concerning confiscation, which may support their consistent application. The PP has an internal mechanism to supervise the confiscation process, with the proportion of assets confiscated in proportion with the assets seized.
- The amounts of proceeds of crime seized and confiscated by Saudi Arabia have been increasing, but are still low and not consistent with the country's risk profile. Deficiencies in Saudi Arabia's ability to effectively investigate and prosecute ML activity are limiting the ability of Saudi Arabia to trace and confiscate criminal proceeds. The failure to conduct co-ordinated investigations with other countries is also significantly limiting the

confiscation of criminals' assets, given a large proportion of the proceeds of crime are estimated to leave the country.

- Confiscation is defined as a priority in Saudi Arabia's National Strategic Plan for 2017-19 as a measure to combat ML and TF. The confiscation of the objects of crime (principally narcotics) does appear as a priority. The lack of detailed statistics makes it difficult to understand whether the types of assets confiscated are in line with Saudi Arabia's risk profile, and understand where additional efforts could most effectively address the weaknesses in the system.
- Saudi Arabia is detecting a large amount of non-declared and falsely declared cash, as well as non-declared and falsely declared gold, precious metals and stones, although is not detecting BNI. Non-declarations and false declarations are being detected, although the amounts of cash confiscated at the border are not in line with Saudi Arabia's risk profile. It is not clear the extent to which sums confiscated are leading to ML or TF investigations.

Recommended Actions

Immediate Outcome 6

- Saudi Arabia should implement measures to allow the SAFIU to access additional information from reporting entities directly, in order to enhance confidentiality, speed and support operational independence.
- The SAFIU should continue to invest in advancements of its IT system to increase the timeliness and sophistication of its financial analysis. Measures to allow the electronic reporting of STRs - although already begun - should be implemented as soon as possible. Introducing an electronic system to share confidential information between the SAFIU and LEAs and OCAs may also help increase the efficiency of the system, and also help minimise the risk of breaches of confidentiality.
- The system allowing the electronic submission of STRs should be fully introduced to support the confidentiality STRs and the efficiency of SAFIU.
- Enhanced and more frequent training should be provided to SAFIU analysts and LEA and OCA staff, drawing on international best practice, to enhance the analytical capacity of the SAFIU, LEAs, and other competent authorities. It is essential that training activities are co-ordinated with all entities that work with financial intelligence in Saudi Arabia.
- SAFIU should reconsider the criteria for archiving STRs. Increasing the number of staff allocated to conducting analysis within the SAFIU may enable additional data points to be included for each STR archived in the system, in turn supporting the SAFIU's ability to make links between transactions drawing on archived material.
- Emphasis should be placed on the use of international co-operation tools in order to better support the operational needs of competent authorities.

- While the assessors do not believe that the SAFIU's operational independence is inhibited based on the evidence reviewed, as the SAFIU has recently moved institution to become a part of the State Security Presidency Saudi Arabia should ensure that it maintains its operational independence.

Immediate Outcome 7

- Saudi Arabia should prioritize the identification, investigation and prosecution of professional enablers and facilitators of ML with a view to increasing proactive ML investigations.
- In order to continue to increase the number of potential cases of ML activity that are being investigated, the National Strategy for AML/CFT should include precise and achievable actions set out over a period of time to build the understanding of LEAs across the country, address gaps in investigatory techniques and capacity, and ensure that new capabilities are applied effectively.
- The Saudi Arabian authorities should pursue joint investigations with foreign jurisdictions in an effort to recover the proceeds of crime leaving Saudi Arabia and identify other subjects implicated.
- The case management system at the PP should be used to collect statistics to track whether investigations, prosecutions are convictions are consistent with the risks Saudi Arabia faces, and to enable the authorities to understand the sanctions being applied to natural and legal persons convicted of ML.

Immediate Outcome 8

- Saudi Arabia should ensure that LEAs and OCAs are prioritising the confiscation of the instrumentalities and proceeds of crime as a normal element of all cases.
- Saudi Arabia should improve the level of capacity, awareness and understanding of confiscation tools, e.g. by developing a procedures manual, issuing further guidelines, and expanding training programmes for the LEAs and OCAs, and by establishing specialised units for asset tracing and confiscation.
- Saudi Arabia should commit to working with other countries to seize, repatriate and confiscate the proceeds of crime that have left the country.
- The Customs Authority should continue to encourage travellers to make declarations, including of BNI, at the border, and more proactively seize and confiscate falsely and non-declared cash where there is a suspicion of ML, a predicate offence or TF.
- Saudi Arabia should improve its mechanisms for collecting statistics on confiscation in order to better understand the weaknesses in the system.

124. The relevant Immediate Outcomes considered and assessed in this chapter are IO.6-8. The Recommendations relevant for the assessment of effectiveness under this section are R.3, R.4 and R.29-32.

Immediate Outcome 6 (Financial Intelligence ML/TF)

Responsibilities of the authorities

125. In Saudi Arabia, alongside the SAFIU, a number of LEAs and Other Control Authorities (OCAs) use financial intelligence and other information as part of ML and TF investigations. See section 1.3 for further information on the role of the different LEAs and OCAs.

126. Investigations into ML and TF are conducted by the LEA or OCA responsible for conducting an investigation into the particular type of predicate offence, for example, the General Directorate of Narcotics Control (GDNC) would conduct an investigation into ML relating to narcotics offences, and the Food & Drug Authority would conduct an investigation into ML if it relates to an offence under the Food and Drugs authority law. All formal ML investigations are co-ordinated by the Economic Crimes Unit at the PP, with the relevant LEA(s) or competent authority(ies) conducting the investigation. All formal investigations into TF are conducted by Mabaheth. Financial investigations are initiated following the dissemination of an STR from the SAFIU, or as a result of an investigation into a predicate offence.

127. While the SAFIU has responsibility for conducting financial analysis as a result of STRs filed and in response to requests made by LEAs and OCAs, LEAs and OCAs also undertake financial investigations following the detection of a predicate offence that sometimes involves elements of financial analysis (although the term *investigation* is always used to describe the activities of the LEAs and OCAs in order to avoid confusion between the roles of the LEAs and OCAs and the SAFIU). The SAFIU will sometimes undertake field investigations, for example seeking information on the suspect's activities, co-ordinating with the relevant LEA or OCA. Field investigations occur if there are significant grounds for suspicion as the result of an STR submitted – such as an investigation into a suspect's activities, the nature of any business activities, and their financial connections outside of the banking system. LEAs may be contacted depending on the nature of the field work.

Processing an STR

128. Reporting entities are required to notify the SAFIU if there is a suspicion of ML, associated predicate offences or TF when submitting an STR. Each STR submitted to the SAFIU is processed through five stages of analysis and evidence gathering. The diagram below describes the process for each STR.

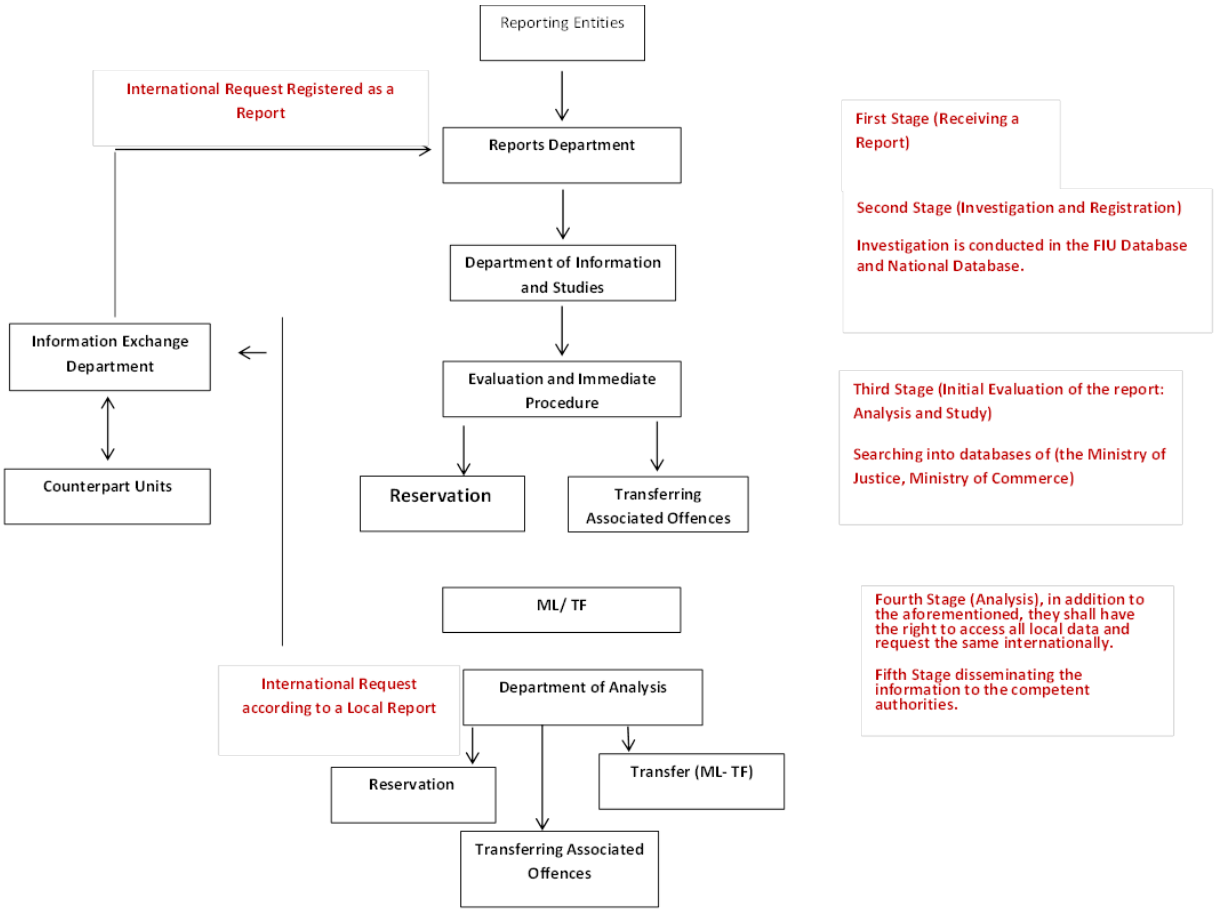
129. Once an STR is received, it is logged on to the system by the Receipt Team. The STR is then passed to the Department of Information and Studies, where searches of key databases take place, the UN lists are checked and links to third countries are assessed. During the third stage, the Assessment and Early Action Department review the information collected by the Department of Information and Studies to determine the urgency of the STR. The team that makes the assessment of the urgency of the STR is made up of financial, legal and security experts. The methodology that determines its urgency is based on a number of factors, including association with high-risk

jurisdictions, whether the person has a criminal record, and the size of the funds linked to the STR. The highest priority STRs must be disseminated within 24 hours. The methodology is updated from time-to-time, for example in response to the outcome of the NRA. STRs with potential links to TF are included in the category of STRs that are considered most urgent. They are disseminated to Mabaheth, normally within 5 hours from receipt, with further analysis completed by the SAFIU with SAMA within a maximum period of 3 days.

130. The STRs that have not been disseminated expeditiously are either sent to the Data Analysis Department, the fourth stage of the process or they get archived due to a number of criteria, such as the low value of the amounts of money involved in the STR. During the Fourth stage, additional databases are accessed and financial information is checked, for example deposits and withdrawals into/from the account, and links to other accounts. International co-operation will sometimes also be sought. The SAFIU may request additional information directly from reporting entities which have submitted an STR and indirectly through SAMA and CMA.

131. Once the analysis has been completed, the STR is referred to the LEA or other relevant competent authority depending on the type of crime and indicators associated with it. Where there are grounds to suspect the existence of ML, the case is referred to the PP. Where there are no grounds for suspicion, the STR will be archived in the SAFIU's database. Should new information related to the case come to light at a later stage, further analysis will be conducted.

Figure 1. **Processing an STR through the SAFIU**



Use of financial intelligence and other information

The SAFIU

132. The SAFIU has access to a wide variety of information, with direct access to a number of administrative, financial and law enforcement databases, and indirect access to a further set of databases via requests to other government departments or through a liaison officer depending on the type of suspicion and its priority. It has direct access to the Criminal Records Register, the Drug Register, the Customs Database (detailing cross-border cash declarations), the Wanted Individuals Investigation Register, Civil Affairs Registry, the National Information Centre, Driving License Register, Land Register, Commercial Register, travel records, company register at MOCI and records of companies registered with SAGIA. The Saudi Authorities have reported that the information is kept up-to-date, with information updated on an ongoing basis, when necessary. All searches are performed manually, with the types of information accessed differing depending on the nature of the STR and the point at which it is accessed. The most important databases (for example lists of UN listed individuals and entities, the Criminal Records Register, and the SAFIU's own database containing archived and previously

filed STRs) are accessed by the Department of Information Studies during the second stage of the process for STRs received. More in-depth analysis is conducted at a later stage in the process. A new IT system was being installed at the time of the on-site, that will mean that the first stage of STR analysis will be automated and electronic receipt will be integrated into the regime.

133. Information in other government databases, for example import or export data or information held by the Zakat and Tax Authority, is obtained by email during the second stage of analysis (the third stage in the above diagram).[Please see Annex A for a complete list of the databases that the SAFIU has access to] A specific department within the SAFIU (the Information Exchange Department) is responsible for exchanging information with other domestic authorities throughout the cycle of the STR through the SAFIU. The SAFIU also accesses open source information throughout the process.

134. More in depth financial analysis is conducted at the fourth stage of the process, if the STR has not been archived in an earlier stage. For the highest priority STRs that have been disseminated at the first stage of the analysis, financial analysis is conducted by the SAFIU and subsequently provided to the relevant LEA or competent authority. Before the completion of the NRA, STRs that related to TF were considered highest priority and disseminated at the first stage. Since the completion of the NRA, a set of criteria for STRs suspected of being linked to ML has been introduced, which include the top four proceeds generating crimes in Saudi Arabia according to the NRA. It is possible that this method could cause confirmation bias, with a large number of STRs disseminated urgently; however, the system had only just been implemented at the time of the onsite, and so could not be assessed.

135. In order to conduct financial analysis, the SAFIU may request additional information directly from the reporting entity that has submitted the STR, or from other reporting entities via SAMA and the CMA. The SAFIU receives the information from SAMA and the CMA within 5-7 days on average. A dedicated point of contact at SAMA and the CMA supports the process, and in urgent cases, the point of contact at SAMA and the CMA may obtain the information immediately. The SAFIU is able to request additional information from DNFBPs directly.

136. Once more in-depth analysis has been conducted by the Analysis Department of the SAFIU following an initial review by the Assessment and Early Action Department, the STR is disseminated to the relevant LEA or OCA. The LEA or OCA may refer back to the SAFIU in order to request additional information relating to potential links between suspects and information on third parties.

Box 1. STR disseminated to the GDNC resulting in ML investigation

The SAFIU received an STR from a bank concerning a Saudi national suspected of conducting suspicious financial transactions through cash deposits and withdrawals, which exceeded his monthly income and were not commensurate with his profession. By examining the STR and other available financial information, the SAFIU found that the suspect had a history of drug possession. Analysis was carried out to determine the source of funds. Examples of these indicators included criminal precedents of the person and the fact that most transactions were in cash.

The General Directorate of Narcotics Control (GDNC) was notified to verify the status of the suspect and to identify his actual employment and other business activities. The GDNC confirmed that the suspect had been involved in suspicious activities, including dealing in illegal drugs, and that he was under surveillance in an attempt to catch him in the act of committing a crime.

The SAFIU sent an analytical study on the suspect highlighting other suspects who may have been associated with the suspect based on the volume of their financial transactions. The individual was prosecuted and convicted for ML having purchased vehicles and properties in the names of his relatives and some of his friends.

137. The procedures set out in the AMLL and internally within the SAFIU provide a mechanism to help ensure a variety of sources of information, both financial and non-financial, are accessed for every STR analysed. Access to information provided by Customs is particularly important given the fact that a large proportion of the proceeds of crime generated within Saudi Arabia is estimated to leave the country, the economy of Saudi Arabia is still largely cash-based (although the Government is taking steps to reduce it) and Saudi Arabia has expansive land and sea borders.

138. On the basis of the case studies presented to the assessment team, the wide range of databases available to the SAFIU are regularly accessed and used by the SAFIU, adding value to the STRs subsequently disseminated. While the use of financial information has been demonstrated, for example through the checking of account activity, the cases provided straightforward financial links between accounts and between financial and non-financial information. Common trends triggering suspicion were large cash deposits and internal and external transfers. No cases that were presented involved more sophisticated trends, for example involving trade-finance banking products (despite several case studies that were presented involving import export companies), non-banking products such as financial leasing or investment, the use of multiple legal persons or legal persons in other jurisdictions or where more complex money laundering networks have been uncovered. In addition, the main trigger that initiates cases was demonstrated to be the presence of a criminal record, i.e. data from criminal records triggers financial analysis rather than analysis being initiated following the detection of financial red flags. This ultimately limits the extent to which financial information is accessed and used by LEAs and OCAs.

139. During the onsite mission, the SAFIU moved from being under the supervision of the Minister of Interior to the supervision of the Presidency of State Security. The Director General of the SAFIU reports directly to the President of State Security. The functions of the SAFIU, its competences and its independence, as prescribed in the AMLL, are also included in the amended AMLL that provides the SAFIU with its legal basis. There was no indication during the onsite visit that the operational independence of the SAFIU had been impeded. Nevertheless, given the changes in responsibility to a newly created department, it will be important for the SAFIU to maintain its operational independence and autonomy.

LEAs and OCAs [ML]

140. Although the SAFIU conducts financial analysis for all of the STRs disseminated to LEAs and law enforcement, elements of financial analysis are undertaken by the LEAs and OCAs in the process of their investigation into suspected ML activity. LEAs and OCAs will also investigate potential ML activity triggered by the investigation into a predicate offence. The MOI, General Mabaheth, Administrative Mabaheth (responsible for combating bribery and crimes relating to the misuse of public funds), GSD and GDNC all have their own financial investigation units. There are approximately 189 financial analysts at the Public or General Security Department (GSD), 90 at GDNC, 51 at Administrative Mabaheth and 41 at Customs. The majority are based in Riyadh, although some are based in regions around Saudi Arabia. Analysts spend the majority of their time working on ML cases (with the exception of the GSD). All of the departments have analysts in units across the 13 administrative regions of Saudi Arabia, apart from Customs that has analysts at 41 border entry/exit points.

Table 5. **Financial investigation units embedded within the LEAs and OCAs**

Authority	No. of analysts for ML & TF crimes	Cases where analysis has been undertaken (includes more than one case)
Directorate of Public Security	189	177 (2017)
Anti-drugs Directorate	90	781 (2016-17)
Mabaheth (general intelligence – TF only)	56 (in addition, regional officers also undertake elements of financial analysis)	5 670 (2013-16)
Mabaheth (administrative – bribery and related crimes)	37 at headquarters (14 analysts are also posted in each region)	3 486 (2013-16)
The Customs Authority	43	57 (2013-16)

141. Many of the LEAs and OCAs have direct access to government databases themselves, can access other databases on request, and can request additional financial information directly from SAMA or from the CMA. Three of the LEAs that are involved with the investigation of ML and TF most frequently (Mabaheth, the General Directorate of Drug Control, Public Security) have direct access to the criminal

records register, civil affairs and records of personal and family information and a number of databases on request (including Customs information and the commercial register). The Customs Authority does not have access to information via SAMA or from the CMA, and can only request information from some databases on request (the Criminal Records database, Civil Affairs, and Travel Data). The LEAs and OCAs, including Customs and the regional offices of the LEAs and OCAs, are able to send requests to the SAFIU to seek further information, to support their investigations, and do so on a regular basis.

Table 6. **Requests by LEAs and OCAs (including regional offices) to the SAFIU**

Authority	Number of requests (2017)
Public Security	223
Drug Control	156
Mabaheth	Bribery (189) TF (127)
Public Prosecution	53
Customs	16
MOCI	35
Zakat & Tax Authority	30

142. There are a large number of officials responsible for conducting ML investigations throughout Saudi Arabia, totalling in excess of 700 individuals taking into account all of the regional and national LEAs and OCAs. Many of the individuals responsible for conducting investigations are also responsible for making use of financial intelligence. This means that Saudi Arabia faces a big challenge in ensuring that they are all adequately trained, and all understand the importance of accessing intelligence and other relevant information. It also means that there is a burden placed on the SAFIU in having to support the needs of a large number of LEAs and OCAs. The extent of the resource devoted to accessing financial and other relevant information does demonstrate Saudi Arabia's commitment to tracing the proceeds of crime. However, building capacity at the SAFIU, so that it is best placed to support the LEAs and OCAs in accessing financial intelligence, would help place the SAFIU in the best position to enable it to uncover other parties related to the ML, TF or predicate offences. This is coupled with the fact that there was little training provided to SAFIU staff specialised in financial analysis according to data provided (for the years 2015-2016). Therefore, it is recommended that the frequency and intensity of the specialised training sessions given to SAFIU financial analysis staff to carry out their analytical work and support the needs of other LEAs and OCAs is increased. Collaborating with other FIUs may be an effective way of sharing best practices.

Box 2. Case Study of a Report received by SAFIU from a Financial Institution

The SAFIU received a STR from a financial institution (a bank). The bank referenced that the STR was very urgent. The suspicion was triggered by deposits of large amounts of money by a group of expatriate workers. Once the SAFIU received the case, it started an investigation by collecting information from the different databases to which the SAFIU has direct access. After that, the SAFIU studied the report. As a result it came out that the information stated in the Commercial Register of the suspected enterprise indicated that its capital did not exceed (SAR 25 000), compared with what was deposited (SAR 12 090 225).

Upon requesting import and export information from the Customs Authority, it was found that no exports or imports were made by the suspected enterprise, suggesting that it was not practicing its commercial activity. The request of information from law enforcement authorities through field investigation, due to lack of sufficient information through the study of the account of the suspect, revealed that the enterprise did not exist, had no headquarters and did not carry out its commercial activities. The report was referred by the SAFIU to the PP in order to complete the investigation, which led to the conviction of the crime of money laundering, as the suspicious could not submit evidence to prove the legitimacy of the sources of the funds. The individual also confessed that he had rented his enterprise's account to a number of foreign workers against a 5% commission of the value of remittances outside the Kingdom.

It was proven to the judge that the owner of the enterprise had committed a money laundering crime. Therefore, the judge sentenced him to a five-year prison term and confiscated the funds in the enterprise's account based on the AMLL. The second non-Saudi was sentenced to a one-year prison term and a financial fine equal to the funds he had obtained, and is to be repatriated from the Kingdom on completion of his sentence, in accordance with the AMLL.

General Mabaheth [TF]

143. The financial analysis department of Mabaheth is well resourced with 56 financial analysts based at the headquarters. This is in addition to a number of investigators in the regions. The work undertaken by the financial analysts at Mabaheth, as with other LEAs and OCAs, would include asking banks for bank statements that they hold (via SAMA), and making use of financial intelligence and other relevant information. Mabaheth has direct access to a wide range of financial, administrative, and law enforcement databases. Often, TF investigations and associated analysis takes place in response to an investigation into an act of terrorism or as a result of a confession. Financial intelligence generated by the SAFIU, or access via requests to the SAFIU is frequently accessed by Mabaheth and used in TF investigations. There is evidence that Mabaheth has undertaken more complex financial analysis for TF, in one case linking a number of individuals without an

obvious connection in a terrorist network. However, the case is currently under investigation and so could not be provided, and no other cases involving more sophisticated financial analysis have been presented to the assessment team. The effectiveness of terrorist financing investigations is assessed under IO9.

Box 3. Case study of Terrorist financing reported by a financial institution

General Directorate of Financial Intelligence (SAFIU): A report was received from a bank concerning a customer (person A), a non-Saudi, suspected of having carried out transfers to several accounts within the Kingdom to persons who were not related to his nationality, area of presence or the nature of his profession. The SAFIU requested the accounts of person A and having examined them, it identified a similar name (person B) among the dealers in the database. It has already received information on suspicion of terrorist activities by the General Intelligence (International Co-operation).

The results of the study of the account and the financial report were passed on to the General Intelligence Directorate (Mabaheth).

General Intelligence: The case was referred to International Co-operation. Based on the search in the electronic system, it showed the existence of person B's name within the statements of one of the detainees. The case was referred to Investigations in order to investigate the operation. The SAFIU addressed the financial intelligence request, providing it to Mabaheth, co-ordinating with SAMA through a secure channel to provide it with the details of the operation, date, place and picture of the process of transfer by a foreign person (person A or C) to person B.

Operations: It was found through investigation that another person (person D) had disappeared after the arrest of his brother (person B). Information was available on person D's location and that he is a supporter of Da'esh. Accordingly, his name was circulated as wanted on security basis. Through security follow up, the location of his presence and his cell associates was confirmed. On raiding him to arrest him, he exploded himself using an explosive belt. The operations were assigned to provide information and carry out research and investigation of the parties associated with person A and the person transferred to him, person B.

Investigations: During the investigation of persons A and B, it became clear that the case was not related to person A the case, and person B that the account in his name and the actual user is his brother.

Arrest: The investigation revealed that person D disappeared after the arrest of his brother, person B, with the information that he is in a particular city and supporter of the organization and called for him to be named as a security risk. Through the follow-up, security determined his location and members of his cell and when there was a raid to arrest him he blew himself up with an explosive belt. Person A was investigated and it was found that the account was in his name, and the purpose of the conversion with person B from person A was confirmed through filming.

STRs received and requested by competent authorities

144. The SAFIU receives a reasonably wide variety of STRs relating to ML, with many of them relating to cases of large unexplained cash deposits or account activity not commensurate with individuals' declared income, and the majority originating from the banking sector. There are few STRs submitted for DNFBPs, despite the fact that some DNFBP sectors (in particular DPMSs) are considered a high-risk sector, although there has been a slight increase for 2017. Almost all of the STRs received are from FIs (mainly banks). Statistics on the STRs filed and how they relate to different predicate offences has not been provided. The SAFIU also receives reports "STRs" from individuals via a government application called "Absher" which provides many government services to nationals, where it has a section where individuals can report a crime. The number of STRs submitted by reporting entities in different sectors is set out in the analysis of IO.4, in Table 5.1.

145. If an STR is to be disseminated, the SAFIU provides a detailed report to the relevant LEA(s) and/or OCA, including information obtained directly or indirectly through the databases, links to individuals, and details of the suspected offences. This will include relevant details of the non-declaration or false declaration of cross-border cash. As above, TF-related STRs are deemed urgent and disseminated to Mabaheth at an early stage with some supplementary analysis undertaken by the SAFIU. In 2016, the SAFIU disseminated 2,702 STRs to multiple entities (including the PCCT, Mabaheth, GDNC, MOCI and the PP). A reasonable number of STRs are being disseminated to a wide range of competent authorities, and overall have been increasing for every agency over the period 2013-2017.

Table 7. **SAFIU reports disseminated to LEAs, OCAs and other competent authorities**

Entity	2013	2014	2015	2016	2017
Public Security Directorate	575	628	551	572	991
Ministry of Commerce and Investment	224	226	185	154	573
Public Prosecution	192	136	172	129	228
General Directorate of Narcotics Control	287	331	228	324	248
Administrative Mabaheth (bribery)	79	88	149	145	155
General Mabaheth (TF)	118	126	232	368	588

146. The Customs Authority submits data on incoming and outgoing cash/BNI declarations to the SAFIU. Data received from the Saudi Customs Authority is updated on the SAFIU database on a daily basis and analysed by a special division in accordance with a defined methodology. Information provided by the Customs Authority has generated a typology on cross-border cash smuggling and the SAFIU has provided it to a number of competent authorities, of which Customs was one. References to the use of customs information in financial investigations was cited in a number of the case studies provided to the assessment team.

Operational needs supported by FIU analysis and dissemination

147. The proportion of STRs analysed and subsequently disseminated is significant (around 66% in 2015, and 58% in 2016). As can be seen from tables 3.3, 3.4, and 3.5, a large proportion of the reports disseminated result in formal investigations by the PP – either following dissemination directly to the PP or via one of the LEAs or OCAs.

In addition, Saudi Arabia has indicated that a number of the subsequent investigations result in prosecutions. However, it appears that a number of the reports that are considered to be disseminated may be as a result of inquiries made by LEAs or OCAs or the PP, rather than following analysis undertaken on STRs provided by reporting entities, as the figures provided for STRs that subsequently trigger an investigation do not match with the figure provided for IO7. It does appear that the SAFIU is providing information to a broad range of competent authorities, although the large proportion that are disseminated suggests that the SAFIU could do more to analyse potential links and sift out false positives with respect to STRs received from reporting entities and subsequently disseminated.

Table 8. STRs received and disseminated by the SAFIU [ML]

	2013	2014	2015	2016	2017
STRs received	2 497	2 366	3 766	6 370	6 575
STRs analysed	2 497	2 366	3 766	6 370	6 575
STRs reserved	664	566	1 267	3 668	2 750
Reports disseminated to competent authority	1 833	1 800	2 499	2 702	3 825
Reports subsequently referred to Public Prosecution for formal investigation	1 028	1 041	1 049	1 155	2 009

Table 9. STRs received and disseminated by the SAFIU [TF]

	2013	2014	2015	2016	2017
STRs received	118	126	232	368	588
STRs analysed	118	126	232	368	588
STRs reserved	89	89	85	161	276
Reports disseminated to competent authority	118	126	232	368	588
Reports subsequently referred to Public Prosecution for formal investigation	29	37	147	207	312

148. A reasonably low proportion of the reports are archived. During the on-site visit, the assessment team were informed that the reasons for archiving STRs included the low value of transactions and the lack of justified red flags. The SAFIU should reconsider archiving STRs on the basis of their value, given it is possible that they may still represent ML or TF. It is also unclear when the STRs are disseminated: in the third stage by the Rapid Dissemination team (where initial financial analysis is conducted), or during the fourth stage where a more thorough analysis is executed. The Rapid Dissemination may be archiving STRs prematurely, and as a result losing the opportunity for further analysis to identify illicit activity.

SAFIU tools, resources and approaches

149. Overall, the SAFIU is well resourced, with a budget of SAR 121m per annum (approximately EUR 27m). The budget has been at around the same level since 2009

shortly before the last MER of Saudi Arabia was adopted. 38 of a total of 128 employees across all of the departments within the SAFIU are analysts (up from a total of 111 employees in 2009). In order to improve the sophistication of the analysis to better support the operational needs of the competent authorities, a greater proportion of staff could be devoted to financial analysis, the core function of the SAFIU. The improved IT system that is being implemented may also help improve the SAFIU's analytical capability. Outreach by the SAFIU and by SAMA in particular appears to have resulted in an increase in the number of STRs submitted. If the increase in numbers of STRs submitted continues, as would be expected as the new risk-based supervisory regime for DNFBPs is relatively new and there are low numbers of STRs submitted by DNFBPs, the SAFIU may need to consider increasing the number of staff devoted to analysis further.

150. The SAFIU has been using non-specialised IT tools in analysing STRs. This may be a factor in the time taken for STRs to be analysed and processed through the SAFIU. Case studies provided to the assessment team during the onsite involved STRs taking a month to be analysed and assessed through the committees within the SAFIU. The SAFIU has a target of reducing the time taken from 1 month to 7 days or less. A new specialised case management tool, in the process of being deployed during the on-site visit in November 2017, is expected to cut down the time needed and help meet the target. However, it was not operational at the time of the on-site and therefore its effects could not be assessed. To ensure that the information is not lost and potential links are established, the old database will need to be integrated into the new one. This will require substantial care and attention as the data is in different formats. In addition, the extra time that is needed for the SAFIU to go through SAMA when it requires additional information from reporting entities not related to the STR submitted (for FIs only), adds to the time taken to analyse an STR. It takes 5-7 days on average. The extra step of needing to go through the supervisor also adds an additional risk to the confidentiality of the information as it needs to go through an additional agency, although there is no evidence that confidentiality has been compromised.

151. A key deficiency inhibiting the extent that SAFIU analysis is supporting the operational needs of LEAs and OCAs is the lack of international co-operation undertaken to support SAFIU products. Given the number of foreign nationals resident in Saudi Arabia, and its extensive land and sea borders, Saudi Arabia needs to assess how the SAFIU could better exchange information with other FIUs. Very few case studies were provided involving the SAFIU that included activity conducted in a third country. The lack of international co-operation is also likely to restrict the sophistication of the SAFIU's analysis, as complex cases with international elements cannot be detected and analysed. [See IO2 (Section 8.1.3 and table 8.8) that covers the exchange of information by the SAFIU on ML and TF].

152. The numbers of incoming and outgoing international requests for information on TF are not in line with the numbers of convictions and the risk profile of the country. The numbers of outgoing requests are also low and not in line with Saudi Arabia's risk profile, with a large proportion of the proceeds of crime expected to leave the country (although this may not necessarily be taking place through the financial sector) [See IO1 and IO2]. More generally, the numbers of incoming and outgoing requests are also not in line with other contextual factors, such as the large number of foreign residents in Saudi Arabia, and the numbers of visitors entering and

exiting the country each year. The numbers of outgoing requests take a downward trend at the SAFIU. The SAFIU should send outgoing requests where information from other FIUs may support its analysis, and ensure it has adequate resource to respond to incoming requests promptly. This will help the extent that SAFIU analysis and dissemination can support the operational needs of competent authorities in Saudi Arabia.

SAFIU products

153. The Information and Studies Department at the SAFIU is responsible for tracking methods and trends of ML activity. The SAFIU has produced around 30 different strategic reports relating to specific vulnerabilities, producing at least one per quarter on average. The SAFIU provided some examples of the reports they prepare and they mentioned that the sources of information are information from LEAs, customs reports and STRs. Some of the typologies produced by the SAFIU were used in the NRA. Examples of strategic reports included:

- Use of cash in purchase of high value cars and their involvement in ML.
- Payment of drug transaction by undervalued vehicles.
- False reporting of cash in the southern borders and its abuse by Yemeni drug traffickers who report inflated amounts of money resulting from selling fish to local traders.

154. Following its analysis, the SAFIU formed a committee to work on limiting the use of cash in car dealerships with MOCI and SAMA, resulting in practical action taken by the authorities and demonstrating that the SAFIU's strategic analysis is having an impact. However, the SAFIU needs to consider whether all of the reports it is producing are in line with the overall risks of ML/ TF being conducted in Saudi Arabia. For example, typology reports analysing cases of ML in relation to corruption have not been produced, which in accordance with the NRA should be a high priority, particularly when considering some of the topics that have been the focus of the other products produced.

Co-operation and exchange of information/financial intelligence

155. Across all of the competent authorities in Saudi Arabia, including the SAFIU, there are large number of departments and individuals within those departments responsible for using financial intelligence and other relevant information in relation to suspected predicate offences, ML and TF activity. While Saudi Arabia has demonstrated that the various authorities are co-ordinating and exchanging information efficiently there are some areas of overlap, since there are similar tasks required when conducting financial analysis and undertaking a financial investigation. This means that the allocation of resource required to ensure the smooth functioning of the system is significant and should be further enhanced. In some instances, LEAs ask for financial information via SAMA and analyse these records themselves, and may turn to the SAFIU later on. Overlaps also raise the likelihood of duplication, slowing down the transit of intelligence through the system and meaning that resource could be allocated within the system more efficiently.

156. The PP has a co-ordinating function when it comes to investigations that involve multiple agencies, enabling the exchange of financial intelligence and other

information. Evidence was provided of co-operation between LEAs, SAMA and the SAFIU, with membership of the permanent committees on AML and CFT helping maintain and regulate the relationships between the different authorities. Every LEA and OCA has appointed a liaison officer at the SAFIU, further supporting co-operation between the competent authorities and the SAFIU. In addition, the SAFIU has a specific department, the Information Exchange and Follow-up Department that is responsible for exchanging information with other domestic authorities (as well as counterparts abroad). The SAFIU signed memoranda of understanding with LEAs as well as the PP, MOCI and other entities, although some MOUs are lacking, such as an MOU between the SAFIU and the Customs that would allow the SAFIU to access information held by the Customs automatically.

157. The analysis that the SAFIU is undertaking sometimes includes elements of field investigations and co-ordination with the LEAs. The SAFIU is therefore undertaking elements of an investigation that would fall to LEAs in many countries. Although the SAFIU is well resourced overall, it may be more efficient for the SAFIU to focus on conducting financial analysis, disseminating STRs at an earlier stage for the relevant LEAs to undertake field investigations. Conversely, many LEAs are conducting the type of financial analysis that the SAFIU may be in a better position to conduct. While co-ordination and the exchange of information appear to be functioning well, Saudi Arabia may wish to review the balance of competence between the SAFIU and the LEAs and OCAs to ensure the most efficient allocation of resource.

Confidentiality of information exchanged

158. The SAFIU receives the majority of STRs in paper form from all reporting entities, receiving sealed envelopes containing STRs. Some reporting entities stated that they send STRs by fax or report suspicious transactions by making telephone calls to the SAFIU. Members of the public are also able to submit STRs to the SAFIU. The telephone number of the FIU is kept in dealers of precious metals and stones and real estate agents and the supervisory authorities penalize firms if they fail to keep the contact details for the SAFIU on display for staff. The SAFIU receives some STRs in the form of CDs and inserts them into their computer system to access the information thanks to new software acquired around the time of the onsite visit. In the Annual Report of 2015, the SAFIU cites that it is implementing a system to enable the electronic receipt of STRs, but this has not yet been implemented. This is an issue that was also recognised in the 2010 MER of Saudi Arabia.

159. The paper receipt of STRs risks the confidentiality of the process. Speeding up the process of automation should be a priority particularly given the SAFIU has an adequate budget to be able to do so. Enabling the electronic submission of STRs will also help speed up the process, in turn supporting the relevance of the information that the SAFIU receives and disseminates.

160. The SAFIU exchanges information with many relevant authorities. The cases disseminated by the SAFIU are submitted to the relevant LEA or OCA in a closed envelope. The MoUs signed between the SAFIU and other authorities contain confidentiality clauses. SAFIU staff are aware of the restrictions on the use of information and the manner in which it is to be handled. Ensuring all of the authorities are able to distribute and receive electronic copies of information in a confidential

manner would support the confidentiality of the process, given knowledge of who has seen the information would be known. In addition, it would help support the efficiency of the AML/CFT regime in Saudi Arabia as a whole.

Overall conclusions on IO.6

161. Saudi Arabia has devoted a significant amount of resource, embedded within LEAs, OCAs and the SAFIU, to order to support financial investigations into ML, TF and associated predicate offences and enable the use of financial intelligence. The SAFIU, LEAs and OCAs have access to large number of sources of administrative and law enforcement related information. The number, and quality of STRs - as reported by Saudi Arabia, submitted by FIs (especially banks), have improved considerably as a result of outreach by the SAFIU and supervisory authorities, although improvements are needed in the DNFBP sector.

162. The SAFIU adds value to the processing of STRs and supports investigations by LEAs by cross-checking, sifting out false positives that it finds and organising and compiling information. However, it is not conducting sophisticated financial analysis to effectively support investigations into more complex cases of ML in particular, and could be doing more to make sure it is disseminating STRs that best support the operational needs of competent authorities while archiving STRs which may not add value. This is likely to be the result of a number of factors, with financial analysts having to manually search databases with STRs taking a long time to process through the SAFIU, a relatively limited amount of resource is devoted to analysis within the SAFIU, limited financial intelligence produced as a result of international co-operation inhibiting the analysis of more complex cases and delays and limitations in the information initially submitted by reporting entities. There is a system in place that allows for co-operation and co-ordination between the SAFIU and LEAs and OCAs in relation to the development and dissemination of financial intelligence, however overlaps within the system may be using up resource and potentially cause delays, given the need for the different authorities to frequently need to co-ordinate.

163. **Saudi Arabia is rated as having a moderate level of effectiveness for IO.6.**

Immediate Outcome 7 (ML investigation and prosecution)

164. The authority responsible for the investigation and prosecution of ML offences in Saudi Arabia is the Public Prosecution (PP). The Economic Crime Unit (ECU) within the PP is responsible for supervising preliminary ML investigations conducted by law enforcement and OCAs, conducting investigations themselves, and prosecuting suspected ML crimes. As explained in the introduction to Immediate Outcome 6, there are a large number of LEAs and OCAs in Saudi Arabia, both in National and Regional Units, with responsibility for the preliminary investigation of suspected ML activity and associated predicate offences.

ML identification and investigation

165. Saudi Arabia has a legal framework that provides it with an adequate basis to investigate and prosecute ML. ML is criminalised on the basis of the Vienna and Palermo Conventions, with Shari'ah providing the basis for an all crimes approach. A new AML law entered into force on 24 October 2017.

166. On 28 February 2017 the PP issued the ML Cases Procedures Manual which broadly serves as a national policy for the identification and investigation of ML cases, promoting a consistent approach by all of the different LEA agencies. It details procedures relating to the various roles and responsibilities between the numerous Saudi Arabian LEAs and OCAs mandated to investigate ML offences as well as the SAFIU and the PP itself. The manual provides detailed guidance and streamlined procedures on the steps to be undertaken when conducting a ML investigation. The drafting of the Manual was a collaborative effort between the PP, LEAs, OCAs and the SAFIU.

167. Due to the importance the Saudi Arabian authorities place on the need to address ML risks and the broad cross-section of agencies involved in investigating and prosecuting ML offences, there are four main ways in which ML offences are identified leading to investigations.

- Following the dissemination of an STR by the SAFIU to an LEA or PP.
- During the course of an investigation into a predicate offence.
- As a result of OCAs noticing potential ML activity during the performance of their functions.
- If the PP come across suspicion of ML when supervising preliminary investigations of predicate offences.

Table 10. Number of ML investigations by trigger type

Year	FIU	During investigation	Other control authority	PP	Total
2013	192	103	11	15	321
2014	136	127	14	18	295
2015	172	538	19	20	749
2016	129	667	23	23	842
2017	288	389	21	25	723

168. While the number of investigations generated as a result of the STRs disseminated by the SAFIU have remained reasonably constant, the number of investigations overall have increased substantially, with the exception of 2017. Saudi Arabia established working groups to co-ordinate with LEAs, OCAs and other government agencies to improve operational efficiency and information sharing in an effort to enhance detection rates, which appears to have been successful overall. Continuing to build understanding across all of the agencies should continue to be a priority. The numbers of individuals responsible for triggering ML investigations totals several thousand, spread across various national and regional offices of the various LEAs and OCAs. The numbers of offences being committed for significant proceeds generating crimes suggests there is more to do in terms of the identification of potential ML and subsequent triggering of an investigation (see table below).

Box 4. Case Study on ML Case Originating from Customs

During regular customs checks at the port of Al-Haditha, a person was found to be in possession of SR 5,362,500, which was hidden in various compartments in his vehicle. The person was not able to justify the legitimacy of the cash. Saudi Customs therefore seized the cash, detained the suspect and referred the case to the relevant LEA. Upon further investigation, the person was found to have a criminal record proving that he was a drug dealer. The LEA gathered information on the financial affairs of the suspect and determined that his lawful income could not have justified the cash in his possession. It was also determined that the suspect was employed as a driver by another person who had been previously arrested on charges of smuggling and slander. The phone records and contents of the conversation between the accused and his employer were analysed which revealed that the cash smuggling operation had been planned between the two persons and other persons.

169. The Saudi Arabian authorities presented a number of case studies to the assessors. In general, parallel investigations are frequently conducted. The financial investigation is conducted by specialised AML Units within the regional offices of each LEA, while working closely with the units conducting the investigation into the predicate offence. AML Units make use of financial analysts with expertise in specific fields, for example in banking, forensic accounting and property valuation. These experts are employed on a case by case basis. Emphasis is placed on the various sources of income and assets of persons to determine whether they justify the legitimacy of the suspects' funds

170. Saudi Arabia was not able to provide any case studies where more sophisticated ML investigation had taken place, and where wider ML activity had been actively pursued.

Box 5. ML Case Originating from SAFIU

An urgent STR was received by the SAFIU from a financial institution pertaining to numerous deposits into a company account by a group of expatriate workers followed by transfers out of the account to a foreign jurisdiction totalling SAR 12 090 225. Information contained in the Commercial Register revealed that the capital of the company did not exceed SAR 25 000. Checks with custom authorities indicated that the company had no import or export activity. Information derived from law enforcement field inquiries revealed that the company had no physical presence and appeared to be conducting no commercial activity.

The case was transferred to the PP for investigation. The investigation revealed that the account holder had rented the company account to a number of foreign workers for a 5% commission fee on all remittances outside the Kingdom. The holder of the account, a Saudi national was convicted of money laundering and sentenced to five years imprisonment and confiscation of the remaining funds in the account. A second non-Saudi was convicted of money laundering and sentenced to one year imprisonment, a fine equal to the funds he had obtained and repatriation from the Kingdom on completion of his sentence.

Consistency of ML investigations and prosecutions with threats and risk profile, and national AML policies

171. The Saudi Arabian risk assessment indicates that crimes committed in Saudi Arabia are estimated to generate annual proceeds in the range of other International bodies' estimates of the proportion of proceeds generated globally (applied to Saudi Arabia to be approximately USD 12 – 32 billion - see IO1), with 82% generated by the top four proceeds generating predicate offences (listed in the table below). It is also estimated that 70% to 80% of domestic POC flows out of Saudi Arabia each year.

Table 11. Number of Investigations of predicate offences for the top 4 proceeds generating offences in Saudi Arabia

Year	Drug offences	Corruption & Bribery	Customs Smuggling	Counterfeiting & piracy of products	Total
2013	2 245	751	2 190	98	5 248
2014	2 956	2 028	2 342	303	7 629
2015	4 112	2 277	2 418	709	9 516
2016	4 097	3 149	2 391	1 036	10 678

Table 12. Number of ML investigations per predicate offence

Year	Drug offences	Corruption & Bribery	Customs Smuggling	Counterfeiting & piracy of products	Total
2014	103	45	13	28	189
2015	262	112	37	74	485
2016	296	126	42	83	547
2017	253	108	36	72	469

172. Broadly speaking, on the basis of the statistics (see table 11 above) and case studies provided, the ML investigations relating to the different predicate offences are broadly in line with the offences that are generating the largest proceeds in the country.. Nevertheless there are too few ML investigations overall to be able to conclude that Saudi Arabia is investigating and prosecuting ML activity in line with the country's risk profile. In addition, no information on the methods or trends used to undertake the ML detected (or suspected of being detected) has been provided, beyond the provision of case studies.

173. As noted above, while the number of proceeds generating predicate investigations isn't insignificant, the ratio of ML investigations to investigations into predicate offences is low. For example in 2016 there were 842 ML investigations (see table 13 below) took place relative to over 10 000 predicate offences occurring (for the top four predicate offences only). This is less than 1 in 10 money laundering investigations stemming from the top 4 proceeds generating crimes. Furthermore, the ratio of investigations that subsequently resulted in a prosecution also appears to be relatively low. While the numbers of ML investigations, prosecutions, convictions and acquittals in each year may not exactly correspond to the same cases (e.g. a conviction in one year may relate to a prosecution from the previous year), there are some clear trends that are evident overall. On average for the three years 2014-16 that statistics were provided, less than 40% of the money laundering investigations lead to a prosecution. The reasons provided by the Saudi authorities for not proceeding with a prosecution included a lack of evidence related to the ML offence and a determination that the suspects of the investigation were innocent of ML offences.

Table 13. Number of ML investigations, prosecutions, convictions and acquittals

Year	ML investigations	ML prosecutions	ML convictions	ML acquittals
2014	295	127	19	24
2015	749	313	36	34
2016	842	295	62	58

174. What perhaps is more concerning is the ratio of cases prosecuted to the ones that end up with a decision in court. Of the 735 prosecutions identified in table 3.9 above for the period 2014-2016, only 233 or 32% end up with a decision in court. This represents only 12 % of the money laundering investigations initiated between 2014 and 2016. The reason for this is unclear. However, Saudi officials noted that the remaining cases prosecuted were either still outstanding, withdrawn, or referred to a different court for a different charge. Having a large number of cases withdrawn or referred to another court for a different charge may indicate that the bar for opening an investigation and pursuing a prosecution is very low and/or a training or evidence gathering issue with respect to the required elements to prove a money laundering

offence. The major deficiency however with Saudi Arabia's system still appears to be the low number of ML investigations originally pursued by LEAs and OCAs in relation to the risk and the number of proceeds generating crimes.

Proceeds of crime entering and leaving Saudi Arabia

175. Saudi Arabia has indicated that they conduct joint investigations with foreign jurisdictions related to ML. Recently there were cases involving informal co-operation with two separate foreign jurisdictions. However, no further cases, statistics or information was provided by Saudi Arabia.

176. This is an important avenue that the Saudi Arabian authorities need to pursue, given that the Saudi Risk Assessment indicates 70% to 80% of domestic proceeds of crime, estimated to be in the range of other International bodies' assessments of the approximate proportion of proceeds of crime to GDP (USD 12-32 when applied to Saudi Arabia – see Chapter 1), flows out of Saudi Arabia each year. Joint ML investigations with foreign jurisdictions are important so as to enable the Saudi authorities to try to recover some of these proceeds and identify other subjects implicated in the offence. While the Saudi authorities indicate that they have on a number of occasions sought information from foreign counterparts, co-operation was either refused or no response was received. Given the large majority of domestically generated proceeds of crime flow out of Saudi Arabia, this has an adverse effect on Saudi Arabia's ability to effectively investigate and prosecute ML activity occurring in Saudi Arabia.

177. During the onsite, the Saudi authorities informed the assessment team that Saudi Arabia was going to improve co-operation with other jurisdictions, including by signing MOUs with other jurisdictions. Enhancing international co-operation and co-ordination in the area of ML/TF also remains part of one of the objectives in the National Strategy (2017-19 and in the 2015-17 National Work-plan). However, the Saudi Arabian authorities have not as yet demonstrated that they have improved the number or effectiveness of joint investigations. Saudi Arabia should apply resources and take steps to improve joint investigations with foreign counterparts as soon as possible.

Types of ML cases pursued

178. The PP, with the aid of LEAs and OCAs, has the authority to investigate and prosecute a wide range of ML offences, including self-laundering, third-party ML and stand-alone ML. The following table identifies ML investigations by type.

Table 14. Convictions by type of ML

Year	Self-laundering	Third party laundering	Stand alone laundering	Total
2013	8	5	2	15
2014	8	2	9	19
2015	17	3	16	36
2016	42	2	18	62

179. Saudi Arabian officials indicated that the majority of ML prosecutions are conducted alongside the prosecution of the predicate offence. In such cases, the

perpetrator of the predicate offence and any linked third parties are prosecuted for ML.

180. Saudi Arabian officials also indicated that the absence of a conviction for a predicate offence is not a legal obstacle to a conviction for ML. There have been several stand-alone ML convictions which were achieved on the basis that, exceptionally, in ML cases, the burden of proof is shifted to the accused. In cases where the financial history of a suspect is found not to correspond to their lifestyle, the suspect is required to prove the legitimacy of their funds. Saudi Arabian officials indicate that there have been at least 20 such cases.

181. The principle of inferring the intent of the perpetrator from objective factual circumstances is well established and routinely applied by the courts. In cases where the ML offence is not prosecuted together with the predicate offence, it is generally sufficient for the prosecution to prove that the funds allegedly laundered do not appear to have a legitimate source and that the accused was not able to provide any justification. In many cases, circumstantial evidence includes the size of the transactions relative to the accused's financial standing, income, activity and failure to account for the origin of funds and/or when the funds came into the possession of the accused.

182. The large of number of convictions for self-laundering in particular appear to refer to cases where Saudi Arabia is convicting individuals where the accused is unable to prove the origin of funds. While this may represent a method for preventing ML, it omits several steps in the effective investigation and prosecution of ML activity. Without further investigation into the origin of the funds or links to other parties it does not support the investigation of an associated predicate offence, nor does it support the investigation of other methods the individual may have employed to conceal the proceeds of crime, should it relate to a predicate offence. In addition, the small numbers of individuals convicted of third-party laundering suggest that Saudi Arabia is not effectively investigating and prosecuting individuals involved in larger scale or professional ML activity.

Box 6. Case Study on ML of the Proceeds of Corruption

A financial institution filed an STR regarding a client (S1) who deposited a cheque issued by a real estate office in the amount of SAR 1 2000 000. The deposit was inconsistent with his employment as a government employee. The SAFIU contacted SAMA who provided information on eight other accounts held by the S1 receiving large amounts of funds and deposits from the same real estate office. Money in these accounts totalled SAR 6,300,000. Searches of the Ministry of Commerce database revealed that the owner of the real estate office was the brother of S1. A search of the Ministry of Justice database revealed that S1 had sold and purchased a property in a short time period. The case was referred to Mabaheth due to suspicion of corruption.

Mabaheth conducted an investigation into S1who was suspected of soliciting bribes for planning approvals in his capacity as the Director of the Planning Department in the Municipality within the region. Further information on the accounts of the real estate office provided by the SAFIU revealed a large number of deposits for large amounts from several individuals. The field investigation revealed little activity at the real estate office as it seemed to be closed most of the time. Intercepted telephone conversations revealed that S1 had an 'agreement' with another individual for speedy completion of the approval procedures relating to a plot of land.

The SAR 6 300 000 was seized and the accused were arrested. Statements from the accused revealed that S1 received bribery money of SAR 1 200 000 from S2 for ensuring speedy approvals with the planning department. S1 had received similar bribery payments from other individuals. S1 made deposits of these bribery payments into the accounts of the real estate office owned by his brother S3 and another individual S4. While the deposits were made in the name of the real estate office it was understood that the true beneficiary was S1 and the purpose of the deposits (and subsequent transfers) were to disguise the origin of the funds.

S1 received a sentence of 10 years imprisonment and a fine of SAR 1 000 000 for bribery and forfeited the SAR 6 300 000 that had been seized. In addition S1 received 3 years imprisonment, a fine of SAR 1 000 000 and a three year travel ban for money laundering. S2 received a sentence of 3 months imprisonment and a fine of SAR 100,000 for breach of duties. S3 received a sentence of 1 year imprisonment, a fine of SAR 500 000 and a two year travel ban for money laundering and S4 received a fine of SAR 500 000 and a two year travel ban for money laundering.

Box 7. Case Study on Third Party Money Laundering

A drug dealer (S1) kidnapped the daughter of a client (S2) for an outstanding drug debt. The father of the girl reported the kidnapping, however the timing of the report and the deportment of the father caused police to be suspicious and look into the affairs of the father as well as pursuing the kidnapping complaint. It was discovered that the father of the girl was under suspicion of drug dealing. The kidnapper was subsequently apprehended and indicated that the father of the abducted girl owed him money. A search of the father's bank account identified numerous deposits including two large deposits (SAR 316 000 & SAR 200 000) made by the father's brother (S3) the uncle of the kidnapped girl. Examination of the uncle's financial activity revealed numerous accounts in the name of his business (foodstuffs) with activity inconsistent with the expected activity for the business. Transfers were made from the uncle's business accounts to his personal accounts. A check of the Ministry of Justice database revealed a recent purchase of a villa by the uncle.

Upon arrest of the three accused it was learned that the father of abducted girl owed money to the abductor for a drug debt. He admitted to transferring proceeds of his drug trafficking activity to the business accounts of his brother (S3) and that the two recent transfers (SAR 316 000 & SAR 200 000) were for completing the purchase of the villa. The uncle admitted that he had set up the business account to receive proceeds from his brother's drug trafficking business and that he had issued a cheque for SAR 815 00 for the initial payment of the villa and that the two deposits to his brother's account (SAR 316 000 & SAR 200 000) were for completing the purchase of the villa.

The kidnapper (S1) was convicted of kidnapping and other drug related charges and received a sentence of fifteen years imprisonment and forfeiture of the car used in the kidnapping. The father (S2) was convicted of drug trafficking and money laundering and was sentenced to 13 years imprisonment and confiscation of SAR 1,901,950 and a luxury vehicle. The uncle (S3) was convicted of money laundering and sentenced to three years imprisonment, forfeiture of the villa, SAR 870,600 and a luxury vehicle.

183. None of the convictions for self-laundering, third party laundering or stand-alone laundering relate to ML activity that has taken place abroad where a conviction has been sought in Saudi Arabia, or relate to cross-border investigations. Given the extent of the proceeds generated in Saudi leaving the country, and the number of individuals entering and exiting Saudi Arabia every year, this represents a significant deficiency.

184. The PP has in place an integrated electronic system for the management of cases. The system allows the PP to conduct high-level analysis of ML cases based on nationality, age and other defining features of the accused, type of underlying predicate offence etc. Through the system, the Head of the ECU may monitor the

progress of all ML investigations and prosecutions and act to ensure that they are concluded in a timely manner. Information from the case management system is also used to inform the AMLPC in tracking policy issues and training needs. In future, should Saudi Arabia more successfully prosecute and convict individuals for participating in ML activity, this tool may help Saudi Arabia track difficulties in cases, and monitor whether the cases are in accordance with the risks.

Effectiveness, proportionality and dissuasiveness of sanctions

185. The prosecution of ML together with the predicate offence may take two forms. ML may be prosecuted as a separate count under the same indictment or prosecuted as a separate indictment in conjunction with the predicate offence. When prosecuted as a separate count, the courts rely on the principle of proportionality to determine the cumulative sentence for both the predicate offence and the ML offence. However, the ML offence is not generally subsumed within the sentence of the predicate offence but rather adds to the severity of the overall sentence.

Table 15. ML convictions and corresponding sentences

Year	Self-laundering	Third party laundering	Stand-alone laundering	Average sentence applied (years)
2013	8	5	2	2
2014	8	2	9	4
2015	17	3	16	3.5
2016	42	2	18	6

186. It is difficult to assess the extent to which the sanctions applied are proportionate and dissuasive given the authorities of Saudi Arabia have not provided more detailed statistics, including whether any other measures are applied including fines and whether or not sanctions have been applied to legal persons (and if so which sanctions have been applied). Nevertheless the sentences do not appear dissuasive in Saudi Arabia relative to sentences for other economic crime offences, with courts sometimes pursing charges for other offences that bring with them more severe sentences.

Use of alternative measures

187. The broad scope of Saudi Arabia's ML offence, where individuals can be prosecuted if they cannot establish a legitimate source of funds, means that it is, in principle, relatively easy to secure convictions and other criminal justice measures may therefore not be required. When taking into consideration the estimated value of proceeds of crime leaving Saudi Arabia and the volume of proceeds generated crimes occurring in the country, high Saudi Arabia does not appear to be proactively pursing 3rd party money laundering to the extent necessary. When ML is pursued, it is the more straightforward cases of self-laundering that are prosecuted.

Overall conclusions on IO.7

188. The framework for the investigation and prosecution of ML cases in Saudi Arabia displays a number of positive elements: ML investigations have significantly

increased in recent years; financial investigations are often conducted alongside the investigation of proceeds generating offences; and awareness raising activities have been organised by the PP to encourage a consistent approach among all LEAs and OCAs.

189. There are, however, areas that Saudi Arabia needs to improve on throughout the process of investigating and prosecuting ML crimes. LEAs and OCAs are not conducting a sufficient number of investigations into ML activity, whether triggered by investigations into proceeds generating predicate offences, or following the receipt of STRs from the SAFIU. When an investigation is conducted, it tends to be reactive rather than proactive. The investigations tend to be unsophisticated and single-layered, predominantly focusing on self-laundering, making use of the wide provisions in the ML offence. This is reflected in the low number of prosecutions being sought and convictions being handed down for 3rd party money laundering, not consistent with Saudi Arabia's risk profile and the nature of the most significant proceeds generating offences, specifically narcotics offences and corruption. When compared to the number of prosecutions initiated by the Public Prosecution for proceeds generating predicate offenses, ML prosecutions are relatively low.

190. The lack of investigations into foreign predicate offences is materially impacting Saudi Arabia's effectiveness in the investigation and prosecution of ML activity, given the large majority of proceeds generated in the Saudi Arabia are transferred abroad. This also needs to be addressed as a priority.

191. Saudi Arabia is working to enhance its methods for collecting statistics to better understand where the weaknesses are in its system and how it can go about addressing them. There is broad reference to improving Saudi Arabia's capacity to discover ML, and analyse, investigate and prosecute ML activity in both Saudi Arabia's 2015-17 Work Plan and the 2017-19 National Strategic Objectives to combat ML/TF. Saudi Arabia needs a more granular and more extensive action plan to improve the investigation and prosecution of ML activity in the country.

192. **Saudi Arabia is rated as having a low level of effectiveness for IO.7.**

Immediate Outcome 8 (Confiscation)

193. Investigations and related seizures are conducted by wide range of LEAs in Saudi Arabia, predominantly the GSD, GDNC, Mabaheth and the PP, but also other LEAs and OCAs for example the Food and Drug Agency and the SAFIU.

194. When there is a suspicion of ML or a proceeds generating predicate offence, the investigating authority (whether an LEA, OCA or the SAFIU) may provisionally seize property for an initial period of a maximum of 60 days or a longer period pursuant to a judicial order from the competent court but shall not prejudice the rights of bona fide third parties as indicated in Article (1/44) of the new AML Law, subject to approval by the PP. The initial period was 30 days until the new AMLL came into force on 24 October 2017 shortly before the onsite visit, with permission from the PP required if the period needs to be extended. According to the ML Procedures Manual the PP must respond to the investigating authority within 48 hours.

195. Upon filing a case of suspected ML or a proceeds generating offence to the court, the PP makes a request that the proceeds associated with the suspected crime,

including those intermingled with legitimate funds, are confiscated. The court reviews the case, hears the submissions of the accused and if the charges are proven, orders the confiscation of the property in addition to the sentence/fine imposed. The judgement is then delivered to the authority that requested the seizure for its execution, and the property is either forfeited in favour of the state or is returned to the victims of the crime.

Confiscation of proceeds, instrumentalities and property of equivalent value as a policy objective

196. Confiscation is defined as a priority in Saudi Arabia as a measure to combat ML and related predicate offences. '*Enhancing capacities to discover the crime and analysis, investigation, litigation, provisional seizure and confiscation in cases of ML/TF*' is one of the eight national AML/CTF strategic objectives that made up the 2015-2017 National Work Plan. Saudi Arabia agreed a new National Strategic Plan in mid-2017 that was adopted by the AMLPC and PCCT, following the completion of the ML and TF NRAs. The National Strategic Plan included the same objective on confiscation as the 2015-2017 National Work Plan. However, the extent that the objectives have been embedded in the objectives of the specific agencies and units responsible for investigating crimes is not clear. Similarly, the more detailed action plan supporting the 2017-2019 National Strategic Plan has been provided but with a lot of redactions of its contents so it is difficult to understand the actions taken in pursuit of the objective or if confiscation of instrumentalities was included as priority.

197. Until October 2017, Shari'ah law was relied upon as the basis to confiscate the proceeds of crime. Shari'ah law requires the confiscation of property derived from a predicate offence, regardless of who is in possession of the property. This was supplemented by separate seizure and confiscation provisions in the different laws applicable to specific crimes, as well as provisions in the 2012 AML law.

198. The new AML law came into force in October 2017, and includes provisions for confiscation of criminal assets, instrumentalities and funds of equivalent value, consistent with the general framework provided for in Shari'ah. The AML law also allows for non-conviction based confiscation in certain cases where the accused has deceased or absconded or where the perpetrator of the offence is unknown (previously the broader provisions under Shari'ah were used for non-conviction based confiscation). Centralising the provisions relating to confiscation in the AMLL may help support awareness amongst the authorities, and the consistency of the application of the provisions.

199. The ML Cases Procedures Manual is provided to all authorities detailing the necessary steps if there is suspicion of ML, but does not cover the process for seizing and confiscating proceeds or instrumentalities of crime. Saudi authorities have organised a series of training programmes to help ensure that competent authorities and the judiciary are aware of the confiscation process. As can be seen from the table below [reference table], there has been a significant increase in the aggregate amount of assets seized and confiscated over the last 3 years, which could be a result of the training programmes that have been conducted.

200. The PP has an internal mechanism to supervise the confiscation process. The head of the economic crime unit (ECU) makes a periodic review of the amounts of

proceeds confiscated relative to the proceeds ultimately seized. If there are thought to be significant discrepancies, the ECD follows up with the Public Prosecutor.

Confiscation of proceeds from foreign and domestic predicates, and proceeds located abroad

201. In cases where the criminal funds are located outside Saudi Arabia, the Saudi authorities have not been able to repatriate any criminal proceeds over the period 2013-16. This impacts Saudi Arabia's ability to confiscate criminal assets to a great extent, as 70-80% of domestic proceeds are estimated to leave the country. Saudi Arabia has made MLA requests in order to attempt to repatriate the proceeds in an ML case [see IO2], but has not been successful.

202. Saudi Authorities provided the assessment team with statistics on the amounts of illegal narcotic substances which are being routinely confiscated, particularly at border crossings where criminals are seeking to transport substances into the Kingdom. This highlights the need for the authorities to more proactively work with competent authorities abroad to confiscate the proceeds of crime leaving the country. Saudi authorities also provided statistics on the 'instrumentalities' of crime confiscated for three of the four top proceeds-generating offences (drug trafficking, corruption and smuggling). However, the figures aggregated proceeds with instrumentalities and the objects of crime (e.g. drugs and counterfeit goods confiscated, vehicles used to transport them), and seizures with confiscations. Saudi authorities were not able to provide disaggregated statistics indicating the amounts of proceeds confiscated in relation to the main offences.

Table 16. Assets seized and confiscated within Saudi Arabia (proceeds of crime, not including assets at the border)

	2013	2014	2015	2016	2017
Cash seized SAR (EUR)	20 099 704 (4 421 934)	18 490 014 (4 067 803)	30 932 124 (6 805 067)	41 975 982 (9 234 716)	62 793 771 (13 814 795)
Cash confiscated SAR (EUR)	7 173 889 (1 578 256)	13 460 213 (2 961 247)	22 772 674 (5 009 988)	28 886 811 (6 355 098)	37 269 484 (8 199 384)

203. In terms of the proceeds, over the period 2013-17 (see table 16 above), the proportion of assets confiscated after the initial seizure has increased to what appears to be a reasonable level. This may be due to the mechanism at the ECU that oversees the confiscation process. In addition, the training programmes for competent authorities appear to have had a positive impact on the value of assets initially seized, which have increased substantially over the period 2013-16. Nevertheless, while the assets seized and confiscated has been increasingly significantly year-on-year, they do not appear to be consistent with Saudi Arabia's exposure to money laundering activity given the size of the country and the nature of the predicate offences occurring (narcotics and corruption offences are estimated to be the predicate offences that generate the largest proceeds in Saudi Arabia's ML NRA).

204. The small number of investigations of ML activity triggered as a result of the investigation into a predicate offence is likely to be a key reason that the assets that are seized and confiscated are low, relative to the risks of ML activity taking place in Saudi Arabia. ML activity is not always being detected, and therefore the authorities are not in a position to be able to trace assets that have been successfully laundered. The large figures of criminal objects (principally seized narcotics) that are being detected and destroyed (see para 171), while suggesting that law enforcement may be doing a good job in detecting certain crimes, also indicates that much more needs to be done to trace, seize and confiscate criminal proceeds, when considering the relatively small amounts of proceeds being confiscated. The case studies provided also suggest that Saudi Arabia is not routinely attempting to trace and confiscate the instrumentalities and proceeds of crime, although they are doing so in some cases.

Box 8. ML Case Originating from Customs

Three persons were charged with ML as they had received large amounts of funds from anonymous sources and could not justify their legality. It was suspected that the funds derived from drug trafficking. One of the accused received SR 1.5 million from an unknown person for onward transfer to another unknown person who in turn transferred the money to the other accused who smuggled the money out of the country. One of the accused persons was also found in possession of SR 38 500 that were intended to be smuggled out of the country, the amount of SR 478 700 in his apartment and counterfeit 100 SR bills. It was determined that the accused intended to hide and conceal the source of the transferred funds knowing that the source of the funds was unknown and couldn't be justified and to transfer those funds. The Court, in determining whether the funds handled by the accused derived from criminal activity, took into consideration the manner in which the funds were received, stored and transferred, which was similar to the manner in which dealers in illegal activities deal with proceeds. The decision was also based on the relationship between the accused and persons outside the Kingdom who instructed the accused on the receipt and transfer of the funds and the frequent travelling of the accused. The accused was convicted of ML and in addition to a sentence and imprisonment, the court ordered the confiscation of SR 1 517 100, mobile devices and a money counting machine.

205. Another factor restricting the seizure and confiscation of criminal proceeds in Saudi Arabia relates to the type and frequency of investigations triggered by LEAs, OCAs and by the PP [See IO7]. Saudi Arabia issued a Ministerial Circulator in November 2017 during the onsite visit that outlines the need for all competent authorities to establish the circumstances when criminal confiscation officers shall commence financial investigations into the original predicate offence, and instructs the seizure of all proceeds of a predicate offence to be frozen. The issuance of rules or guidelines by competent authorities for the benefit of the officials responsible for seizing and confiscating instrumentalities and criminal proceeds may help increase the extent to which criminal proceeds and instrumentalities are confiscated.

Alternatively, or in addition, the authorities may wish to develop a detailed Procedures Manual on seizure and confiscation.

Confiscation of falsely or undeclared cross-border transaction of currency/BNI

206. Given the widespread use of cash in the Saudi economy, the extensive land and sea borders surrounding Saudi Arabia, and the large numbers of individuals entering and exiting Saudi Arabia (there are 10m foreign workers in Saudi Arabia, and approximately 2m people visit Saudi Arabia on pilgrimage each year), the system for monitoring the cross-border movement of cash is an extremely important part of Saudi Arabia's AML/CFT system. There are also a number of politically unstable countries bordering Saudi Arabia or are located close to it, in particular Yemen and Syria, that increase the risks of cross-border cash movements taking place that relate to ML or TF.

207. The Saudi Customs Authority has a sufficient range of powers to seize falsely/non declared cash transported across the borders (land, sea and airports). Saudi Arabia has a declaration system, with individuals required to declare cash BNIs and precious metals and stones (or similar) entering or exiting the country above a threshold of 60,000SAR (approximately 14,200 Euros). The 2017 AMLL extends the obligation to include the declaration of jewelry above the same threshold.

208. Special measures have been put in place to control the funds of pilgrims coming to the Kingdom for the Hajj and Umrah. Hajj and Umrah offices enable individuals to open bank accounts in the Kingdom which are active only for the duration of the Hajj or Umrah (there are Hajj and Umrah offices in all countries where there are large numbers of residents travelling to Saudi Arabia for Hajj or Umrah pilgrimages). Transfers into the account are permitted only from the country in which the Hajj office operates. The disbursement from the account is effected only by issued bank checks, and is deposited only in the name of the Hajj or Umrah offices. The Hajj or Umrah offices must then provide to the authorities in the Kingdom all the names and identification documents, hotel in Saudi Arabia, transportation arrangements etc. of persons authorized under such accounts. The volume of cash carried through the Saudi ports during Hajj and Umrah periods has decreased by more than 99% during the last three years.

209. Separately, a monitoring mechanism is in place at all official check-points that involves the profiling of travelers entering and exiting Saudi Arabia to identify possible suspicions. The Customs Authority has also taken steps to limit the risks of illicit cross-border cash movements across unofficial transit points by increasing its co-operation with the local police force responsible for patrolling the borders.

Box 9. Case study on Confiscation following detection of undeclared cash by Customs

In mid-December 2013, a person driving a truck, with the intention of travelling to the United Arab Emirates, was checked and sent to X-ray machines to ensure they were free of any prohibited or restricted export items. The truck was searched manually outside of Saudi Arabia, where an envelope was found, containing 2.9 million SAR in cash (approximately 640,000 Euro). The driver reported that the amount found was not related to him, but rather, was given to him by another person. The driver did not know the other person's name, but has his mobile phone number.

The driver's information was checked against a database by the Saudi Customs Authority, but no data was found regarding false/non declared amounts, and no other irregularities (in terms of customs information) were discovered. Additional information on the driver was requested from the SAFIU, and it was found that the individual did not have a criminal record. Bank accounts of the individual were requested through the Public Prosecutor's Office, but no accounts were found in the kingdom.

Suspicion was raised on the basis that no records were found concerning the driver. A case file was forwarded to the public prosecution, and the suspect was interviewed by the authorities to try to determine the source of the funds. The suspect stated that he had received the funds from a person in Riyadh, and was not aware of the source of the funds. Due to evidence that the driver had violated the anti-money laundering law through attempting to smuggle funds outside of Saudi Arabia, he was referred to the competent court. The individual was sentenced in mid-May 2014 as follows:

1. The driver was convicted of money-laundering.

2. The driver was imprisoned for two years from the date of his arrest and his removal from the country.

3. The value of the entire amount (2.9m SAR) was confiscated.

210. Cases of undeclared and falsely declared cash declarations are being been identified, both in transit to and from Saudi Arabia – see table 17 below. In these cases, the cash is seized and kept by customs. The SAFIU is also immediately notified. Where insufficient evidence of ML is found by the PP, the cash is released and the person is subject to a fine for non-declaration. A number of case studies provided to the assessment team were triggered as a result of the false or non-disclosure of cash cross-border. Although the law permits BNIs to be seized, none have been seized over the period 2014-16 and it appears that the declaration form did not include BNI at the time of the onsite visit. The new AMLL via the implementing regulations that came into force in November 2017, allow the customs authority to conduct a preliminary investigation into the reasons for a false declaration, failure to declare, or when there is suspicion of ML or a predicate offence.

Table 17. Cross-border declarations by natural persons (incoming and outgoing)

	2013	2014	2015	2016
Arrivals				
Total no of declarations	4 161	4 504	5 972	5 529
Instances of non-declaration	29	17	38	41
Instances of false declarations	20	30	32	49
Departures				
Total no of declarations	7 729	8 363	11 091	11 864
Instances of non-declaration	242	247	388	358
Instances of false declaration	42	70	95	83
Totals				
Total no of declarations	**11 890**	**12 867**	**17 063**	**17 393**
Total no of instances of false declarations or failures to declare	**333**	**364**	**553**	**531**

Table 18. Value of declared and undeclared cash, BNI, gold and precious metal and stones by natural persons (incoming and outgoing) [SAR (EUR)]

	2013	2014	2015	2016
Arrivals				
Total value of declarations (Cash and BNI)	1 854 082 486 (407 898 147)	855 412 198 (188 190 684)	1 363 431 028 (299 954 827)	1 583 079 883 (348 277 575)
Total value of declarations (precious metals and stones)	461 520 618 (101 534 536)	24 861 763 (5 469 588)	701 193 100 (154 262 482)	545 595 271 (120 030 960)
Total undeclared or falsely declared cash	9 986 012 (2 196 923)	13 915 667 (3 061 447)	8 153 401 (1 793 748)	7 744 012 (1 703 683)
Total undeclared or falsely declared BNI	2 550 000 (561 000)	0	0	0
Total undeclared or falsely declared gold	1 572 386 (345 925)	930 200 (204 644)	658 450 (144 859)	1 342 200 (295 284)
Total undeclared previous metals and stones	359 840 (79 165)	430 980 (94 816)	341 550 (75 141)	230 845 (50 786)
Departures				
Total value of declarations (Cash and BNI)	3 413 581 757 (750 987 987)	3 421 648 793 (752 762 736)	4 090 293 084 (899 864 481)	4 505 688 896 (991 251 559)
Total value of declarations	835 395 435 (183 786 996)	1 008 164 376 (221 796 163)	1 636 117 233 (359 945 792)	1 479 523 674 (325 495 209)

	2013	2014	2015	2016
(precious metals and stones)				
Total undeclared or falsely declared cash	56 587 396 (12 449 227)	244 052 505 (53 691 551)	81 561 500 (17 943 530)	75 652 370 (16 643 521)
Total undeclared or falsely declared BNI	4 300 000 (946 000)	0	0	0
Total undeclared or falsely declared gold	524 114 (115 305)	130 150 (28 633)	532 765 (117 208)	744 130 (163 709)
Total undeclared previous metals and stones	175 390 (38 586)	90 460 (19 901)	480 235 (105 652)	124 476 (27 385)
Totals				
Total value of declarations (in and out)	**6 564 580 296** (1 444 207 665)	**5 310 087 130** (1 168 219 169)	**7 791 034 445** (1 714 027 578)	**8 113 887 724** (1 785 055 299)
Total value of false declarations and non- declarations (in and out)	**63 519 126** (13 974 208)	**259 549 962** (57 100 992)	**91 727 901** (20 180 138)	**85 838 033** (18 884 367)

211. Overall, both the numbers of declarations and total amounts declared by travelers entering and exiting Saudi Arabia are large. Given the various contextual factors that impact the expected number of reports (overall number of travelers, extent than the economy is cash-based etc.) it is difficult to know whether the number of reports is appropriate or not. However, efforts by the customs authority in raising awareness of the need to make declarations at transit points has had a positive impact, with the numbers and amounts declared increasing substantially in the period 2013-2016. The Saudi authorities also informed the assessment team that there are also large numbers of declarations representing large sums for legal persons, although these have not been provided. In terms of declarations of cash and BNI through mail and cargo, statistics have also not been provided, although the Saudi authorities have informed the assessment team that restrictions in sending cash through the mail limit the extent sending cash through the mail can occur.

212. As can be seen from table 3.13 and 3.14 above. There is a large discrepancy between the numbers of declarations of incoming travelers and outgoing declarations. The Saudi authorities explained that this was due to the number of foreign workers resident in Saudi Arabia, and due to the fact that Saudi Arabia's income per capita is higher their countries of origin. It should also be noted that the figures are skewed for 2014 on the basis of a particularly large sum of cash that was undeclared by a traveler exiting Saudi Arabia.

213. While Saudi Arabia does not seem to have implemented the cross-border regime for the declaration of BNI, it has implemented a declaration regime for precious metals and stones, including gold. The new AML law also requires the reporting of jewelry above the same threshold as cash and BNI. Given Saudi Arabia has assessed that there is a high level of risk of ML associated with precious metals

and stones, and there is a large market for gold and jewelry in Saudi Arabia and in surrounding countries, this seems an appropriate step.

214. As can be seen from table 3.13 above, the numbers of false and non-declarations being discovered seems relatively low, when considering the total number of declarations being made, although as above it is difficult to make a judgement on what is an appropriate number. A fine of SAR 5 000 (approximately EUR 1 100) has been applied to all cases of false and non-declaration included in the above tables. The fine does not seem dissuasive or proportionate, given the potential incentives for travelers to avoid declaration for example if they are attempting to avoid paying customs duty (although the implementing regulation to the AML law that came into force in November 2017 increases the penalties to 25% of the total or 50% for repeat offenders – a fine that has been assessed as dissuasive and proportionate). However, Saudi Arabia has stated that there are no repeat offenders. The customs department has a database of all those who were involved in false or non-disclosure so that when they enter the kingdom customs and other security agencies are being notified immediately and he will be subject to a comprehensive inspection, which may be acting as an effective deterrent.

215. Saudi Arabia provided information on the amounts confiscated at the border when there is suspicion of ML, TF or a predicate offence: In 2014, SAR 1 520 746 was confiscated (approximately EUR 335 000), in 2015 SAR 2 418 678 was confiscated (approximately EUR 530 100), and in 2016 SAR 2 975 519 was confiscated (approximately EUR 655 000). It is not clear whether the subsequent investigations by the PP led to a formal investigations into ML, TF or a predicate offence, and whether any of the investigations ultimately led to a prosecution and a conviction.

216. While the amounts confiscated have been increasing, they remain low relative to the numbers of visitors to Saudi Arabia and the number of declarations. Saudi Arabia has secured positive results in increasing the numbers of declarations and the amounts declared. Focusing more attention and investigative resources on following-up on declarations that may be related to ML, TF or a predicate offence could help address this issue more effectively. Such follow-up could be done by customs (using the powers granted in the November 2017 AML law) of in co-operation with other authorities.

Consistency of confiscation results with ML/TF risks and national AML/CFT policies and priorities

217. The figures provided for the proceeds of crime confiscated in Saudi Arabia are not consistent with the number or the nature of predicate offences occurring within the country. This includes the large scale proceeds generated from narcotics offences, corruption, smuggling and counterfeiting. The lack of the successful confiscation of assets outside Saudi Arabia represents a significant deficiency, with the large majority of proceeds generated in Saudi Arabia (70-80%) moving out of the country.

218. The Saudi Authorities informed the assessment team that the most significant amounts seized and confiscated are from the proceeds of narcotics and corruption offences, in line with the findings of the ML NRA (although there could be a case of confirmation bias, certainly to some extent). The assessment team also noted that the case studies presented were consistent with the predominate proceeds generating

predicate offences occurring in Saudi Arabia, although it is difficult to draw any broad conclusion on the basis of a relatively small number of case studies.

219. More detailed statistics of the proceeds confiscated would help Saudi Arabia to understand whether the assets seized and confiscated are in line with Saudi Arabia's risk profile. The PP already has a case management system to enable it to trace ML cases from the investigation stage through the court process should the PP pursue a prosecution. The system allows the PP to assess whether assets are being confiscated effectively once they have been seized. Collecting statistics on the predicate offences that the assets confiscated relate to and the types of assets confiscated, for example, would help Saudi Arabia to better understand the strengths and weaknesses in the system and the patterns used by criminals to conceal or disguise the proceeds of crime.

Overall conclusions on IO.8

220. Saudi Arabia is not effectively confiscating the proceeds of crime relative to its risks. Expanding the system at the ECU that tracks cases to include the types of predicate offence could help Saudi Arabia gain a more detailed understanding of the extent to which the proceeds of crime confiscated are in line with Saudi Arabia's risk profile.

221. Shortcomings in Saudi Arabia's system under IO2, IO6 and IO7 mean that it is difficult to ascertain whether Saudi Arabia's system for confiscation is ineffective, or whether weaknesses in the detection, investigation and prosecution of the proceeds of crime, and ineffectual International Co-operation are limiting the possibility of confiscating the proceeds and instrumentalities. Should Saudi Arabia embark on an action plan to improve the effectiveness of the use of financial intelligence by law enforcement, it should at the same time ensure that LEAs and other competent authorities are also aware of the process for seizing and confiscating criminal assets and ensure that they use the tools at their disposal to do so effectively. It has already begun to do this, including by issuing a ministerial circular in November 2017 highlighting the importance of competent authorities seizing and confiscating the proceeds of crime, and including an objective in its 2017-19 National Strategic Plan on enhancing capacities to seize and confiscate assets in cases of ML and TF. The increasing quantities of proceeds confiscated, albeit to amounts that are modest relative to the risks, suggests that Saudi Arabia's efforts to enhance capabilities to seize and confiscate criminal proceeds under the 2015-2017 National Work Plan has been successful to an extent.

222. Saudi Arabia has taken measures to respond to the heightened risk associated with the large numbers of individuals entering and exiting the country every year, implementing measures to limit the amounts of cash brought into the country by individuals on pilgrimage. In addition, educating travelers on the need to submit declarations at the border appears to have resulted in an increase in the number of declarations being made and the amounts declared. However, more can be done to detect and seize funds at the border that are suspected of being related to ML, TF or predicate offences.

223. **Saudi Arabia has a low level of effectiveness for IO.8**.

CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

Key Findings and Recommended Actions

Key Findings

- Saudi Arabia's overall strategy for fighting terrorist financing mainly focuses on using law enforcement measures to disrupt terrorist threats directed at the Kingdom and its immediate vicinity. While this is an understandable priority, the almost exclusive focus of authorities on domestic TF offences means the authorities are not prioritising disruption of TF support for threats outside the Kingdom. They are also not taking full advantage of TFS to enhance the disruptive impact of their law enforcement actions both in Saudi Arabia and beyond their borders. Saudi authorities are particularly focused on domestic TF offences at the expense of international TF networks, which has an effect on their approach to both Immediate Outcome 9 and Immediate Outcome 10.

  Terrorism financing investigation and prosecution – TF offense (Immediate Outcome 9)

- TF cases are generally identified during terrorism-related investigations conducted by Mabaheth. The various authorities dedicated to anti-terrorism have successfully identified, investigated and prosecuted many TF cases within the Kingdom.
- Saudi Arabia has demonstrated an ability to respond to the dynamic terrorism threat it faces in country. For instance, in 2017, Saudi authorities were able to adapt and increase their attention on domestic terrorist cells while remaining vigilant with respect to the TF threat posed by foreign terrorist fighters (FTFs).
- Financial investigations are routinely carried out in connection with terrorism cases. A range of investigative techniques are used to find evidence of TF activity, including preventative terrorist financing measures (mainly pertaining to FTFs), phone interceptions and social media scrutiny.
- Saudi Arabia has investigated, prosecuted and secured convictions on a high number of TF cases. However given the high risk of TF in relation to funds raised in the Saudi Arabia for support of terrorist entities outside the Kingdom, particularly outside the Middle-East region, as partly identified in the NRA on TF the number and types of cases focused on this area is inconsistent with the risk profile.

- In addition there is little evidence, other than TF investigations related to foreign terrorist fighters, that Saudi authorities proactively pursue TF cases as a preventative measure to terrorism within the Kingdom. TF related targeted financial sanctions and NPOs

Preventing terrorists from raising, moving and using funds (Immediate Outcome 10)

- Saudi Arabia has an established legal framework and co-ordination process for implementing targeted financial sanctions (TFS) without delay under the relevant United Nations Security Council Resolutions (UNSCRs). Saudi Arabia has co-sponsored designations to the 1267 UN Committee and has partaken in de-listing and exemption requests. Saudi Arabia has not proactively nominated individuals or entities to the UN for designation as would be expected considering the risk-profile of the country. Domestically, Saudi Arabia has made significant use of designations under the UNSCR 1373 system, accepting 41 designation requests from foreign countries and, up through 2016, designating 150 individuals on its own motion.
- Even though domestic designations are largely communicated to FIs and DNFBPs, there is no publicly available list of designees or guidance regarding implementing obligations, which hinders effective and consistent sanctions implementation.
- Saudi Arabia prefers other mechanisms than TFS, including criminal investigations and prosecutions, to deprive terrorists and terrorist financiers of their assets and instrumentalities. As a consequence, the largest number of freezes is made by applying financial restrictions on suspected persons on the basis of the criminal law to counter TF. The Saudi authorities consider that these have greater dissuasive and effective results rather than targeted financial sanctions, nevertheless these do not provide for legal processes in line with targeted financial sanctions and the FATF Standards, and may not be communicated to all the relevant domestic and foreign stakeholders. Assets and instrumentalities related to terrorism and terrorist financing are effectively confiscated after prosecution.
- The PCCT does not have sufficient resources to deal with all its competing mandates.
- Saudi Arabia's NPO sector is very small in number and tightly regulated. NPOs utilise the financial sector for virtually all their transactions are under tight control for fundraising activities, and have highly restricted access to international transfers in and out of the country. In addition to these measures, Saudi Arabia has taken steps to raise awareness of TF abuse risks within the sector and the public at large. These measures have had the effect of drastically reducing the risk of terrorist financing abuse in the sector. However, NPOs continue to be treated by FIs/DNFBPs as high-risk clients for terrorist financing. In 2017 Saudi Arabia began analysing information derived from compliance visits of NPOs to implement a risk-based approach based primarily on financial integrity.

PF related targeted financial sanctions (Immediate Outcome 11)

- The Kingdom of Saudi Arabia established a Chapter VII committee in 2006 which serves as an interagency body for sharing information related to all Chapter VII UNSCRS including those related to proliferation financing (PF) and weapons of mass destruction. Saudi Arabia established mechanisms for implementing UN TFS related to WMD proliferation in November 2017.
- Saudi Arabia has not frozen any assets or blocked any transactions as a result of TFS related to PF.
- There are significant delays in implementing and communicating new TFS relating to PF – both within the public sector (from the Chapter VII Committee to the relevant authorities) and with the private sector.
- Financial institutions screen all UN lists on an automatic daily basis to check for UNSCR updates – and did so prior to the recent introduction of the Mechanism. Nevertheless, FIs and DNFPBs have a weak awareness of PF risks and of the potential for sanctions evasion, which is fairly significant given Saudi Arabia's geographic location.

Recommended Actions

Immediate Outcome 9

- To keep in line with the risk-profile of the country, in addition to domestic cases, Saudi Arabia should also prioritise TF cases generating from within the Kingdom and going abroad, including beyond the Middle-East region. This should include proactive TF cases that would have a disruptive effect on the raising of funds within Saudi Arabia for support of terrorist entities outside the Kingdom.
- Saudi Arabia should pursue proactive TF cases as a tool to prevent terrorism offences occurring in the first place and financially disrupt terrorist groups.
- With a view to positively affecting the dissuasiveness of sanctions relating to TF offences, Saudi Arabia should look for ways to enhance the transparency of court proceedings, and publish in greater detail the results of court outcomes related to TF cases.
- In order to ensure the full development of all investigative methods and to develop jurisprudence in relation to financial investigation techniques and prosecutions, Saudi Arabia should reduce the reliance on confessions to secure convictions in TF cases, particularly in light of the new CFT Law.

Immediate Outcome 10

- Saudi Arabia should develop a consolidated and comprehensive list of 1373 domestic designations and make it publicly available to all supervisory and FIs, DNFBPs, and natural and legal persons to facilitate communication and effective implementation of targeted financial sanctions. Saudi Arabia should similarly make guidance publicly available so that all natural and legal persons understand their obligations for implementing TFS and to ensure designated individuals are familiar with their rights as bona fide parties.

- Given Saudi Arabia's use of domestic sanctioning authority, the country should independently nominate individuals and entities for designation to the UN, and should extend requests to other countries for 1373 designation consideration in an effort to enhance the impact of sanctions beyond Saudi Arabia's jurisdiction.
- With a goal of enhancing the impact of targeted financial sanctions to the greatest extent, Saudi Arabia should reduce reliance on financial restrictions based on watch-lists in favour of targeted financial sanctions to deprive terrorist financiers access to their assets.
- Saudi Arabia should provide additional resources to the PCCT, in an effort to alleviate capacity challenges that hinder the effective implementation of targeted financial sanctions.
- The supervisors should monitor and enforce the effective implementation of TFS by real estate agents and DPMS. Saudi Arabia should also strengthen awareness and supervision of smaller DNFBPs to ensure the implementation of targeted financial sanctions without delay.
- Saudi Arabia should fully implement the risk-based approach to supervision, which has started in 2017. Saudi Arabia should use the information derived from the compliance visits with NPOs to identify measures that could be simplified for some organisations that would have an effect of enhancing legitimate NPO activities. In addition, Saudi Arabia should provide guidance to FIs and DNFBPs that NPOs are low risk for TF due to the measures in place.

Immediate Outcome 11

- Saudi Arabia should establish a system that ensures full implementation of proliferation-related TFS by FIs and DNFBPs without delay. The remaining technical gaps should also be addressed.
- Saudi Arabia should revisit the current co-ordination mechanism for all relevant authorities, including SAFIU, to ensure sharing information and detecting and responding to proliferation related sanctions threats occur in an effective manner.
- Saudi Arabia should provide clear direction and guidance to FIs and DNFBPs to support proper implementation of TFS related to PF. Saudi Arabia should conduct outreach to increase awareness regarding the characteristics and typologies associated with sanctions evasion relating to PF amongst FIs and DNFPBs.

224. The relevant Immediate Outcomes considered and assessed in this chapter are IO.9-11. The Recommendations relevant for the assessment of effectiveness under this section are R. 1, 4, 5–8, 30, 31 and 39.

Immediate Outcome 9 (TF investigation and prosecution)

225. The risk of terrorist financing in Saudi Arabia is high, with threats related to the fundraising for terrorist groups operating in Saudi Arabia and outside Saudi Arabia, and in relation to foreign terrorist fighters.

226. Mabaheth is the law enforcement responsible for conducting investigations of terrorism and terrorism financing offences in Saudi Arabia. A specialised unit within the Public Prosecution Office (PP) is responsible for TF prosecutions and Saudi Arabia has established a specialised criminal court and a court of appeal to adjudicate terrorism and terrorism financing cases.

Prosecution/conviction of types of TF activity consistent with the country's risk-profile

227. Saudi Arabia faces a high and diverse risk of terrorism financing, which includes the financing of terrorism both within and outside Saudi Arabia. Saudi Arabia also faces a high risk of terrorist acts carried out in Saudi Arabia, as can be seen by incidents of attacks on Saudi Arabian territory. The risk of terrorism and terrorist financing within Saudi Arabia is linked to the presence of cells of Al Qaeda, ISIS, affiliated groups, and other groups identified by Saudi Arabia. The number of foreign fighters is significant, relatively to the population. The risk of financing of terrorist group abroad is linked to the many Saudi foreign fighters who travel, or attempt to travel, to conflict zones and to individuals who may raise funds and move assets from Saudi Arabia.

228. In August 2017, Saudi Arabia produced a separate National Risk Assessment on TF. The main finding of the NRA on TF revealed that TF risk still exists in Saudi Arabia and the Kingdom should ensure that addressing TF risk remains a priority. The international political situation, the lack of stability in the region, the presence of terrorist groups neighbouring Saudi Arabia and the presence of terrorist cells within the Kingdom were all identified as reasons to assess the likelihood of TF as high with certain risks believed to be on the increase. Among the vulnerabilities are the presence of some foreign communities, the calls by individuals to raise non-official contributions domestically and internationally for human purposes, and the use of social media. Saudi Arabia has taken significant steps to reduce and mitigate these risks, as discussed under IO.1.

229. Terrorist fundraising risk has been identified primarily through collection of cash and historically through the abuse of the need to provide charity. Those avenues have been addressed through initiatives towards a cashless society, by tightening up regulation and supervision of the NPO sector and through awareness raising (see IO.10 below).

230. The summary national risk assessment revealed that TF risk still exists in Saudi Arabia and the Kingdom should ensure that addressing TF risk remains a priority. The main TF threats to Saudi Arabia were identified as:

- raising funds inside the Kingdom and transferring them outside the country for the support of external terrorist groups;
- raising funds inside the Kingdom and transferring them outside the country for the purchase of weapons to be smuggled back into the Kingdom;
- raising funds inside the Kingdom for the purpose of carrying out attacks inside Saudi Arabia;
- funds coming from outside the Kingdom for the purpose of carrying out attacks inside Saudi Arabia or as a transit point for another country; and,

- raising funds inside the Kingdom for the purpose of facilitating the travel of foreign terrorist fighters.

231. Saudi Arabia has convicted for TF offences a large number of people affiliated with a host of different terrorist groups. Between 2013 and 2016, 1 743 persons were prosecuted for the crime of terrorist financing. In the majority of cases, a guilty verdict was passed by the courts, convicting 1 133 persons.

Table 19. Number of TF Convictions by year and affiliation

	Al-Qaeda	ISIS	Al-Nusra Front	Taliban	Lashkar-e-Taiba	Hezbollah
2013	366	-	-	2	4	1
2014	245	334	-	2	-	2
2015	24	79	2	-	-	-
2016	14	53	4	-	-	1
Total	**649**	**466**	**6**	**4**	**4**	**4**

Note: * The table only represents those terrorist financing convictions related to terrorist groups identified by the United Nations and domestically by Saudi Arabia. The Saudi authorities maintain that these convictions are consistent with Article 2 of the International Convention for the Suppression of the Financing of Terrorism (see R.5 Criterion 5.1).
Source: SCC, Mabaheth.

232. As noted in Recommendation 5, the definition of terrorism is overly broad and includes non-violent actions, such as any act with the intention to disturb public order, undermine state reputation, and attempt to coerce Saudi authorities into a particular action. This broad definition of terrorism may contribute to a higher number of investigations and convictions into TF. In addition to the figures above, there are also other prosecutions and convictions for TF in Saudi Arabia that are not linked to the terrorist groups mentioned above, and Saudi Arabia did not provide statistics or information on these cases. Because of the overly broad definition of terrorism in Saudi Arabia, it is possible that the authorities pursue cases of financing of acts that would not be included in universal counter-terrorism instruments, and as such divert attention and resources to specious cases from more important cases of TF.

233. The case management system used by the PP allows the Saudi authorities to classify the TF cases by the type of substantive TF charges. The following box presents the types of TF prosecution and convictions conducted by Saudi Arabia.

Box 10. Case Study on Financing of a foreign terrorist fighter (ISIS)

After a bombing, Mabaheth collaborated with a foreign country (Kuwait) to identify the responsible and the facilitators. Three people were arrested in Kuwait, including a Saudi national who was extradited to Saudi Arabia. During interrogation, the Saudi national confessed that a vest was delivered to Kuwait in his brother's car; however, the owner was not aware of the purpose of the trip. The Saudi national confessed that he had paid SAR 10 000 to provide medical care to one of his brothers who was fighting

in Iraq with ISIS. It is not known to whom the money was paid to as the cash was left in a bag for pick up. The Saudi national was convicted to 4 years in jail (3 years for attempting to travel to a conflict zone and 1 year for paying SAR 10 000 for the purpose of supporting a foreign fighter).

Box 11. Case Study of an attempt to smuggle weapons from Yemen (Eastern Province of Saudi Arabia)

A Saudi national, part of a terrorist network in the country's eastern province, was attempting to smuggle arms into Saudi Arabia. The Saudi national was planning to buy 110 RPGs and 40 shells for SAR 370 000. The Saudi national met with a Yemeni national to negotiate the smuggling of the weapons. The plan was to smuggle the weapons into Saudi Arabia through an eastern port. The Yemeni national informed to Mabaheth on the Saudi national and a controlled delivery was arranged. The Yemeni national asked for a deposit of SAR 50 000 to be delivered to a third party in a city near the eastern port. The SAR 50 000, documented by Mabaheth in photos, was paid by the Saudi national to the third party.

The Saudi national was subsequently sentenced to 15 years in prison (2 years for dealing in weapons and munitions, 8 years for sympathizing with terrorists and 5 years for terrorism financing). The SAR 50 000 was confiscated and forfeited.

Box 12. Case Study of an attempt to leave Saudi Arabia for the purpose of fighting with ISIS (FTF)

A Saudi national requested a credit card to be opened in a nickname. The bank issued an STR. Monitoring of social media activity revealed his radicalisation and affiliation to ISIS. Phone tapping indicated that the Saudi national was in contact with another person abroad to organise a travel to a conflict zone. As the Saudi national attempted to leave the country, he was arrested at the airport by Mabaheth and SAR 57 000 was seized from him. The Saudi national confessed he was travelling to a conflict zone to join ISIS. He was sentenced to 11 years (7 years for attempting to travel to conflict zone and 4 years for carrying money and attempting to deliver it to a terrorist group).

Box 13. Case Study of Financing of propaganda

During an investigation, information was obtained that a Saudi national had provided logistical support to Al-Qaeda members and facilitated the targeting of citizens, residents and security personnel from the General Intelligence. The Saudi national was arrested. During the interrogation, the Saudi national stated that he provided support to members of a local Al-Qaeda cell (5 members). The Saudi national had harboured some members in his home; he provided them with a fixed telephone and a laptop to access the Internet in order to prepare the publication of documents supporting the Al-Qaeda terrorist ideology for recruitment. He also provided other means of support, including a sum of SAR 2 100 and helped them in the escape of wanted persons and transferred their equipment.

He was sentenced to 17 year prison term and banned from travel for a similar period after his release. In addition he was fined to SAR 5 000. It is unclear what the sentence for TF was.

Box 14. Case Study on Financing of terrorism outside Saudi Arabia

A Saudi national and ISIS sympathizer (S1) travelled to a foreign country to meet with a foreign national (S3) to discuss fund raising for ISIS. S2 asked S1 to open an account in Saudi Arabia to receive donations of money intended to support ISIS because S2 cannot open an account in Saudi Arabia. S1 initially agrees. Upon returning to Saudi Arabia, S1 inform S2 that he cannot open the account as he is concerned, due to warnings issued by the Ministry of the Interior that he will not be able to justify the activity in the account based on his income. S2 then indicates that he will arrange for the money to get to S1 via another individual (S3). S3 subsequently meets with S1 and hands over EUR 200 000. S1 then contacts another Saudi national (S4), who is also an ISIS sympathizer, and asks him to arrange for the money to be transferred to Syria. S4 whose communications are being monitored by Saudi authorities indicates that he will be travelling to Syria and can make the delivery. S1 subsequently gives the money to S4. S4 is arrested while attempting to leave Saudi Arabia bound for a country neighbouring Syria. S4 is found in possession of EUR 203 200 (the EUR 200 000 from S1 and EUR 3 200 of his own money for expenses).

S4 was convicted and sentenced to 10 years in jail and the money was forfeited.

234. A large number of Saudi TF cases relate to the financing of travel by foreign terrorist fighters and the subsequent financing of foreign terrorist organisations and their facilitators. Some cases relate to the support and financing of active terrorist cells affiliated with ISIS (and with Al Qaeda), as well as networks of terrorists active

in Saudi Arabia. Saudi officials have prosecuted offenders from the various types of TF activity including the provision, raising, transfer and use of funds. Around 10% of the TF prosecutions and convictions relate to TF committed outside Saudi Arabia. These external cases relate to the financing of terrorist groups by persons who travelled or attempted to travel to Syria and Iraq to join ISIS or Al-Nusra Front.

235. It is clear that Saudi Arabia prosecutes and convicts a large number of people for terrorist financing. However TF is often prosecuted as an ancillary offence to other terrorism-related crimes.

236. There are no, or very few, convictions for terrorist financing that are independent from the prosecution of other terrorist-related offences. There are also no, or very few, prosecutions and convictions of persons who are financing terrorism and who are not involved in the commission of terrorist act or affiliated with these terrorist groups. Around 10% of the TF prosecutions and convictions relate to TF committed outside Saudi Arabia. These external mainly cases relate to the financing of terrorist groups by persons who travelled or attempted to travel to Syria and Iraq to join ISIS or Al-Nusra Front. However, given that the support for external terrorist groups is a major TF risk for the country, the overall number of cases pertaining to raising funds inside Saudi Arabia and transferring them outside the country is low.

237. In sum, while the types of prosecutions and investigations of TF offences by Saudi Arabia responds to the risk of TF related to the presence of terrorist groups inside Saudi Arabia and the large number of foreign fighters from Saudi Arabia. With the exception of FTF cases, Saudi has not yet tackled the risk of financing of terrorism by third-party and facilitators, and the financing by individuals for terrorist organisations outside the country.

TF identification and investigation

238. Saudi Arabia, as evidenced by the table below, pursues TF investigations stemming from a variety of sources.

Table 20. Trigger of TF investigations - Identification of TF Cases

Year	FIU/STR	Reports from the Public	Terrorism Investigation	Foreign Counterparts	Total
2013	24	19	146	17	**206**
2014	23	12	86	7	**128**
2015	15	6	77	3	**101**
2016	16	7	51	2	**76**
Total	**78**	**44**	**360**	**29**	**511**

239. All TF STRs submitted by reporting entities to the SAFIU are immediately forwarded to Mabaheth, where financial investigators analyse the information, while other units conduct field enquiries. At the same time, the SAFIU proceeds with its analysis and disseminates an analysis report to Mabaheth consisting of detailed information related to bank accounts held and other relevant information (see Immediate Outcome 6). Where additional information is needed to identify possible links, SAMA is requested to obtain additional information from FIs.

240. While there are relatively few international terrorist financing investigations, Mabaheth maintains regular contact with its foreign counterparts both within the region and beyond (see table 39 included in the analysis of IO.2, in chapter 8). Mabaheth exchanges information with foreign counterparts on an ongoing basis throughout the life-cycle of most terrorism and TF investigations. Saudi Arabia has identified a number of TF cases based on information received from foreign counterparts.

241. Within Mabaheth, a specialised Department of Financial Investigations made of 56 staff members works on financial investigations. Financial investigation staff receive training in conducting financial investigations. Financial investigations are routinely carried out in the context of a terrorist investigation. Their focus is to trace the movement of funds in the bank accounts and establish links with terrorist organisations outside Saudi Arabia or with terrorist cells within Saudi Arabia. They also focus on identifying transfers to high-risk jurisdictions. Mabaheth co-ordinates with all relevant authorities and requests financial data from appropriate supervisory authorities

242. A range of investigative techniques are used to find evidence of TF activity, including phone interceptions, social media scrutiny, and controlled transfers with persons subject to targeted financial sanctions. Information is also often collected from FIs and government agencies.

243. When an investigation is concluded, the case is passed to the special unit within the Public Prosecution Office (PP) which will decide whether to bring the case to the Specialised Criminal Court (SCC) for trial. The role of the PP is to consider the evidence collected by Mabaheth, and decide whether this is enough to justify referral to court. In majority of cases, the PP considers that the information collected by Mabaheth is sufficient for a trial. In a minority of cases, PP requests Mabaheth to collect more information in relation to the specific case, or to further explore possible links.

Box 15. The Specialised Criminal Court

The Specialised Criminal Court (SCC) was established in 2008 in response to the increasing terrorist threat posed to Saudi Arabia in the early 2000s and the thousands of detainees waiting for a trial in terrorism-related charges. The SCC falls under the jurisdiction of the Supreme Judicial Council Cases can be appealed to a Court of Appeal within the SCC, and in some circumstances they can be brought to the Supreme Court. The CFT Law passed in December 2013 formally codified the SCC jurisdiction on all cases related to terrorism, including terrorist financing.

244. TF is primarily investigated and prosecuted as an ancillary offence to terrorism charges. Most persons convicted for terrorism also received a TF conviction since in most terrorism cases, an individual would perform many roles, such as facilitating, financing, and/or carrying out terrorist operations within a single cell. It should be noted that virtually all convictions for TF included a confession or a denunciation by an implicated witness.

245. The Specialised Criminal Court for terrorism and TF offences, the dedicated unit within the PP focused on TF prosecutions along with the General Department of Financial Investigations within Mabaheth has allowed Saudi Arabian authorities to successfully identify, investigate and prosecute many TF cases within the Kingdom.

Box 16. Case Study on Investigation of Foreign Terrorist Fighters (FTFs)

An individual reported to the 990 public hotline that his brother (a Saudi national) left Saudi Arabia for a transit country with the intention to join ISIS in Syria. Once the Saudi National had arrived in Turkey, he paid USD 2 000 to an ISIS-trusted facilitator. During an unrelated raid by security forces, Turkish authorities arrested the Saudi national and four other men attempting to travel to Syria. Turkey deported the Saudi national back to Saudi Arabia, where he was arrested by Mabaheth at the airport. SAR 4 500 and an I-pad were seized from the Saudi national upon arrest. The Saudi national confessed and was sentenced to 13 years of prison (8 years for attempt to travel to conflict zone, 4 years for electronic crimes linked to terrorist propaganda, and 1 year for self-financing his travel and financing a terrorist group through a facilitator). The I-pad and SAR 4 500 were confiscated.

The investigation involved several departments within Mabaheth, such as the International Department, General Department of Financial Investigations, and the Operational Department. The investigation was supported by FIU analysis, and included international co-operation. The SAFIU checked its own databases and the travel history of the person (negative). Mabaheth monitored the social media account of the Saudi national, finding evidence of support and affiliation to ISIS. The International Department of Mabaheth liaised with Kuwait (the first transit country) and learned that he was travelling to Turkey (the second transit country). Mabaheth obtained bank statements through SAMA, revealing that the person only had SAR 100 left in the account, and that he was receiving a university scholarship and support from the father. The bank account was subsequently frozen.

The I-pad contained terrorist propaganda material (jihadist videos and pictures). The confession revealed the co-ordination with a person in Syria. The Saudi national financed the travel and the payment to the facilitator by selling his car for SAR 8 500.

TF investigation integrated with –and supportive of- national strategies

246. Following the adoption of the national risk assessments on ML and TF, the AMLPC and PCCT identified eight strategic objectives to reduce the risk of ML/TF as follows:

- Enhancing local and international co-operation and co-ordination in the area of combating ML/TF;

- Enhancing capacities to discover the crime and analysis, investigation, litigation, provisional seizure and confiscation in cases of ML/TF;
- Ensure the existence of understanding and assessment of ML/TF risks within the entities subject to supervision;
- Enhancement of capacity building and training programs in the area of combating ML/TF;
- Raising the level of awareness of combating ML/TF;
- Reduction of reliance on cash and curbing financial remittances through informal systems;
- Enhance knowledge of beneficiary ownership; and,
- Enhancing technology in the area of ML/TF.

247. While the development of these strategic objectives is relevantly recent, in the area of TF investigations, Saudi Arabia experience in investigating TF offences has guided their understanding of financial investigations throughout the Kingdom. As evidenced by the number of information exchanges with foreign jurisdiction outlined in the table above, Saudi Arabia has capitalised on international co-operation and co-ordination in the area of TF investigations. The counter-terrorism and counter-terrorism financing framework has significantly evolved since the 2000s, with a CFT legislation providing the investigators with enhanced tools related to provisional detention and seizures and by establishing the specialised criminal court to hear cases and the penalties for violating the law. These have enhanced the capabilities of the Saudi authorities to successful prosecute terrorism and TF crimes.

248. The number of prosecutions advanced by Saudi Arabia has demonstrated the willingness and ability to pursue TF cases resulting from STRs and leads from the public with respect to FTFs, as a matter of routine in parallel with terrorism offences and through international co-operation with those in the region and beyond. The specialised financial investigators within Mabaheth receive advanced training on conducting financial investigations. This coupled with a dedicated unit within the PP and a specialised court to hear terrorism and TF cases has allowed Saudi Arabia to address the risk of TF in the Kingdom effectively.

249. Mabaheth has demonstrated a considerable capacity to react to the changing environment of terrorism and by extension TF in the country. As ISIL leaders in 2017 indicated that Saudi nationals would serve the terrorist group more effectively by remaining in the Kingdom and perpetrating terrorist acts as home, Saudi authorities were able to adapt and increase their attention on domestic terrorist cells while remaining vigilant with respect to the TF threat posed by FTFs.

Box 17. Dealing with Foreign Terrorist Fighters (FTFs)

Since 2011, approximately 2 800 people have left Saudi Arabia to fight for terrorist organizations outside of the Kingdom, predominately Syria. Ninety eight percent of FTFs are Saudi nationals between the ages of 17 – 30, with only 2% being migrant workers living in Saudi Arabia. In 2014, Saudi Arabia has criminalised FTFs with a sentence of 3 – 20 years in prison. Saudi Arabia established a public hotline (990) where to report cases of radicalisation or suspect terrorist activity. While many FTFs are identified by the public, in particular family members, Saudi authorities identify and expand cases through social media monitoring.

Saudi officials have been particularly successful in reducing the risk of funding for FTFs (usually after they have left) by the use of provisional seizures of their bank account and close monitoring of their family's accounts (to prevent them from being the victims of ransom scams).

Table 21. Foreign Terrorist Fighters (FTFs) from Saudi Arabia during 2000-2018 (12 February)

Left Saudi Arabia	3 389
Returned to Saudi Arabia	825
Deceased	1 117
Active	1 447

250. Financial investigations are regularly carried out in the context of terrorism-related inquiries. This work, done by a dedicated unit with Mabaheth in close co-operation with other departments, is very useful in a counter-terrorism investigation to identify movement of funds and bank accounts to be frozen. There is indication that some on-going financial investigations support the tracing of assets and the identification of wider networks.

Box 18. The Use of Social Media Monitoring to Combat TF

Saudi Arabia utilises monitoring of social media as a technique to identify potential terrorists and terrorist financiers.

Within the Ministry of the Interior (currently the State Security Presidency), Mabaheth monitors and follows up on what is published on the Internet and social media related to terrorism and its financing. The unit then refers individual targets to local investigative authorities. Bank accounts suspected of being used to raise funds are reported to competent authorities to take necessary actions with respect to seizure and stopping remittances to foreign accounts in accordance with resolution 1373. As for the individuals, the General Directorate of Operations shall track and identify them in co-ordination with the General Directorate of Technical Affairs, review their criminal records and take any necessary and appropriate action.

Effectiveness, proportionality and dissuasiveness of sanctions

251. Until November 2017, sanctions for TF were inferred from Sharia or from the AML Law as the old CFT Law did not specifically provide for those sanctions. The Specialised Criminal Court has applied a wide range of sanctions against those that violate TF laws. The court has demonstrated that it can apply effective, proportionate and dissuasive sanctions against those that violate TF laws.

252. The duration of terrorism financing cases, from the arrest to verdict, is on average one to three years. The investigative authority can extend the detention up to one year. In cases which exceed one year from the date of the arrest before the case is brought to court, the detention must be extended by the Specialized Criminal Court. When a prison sentence is about to expire, selected convicts are sent to a rehabilitation centre which provides support and aims to reintegrate them in the society.

253. Violations of the Law of Combatting the Financing of Terrorism carry severe sentences in Saudi Arabia and the specialised court.

254. The updated CFT Law introduced specific sanctions for providing or collecting funds and other assets to terrorist organisations or individual terrorists; however, this new law has only been in force since November 2017 and it is not possible to evaluate its effectiveness.

255. There are circumstances in which the Special Court has reduced or suspended the sentence when it was convinced that the convicted person would not repeat the sentence or in case. In case of collaboration, there were examples where the prosecution was not brought forward (with the information being referred to Mabaheth). The updated CFT Law identifies more precisely those circumstances. Repeat offenders, however, were and are prevented from receiving reduced sentences.

256. The CFT legislation has allowances for authorities to keep the accused away from contacts with any external person, including a lawyer, for up to 90 days at the

decision of the investigative authority in the interest of the investigation,[9] and even longer periods at the decision of the Special Court. The Saudi authorities indicated that in practice once an accused is arrested, they are entitled to contact their family to inform them of their arrest. With regard to a lawyer, the law stated that the accused shall be entitled to use a lawyer to defend him before the case is brought to court in sufficient time decided by the investigation. Under the new CFT Law issued in November 2017, the Saudi authorities indicate that the right of recourse to a lawyer can be exercised from the date of arrest, but that this right can be restricted if the interest of the investigation requires it (CFT Law, art.21).[10]

257. Saudi authorities indicated that as a principle the Court's hearings are public and that in rare cases trials are heard in private at the discretion of the judges. The judgments themselves are not made public; however the Ministry of Justice publishes information concerning the name of the convicted person, the terrorist organisation they belong to, and the sanctions. This information about a sentence is not always made public.

258. It is clear that Saudi Arabia prosecutes and convicts a large number of persons for terrorist financing, which is consistent with the high-risk of terrorism and terrorist financing in the country. The cases provided by Saudi Arabia indicate that sanctions applied by the SCC for terrorist financing are proportionate and dissuasive. A lack of consistency and comprehensiveness in the publishing of convictions however can have an adverse effect on dissuasiveness. This lack of clarity is somewhat aggravated by the fact that TF convictions are most often based on confessions/denunciations.

Alternative measures used where TF conviction is not possible (e.g. disruption)

259. Saudi Arabia has not been hindered by a lack of ability to secure convictions for TF offences and has demonstrated success in addressing the risk of TF in the country by using some of the special investigative and preventative tools available to them in Saudi law. Saudi officials have been particularly successful in reducing the risk of funding for FTFs (both when Mabaheth gets information about an individual attempting to travel and after they have left) by the use of provisional seizures of their bank account and close monitoring of their family's account (to prevent them from being the victims of ransom scams).

260. In cases where prosecution for TF offences are not practical, suspected persons have been added to a watch-list. A number of lists of persons suspect to be linked with terrorist groups are maintained by Mabaheth, which are used to monitor the person, monitor transactions and also impose financial restrictions (see Immediate Outcome 10 below).

---

9 Under the new CFT Law, the decision to keep the accused away from contacts up to 90 days is made by the prosecution authority (art.20).

10 For a thorough discussion on the respect of the rights of the accused, the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has conducted a review of the of current Saudi counterterrorism law and practices. The final report is accessible here: http://www.ohchr.org/Documents/Issues/Terrorism/SR/A.HRC.40.%20XX.Add.2SaudiArabiaMission.pdf

261. Saudi Arabian authorities also have imposed travel bans on individuals suspected of terrorism or TF offences and have repatriated migrant workers with possible links with terrorism. Travel bans have been particularly successful to preventing suspects believed to be motivated to leave the Kingdom to become foreign terrorist fighters. The travel ban also serves as part of the sentencing for convicted offenders. Saudi nationals convicted of offences against the CFT Law are banned from travelling outside the Kingdom for a period equal to their prison term, upon completion of the term, and non-citizens are repatriated from the Kingdom upon completion of their prison terms and banned from returning to the Kingdom.

Overall conclusions on IO.9

262. Saudi Arabian authorities have demonstrated that they have the training, experience and willingness to pursue TF investigations in conjunction with and alongside terrorism cases. They possess the tools necessary to successfully prosecute those that violate the CFT Law offences.

263. Saudi officials have pursued investigations and prosecuted offenders from the various types of TF activity including the provision, raising, transfer and use of funds. The cases they pursue and prosecute is consistent for the most part with their national TF risk profile and is consistent with and supportive of their national counter-terrorism strategy. The notable exception to this is the priority of cases of TF within the Kingdom for support of terrorist groups and activity outside of the country to the extent that would be consistent with the risk profile and the TF threat identified by them during the National Risk Assessment of TF exercise.

264. Saudi Arabia has demonstrated an ability to respond to the dynamic terrorism threat it faces in country through preventative terrorist financing measures and by pursuing TF cases alongside terrorism cases. They have demonstrated the use of social media monitoring as an effective tool to identifying, preventing and where appropriate prosecuting TF offences in particular in relation to FTFs.

265. **Saudi Arabia is rated as having a substantial level of effectiveness for IO.9.**

Immediate Outcome 10 (TF preventive measures and financial sanctions)

Implementation of targeted financial sanctions for TF without delay

266. The Permanent Committee for Counterterrorism (PCCT) has primary co-ordinating responsibility for implementing targeted financial sanctions. Saudi Arabia uses its domestic authorities, granted via Royal Decree No. (M/16) dated 24/2/1435H,[11] to implement UN sanctions under UNSCRs 1267/1988/1989/2253 and their successor resolutions and to apply sanctions at a domestic level pursuant to UNSCR 1373. Saudi Arabia issued the Law on Combating the Financing of Terrorism issued in November 2017, repealing Royal Decree No. (M/16) and updating the relevant provisions. The authority responsible to decide on a domestic designation resided within the Ministry of Interior (since November 2017, the State Security Presidency) and can be elevated to the Royal Court in particular cases. Identification

11 A new CFT Law passed in November 2017 superseded the previous law. Royal Decree No. (M/16)was superseded, see R.5, R.6 in TC Annex below.

of possible targets for sanctions is the responsibility of Mabaheth. The PCCT is responsible for considering foreign requests for designation under UNSCR 1373 and for proposing or co-sponsoring designation at the UN Security Council.

267. Saudi Arabia implements domestic targeted financial sanctions on all individuals and entities designated pursuant to the 1267/1989/2253, 1988 regime automatically and without delay. Saudi Arabian law does not require any transposition from the UN at the national level, and UN designations thereby have immediate legal effect within the country. In the event that an individual or entity is removed from the UNSCR 1267 list, Saudi Arabia may choose to continue to implement domestic prohibitions when it disagrees with the de-listing decision. This has occurred in 2 occasions.

268. There are 12 Saudi nationals listed under 1267 and its successor resolutions. Saudi Arabia has co-sponsored several proposed listings at the United Nations at the request of other countries, but has never undertaken a proposal unilaterally. The lack of unilateral proposals to the UN Committees is not commensurate with the risk profile of the country, as identified by Saudi Arabia in its NRA, and as shown in the thousands of convictions for TF in relation to Al-Qaeda, ISIS and affiliated groups (see Immediate Outcome 9 above), and in the significant number of Al-Qaeda affiliated individuals listed under UNSCR 1373 (see below). Saudi authorities have a clear preference to prosecute terrorist financiers operating in the Kingdom, and also prefer to place individuals on a watch-list that triggers financial restrictions if they have left the Kingdom (usually as FTFs) given the large and constantly evolving number. A total of 14 current accounts, one credit card, 2 memberships of remittance centres, 1 investment portfolio and 1 company are frozen in Saudi Arabia pursuant to UNSCRs 1267/1989/2253. The total value of frozen assets is SAR 510 463 (approximately EUR 110 000), which were frozen immediately upon listing at the UN 1267 Committee.

269. Domestically, Saudi Arabia designated 150 individuals on its own motion pursuant to UNSCR 1373 between 2002 and 2016 (18 names between 2015 and 2016). There are other individuals and entities designated in 2017 that were not provided to the assessment team, including 11 individuals and two entities linked to ISIS and AQAP in Yemen.[12] Saudi Arabia also designated 68 individuals and 21 entities in co-ordination with the United Arab Emirates, Bahrain, and Qatar in 2017.[13] For those designated through 2016, the Saudi authorities have frozen 230 bank accounts for a total value of SAR 374 798.12 (approximately EUR 81 500). On the basis of seven requests by foreign jurisdictions, Saudi Arabia has also designated 29 individuals and 12 entities, frozen 3 current accounts and 1 membership of remittance centre, for a total value of SAR 3 273,50 (approximately EUR 700). All accounts frozen under 1373 measures were frozen immediately in co-ordination with the relevant financial institution. Saudi Arabia has not requested foreign countries to designate individuals under UNSCR 1373, which should be expected given the high number of domestic designations.

12 https://www.treasury.gov/press-center/press-releases/Pages/sm0187.aspx.

13 https://www.saudiembassy.net/statements/joint-statement-saudi-arabia-uae-bahrain-and-egypt-relating-new-terror-designations; https://www.thenational.ae/world/saudi-arabia-uae-and-egypt-issue-qatar-linked-terrorism-list-1.51035.

Table 22. Number of persons designated domestically under UNSCR 1373 mechanism by year

Year	2002-2010	2011	2012	2013	2014	2015	2016	2017
No. of designated persons (domestic)	84	41	7	-	-	16	2	-
No. of designated persons (foreign request)	-	-	-	-	-	16	24	1

Source: PCCT, Mabaheth

Table 23. Number of persons designated domestically under UNSCR 1373 mechanism by affiliation

Terrorist Group	Al-Qaeda	Hezbollah	ISIS	Lashkar-e-Taiba, al-Qaeda, the Taliban
No. of designated persons (domestic)	126	6	18	-
No. of designated persons (foreign request)	7 (6 of which from Al Qaeda in Yemen and Al-Nusra Front)	28	-	6

Source: PCCT, Mabaheth

270. The PCCT communicates to the designated person his/her rights and how to submit a de-listing request or exceptions. Saudi Arabia's UNSCR Implementing Mechanisms include detailed guidelines for submitting requests but this guidance is not publicly available. The PCCT has supported de-listing requests and exemptions requests for access to funds, including five exemptions since 2009 for designated individuals to travel to Saudi Arabia to conduct Hajj and Umrah. In these instances, the PCCT requires exact dates, travel details, and Mabaheth monitors the individuals while in Saudi Arabia.

Box 19. Joint Designation of Six Individuals and Entities for Providing Support for Lashkar-e—Tayyiba, al-Qaida, and the Taliban

In March 2016, the PCCT received a request from the United States to sanction four individuals and two entities for providing support to Lashkar-e-Tayyiba, al-Qaida, and the Taliban in line with UNSCR 1373. Of the six targets, Saudi Arabian authorities required additional information to sanction one individual, Saudi-based Muhammad Ijaz Safarash. The PCCT co-ordinated with SAFIU, and Mabaheth, to obtain additional information in support of their designation. Upon conclusion of their investigation, the PCCT jointly designated all the six individuals and entities with the United States and issued a public statement announcing the action on 31 March 2016. Saudi Arabia designated these individuals and the entities under its

Law of Terrorism Crimes and Financing and the Royal Decree A/44, and as a result of this action, any property or interest in property of these individuals under Saudi jurisdiction was frozen and Saudi citizens were prohibited from doing business with them.

Safarash had a small amount of funds that were frozen in his Saudi Arabian bank accounts, which totalled SAR 3 000 (approximately EUR 650). At the time of the on-site, the PP had a criminal case ongoing against Safarash.

271. Saudi Arabian authorities respond to requests from third countries regarding sanctions. When bilateral requests are received from foreign countries, Saudi Arabian authorities have the ability to pursue their own internal investigation to determine if the information meets the reasonable grounds threshold for designation, to freeze assets of, and the provision of funds and financial services to, designated individuals. In 41 of the 191 domestic designations, the designations were triggered by a foreign country request. The PCCT response time to third party requests varies between a matter of days and six months, depending on the level of political sensitivity of the issue and how long it would take for the Royal Court to make a final decision to implement a designation. In cases that are particularly politically sensitive, the Royal Court, which has the authority of the King of Saudi Arabia, must decide whether to implement a designation.

272. The Ministry of Interior (currently the State Security Presidency) communicates directly to the relevant authorities the designation decisions. The authorities then communicate with the relevant institutions to implement the freezes immediately. However, there is no consolidated or publicly available list of Saudi designated individuals or entities. Relevant supervisors have primary responsibility for ensuring compliance with sanctions obligations amongst FIs and DNFBPs. SAMA reports that they issue circulars to all FIs upon updates to the UNSCR lists and following a domestic designation. The timing of the issuance of the circulars could not be confirmed. FIs and DNFBPs are responsible for checking UNSCR lists on a daily basis and most have automatic screening systems in place. DNFBPs were broadly aware of UNSCR lists. Domestically designated persons are also included in the Shomoos system, maintained by Ministry of Interior. However, other than SAMA, Saudi Arabia did not demonstrate that supervisors have communicated the designations to their reporting entities immediately.

273. SAMA and CMA inspectors have specific inspection procedures to check FIs for sanctions screening during their onsite visits and can impose fines and sanctions. Inspectors examine whether the FI uses current UNSCR lists and if they have filed the appropriate reports in the cases of violations. There were two instances where CMA and SAMA both identified insufficient controls in place, and in one case a fine of SAR 40 000 was levied. SAMA and CMA issue guidance to banks and APs, who check the 1267 list on a daily basis and freeze accounts in response to sanctions listings. Financial institutions are required to provide information to SAMA and CMA on any and all assets that are frozen following a designation listing. In the case of attempted transactions, the financial institution is responsible for sending an STR to the FIU. This is inconsistent with the obligation to report freezes to the supervisors, who have primary responsibility to ensure implementation of TFS, nonetheless, the FIU is part of the PCCT and could raise any attempted transaction there.

274. DNFBP supervisors have only started focusing on TFS obligations as of mid-2016. The DNFBP sector is informed of potential terrorist financing risks to their sector and has an inconsistent understanding of its requirements or implementing UNSCRs obligations. Larger DNFBPs, to include lawyers, were better informed and reported checking UNSCR lists to verify they were not conducting business with designated terrorists. They also have access to the Shomoos system which includes domestically designated individuals. Smaller entities tend to rely on familial relationships to establish their client bases and rely on informal KYC mechanisms. As a result FIs and some DNFPBs (including lawyers) have awareness and implement TFS, while implementation amongst smaller DNFBPs is subject to further improvement to ensure that TFS are implemented effectively and without delay.

275. FIs and DNFBPs identify the beneficial owner as part of the CDD process, while updating this information has been a challenge for Saudi Arabia (see Immediate Outcome 4). No guidance has been issued in relation to the percentage of ownership in a company that would trigger freezing measures for the whole company and its bank account. Nonetheless, where it was identified that a designated person has ownership rights in a company, the PCCT would consider the bona-fide rights of third parties and the proportionality of the freezing measures. In practice, where such a situation occurred under both the 1267 and the 1373 regimes, the PCCT has frozen the membership of the listed individual in the company. If the company itself were to be designated or the designated person was the majority shareholder of or controlling a company, the PCCT would freeze the whole company and its bank account.

Targeted approach, outreach and oversight of at-risk non-profit organisations

276. Due to a very narrow interpretation of an NPO as defined by Recommendation 8, Saudi Arabia's NPO sector is relatively small in number. The NPO sector in Saudi Arabia covers religious Associations and Foundations. As of July 2017, 1 424 Foundations were in existence but the number is now growing at a rate of approximately 17% per year.

277. Civil society organisations, often considered part of any county's broader NPO sector, do not exist in Saudi Arabia.

278. In the past, Saudi NPOs have been heavily exposed to the risk of misuse for terrorist financing. Since 2001 Saudi Arabia has made a series of major changes to ensure its NPO sector is not hindered by being vulnerable to TF. On March 17th 2016 a new Law on Associations and Foundations came into effect in Saudi Arabia.

279. The new law brings all Foundations and Associations under the supervision of the Ministry of Labour and Social Development (MLSD). There are still however a few organisations still being migrated to the new supervisor from the Ministry of Islamic Affairs. The following table shows the breakdown of the different types of Associations and Foundations in Saudi Arabia:

Table 24. Types of Associations and Foundations in Saudi Arabia.

Type of Organisation	Supervisor	Number	Percentage
Associations Providing Income Support and Maintenance	MLSD	536	37%
Associations Providing Social Services	MLSD	238	17%

Type of Organisation	Supervisor	Number	Percentage
Associations Providing Health Services	MLSD	60	4%
Associations Providing Housing Services	MLSD	10	1%
Co-operative Offices for Call and Guidance	Islamic Affairs	412	29%
Associations for Quran Memorization	Islamic Affairs	168	12%
Totals		**1424**	**100%**

Source: MLSD.

280. Foundations can be further divided into two main types of services: Foundations, which provide cash or in-kind assistance and Foundations which provide programs and activities that satisfy the Foundation's objective but do not provide cash or in-kind assistance. Total assets of Foundations supervised by the MLSD amounts to approximately SAR 13 808 633 984 (approximately USD 3.5 billion) with an annual income of SAR 5 940 890 052 (approximately USD 1.5 billion) in 2016. Associations supervised by the Ministry of Islamic Affairs have assets totalling SAR 4 998 705 813 (approximately USD 1.3 billion) with income of SAR 1 640 407 107 (approximately USD 400 million) in 2016.

281. Associations and Foundations in Saudi Arabia must be organisations involved in the eight categories of causes for the proper distribution of Zakat. In addition they must be for the benefit of local communities. As such, not only are they prevented from having programs abroad, an organisation registered for operations in Riyadh is not permitted to carry on services outside a defined geographical territory. Foundations are required to establish bank accounts for all their operations Accounts held by NPOs are all considered high-risk by banks and are tightly monitored. Any attempt to conduct an in-bound or out-bound cross-border transaction will be detected by the bank, blocked, and reported to the FIU.

282. Effectively Saudi Arabia's NPO sector operates in a cashless society, as they are prohibited from accepting or dispersing cash. All donations must be made through electronic means or in cash at the organisation headquarter. Organisations involved in direct financial support for the needy do so with the use of monitored money value cards and monitored joint bank accounts. Fundraising campaigns must be previously approved by MLSD.

283. Strict regulatory requirements are placed on all NPOs including the obligation to report suspicious transactions to the Department of Financial Intelligence. This is done to ensure financial integrity and thereby building public confidence in the sector. Each organization currently receives 4 audit visits every year with a year-end report from the 500 inspectors employed throughout Saudi Arabia. Beginning in 2017, MLSD began developing a risk-based tool by analysing information from these visits to determine those organisations that are most at risk. The indicators developed are primarily focused around financial integrity. A total of 2.4% of the organisations were identified as high risk and were therefore subject to both desk audits and an additional 4 compliance visits per year. During the recent TF Risk Assessment process, NPOs were determined to be low risk due in large part to the restrictive measures put in place since 2005, with no TF cases or STRs involving NPOs.

284. These measures, taken to more tightly regulate the activities of Foundations as well as the awareness campaigns and supervision mechanisms were put in place, at least in part, to mitigate the risk of terrorist financing. This has significantly mitigated the risk of misuse of these entities for terrorist financing. While considered low risk as a result of the TF Risk Assessment process, this is a residual risk determination based in part on the heavy regulations imposed on the sector. For the financial sector NPOs are considered high risk customers with their accounts being heavily monitored and operating under certain restrictions such as a prohibition on national funds transfers.

285. Saudi Arabia has supplemented the restrictive regulatory regime with a comprehensive training program for NPOs focused on financial crimes including money laundering, TF, corruption and fraud. MLSD has delivered 36 training sessions covering financial crimes for NPO's over the last 2 years. In addition, MLSD has implemented 8 awareness sessions on a NPO Governance Project, which was attended by about 1 400 members of the boards of directors of NPOs and ministry employees in various regions of the Kingdom during the first half of 2017.

286. MLSD has also begun planning for 60 training sessions covering AML/CFT for relevant individuals at NPOs as well as for MLSD staff. Twenty to thirty trainers will be qualified to complete awareness-raising sessions on behalf of MLSD on the risks of money laundering and TF. The 60 courses will be delivered in different areas of the Kingdom with a planned audience of 1 800.

287. In addition to raising awareness within MLSD and NPOs, Saudi Arabia has developed awareness campaigns for the public to educate them on the laws and safe giving. Some information pertaining to NPOs is publicly available, from Saudi Arabia only, through a new online portal at MLSD's homepage opened in 2017.[14] The portal provides information related to individual NPOs and allows for the searching of information by name, region, size, income, expenditure, liabilities, assets, number of employees, number of volunteers, board members, services provided, and goals.

288. Although the organizations under the Ministry of Islamic Affairs provide programs and activities that do not provide cash or in-kind assistance, a training program was set up to educate the workers in the sector (Money Laundering and Terrorist Financing Program), in co-operation with the SAFIU. Saudi Arabia conducted 14 training sessions for 373 trainees from Quranic memorization and advocacy offices over the past three years.

289. Some waqfs can conduct activities which would fall within the FATF definition of NPO. Waqfs must be registered with a judge or the Ministry of Religious Affairs. While there is no specific awareness raising or supervision targeting the misuse of waqfs for terrorist financing, there is a range of measures to prevent the misuse of waqfs for terrorist financing, including registration with public authorities, supervision by a judge that the activities are in accordance with the purpose of the deed, and direct administration by the Ministry of Religious Affairs in the case of public-purpose waqfs (see Immediate Outcome 5 below). Waqfs cannot receive donations unless they receive prior authorisation by the supervising judge. There is no prohibition that the assets generated by the waqf stay in Saudi Arabia.

14 https://makeen.mlsd.gov.sa.

Box 20. Muslim World League (MWL) and the World Assembly of Muslim Youth (WAMY)

International donations coming from Saudi Arabia can be made through the official aid agency of Saudi Arabia (the King Salman Humanitarian Aid & Relief Centre) as well as two organisations: the Muslim World League (MWL) and the World Assembly of Muslim Youth (WAMY). These two bodies, formed in 1962 and 1972 respectively, are considered by Saudi Arabia as international organisations under specific agreements signed with the Government of Saudi Arabia, although they consider themselves as non-governmental organisations. They have a large network of branches abroad and their main purpose is the teaching of Islam, which is fulfilled, among others, by publishing books and contributing to building mosques, schools, and cultural centres. They are under a different regulation and supervision regime than Foundations and Associations. Under the applicable regimes, MWL and WAMY need an authorisation from the Minister of Foreign Affairs to open branches in a foreign country and to transfer money abroad. Charitable organizations arising from MWL and WAMY are prohibited from raising charitable donations within the Kingdom.

Saudi Arabia signed two Headquarters Agreements and a protocol with MWL and its related bodies including the Islamic Relief Organisation in 2009, and with WAMY in 2010. These agreements regulate the administrative and financial relationship, responsibilities, appointment mechanism in the organisation and mechanism of money remittances.

In order to ensure compliance with the Agreement and the protocol, in 2016, on-site inspections were carried out on the offices of MWL and its related bodies and institutions, including the Islamic Relief Organization and the offices of the WAMY. Based on the inspection tours, several offices were closed with several administrative and financial violations, not for financing terrorism, but to ensure that financial and administrative imbalance is not exploited.

Deprivation of TF assets and instrumentalities

290. Saudi Arabian authorities use TFS, as well as other measures such as criminal procedures and a preventive watch-list mechanism, to deprive terrorists and terrorist financiers of their assets and instrumentalities. Individuals and entities designated in response to partner requests pursuant to UNSCR 1373 do not typically hold funds within the Kingdom (total sum of freezes is SAR 3 273.50), and Saudi Arabian preventive measures focus heavily on responding to self-financing crimes that support foreign terrorist fighters. In contrast, the names that Mabahith listed domestically pursuant to 1373 have frozen funds in the total amount of SAR 374 798.12.

291. Saudi Arabian authorities reported over 1 000 convictions related to terrorist financing incidents from 2013-2016 and a total of approximately SAR 2.3 million (approximately EUR 500 000) involving different currencies were confiscated in the

context of criminal convictions for terrorism or terrorist financing cases. Instrumentalities, for example personal computers and tablets, are also confiscated.

Table 25. Assets confiscated following TF convictions by year and currency.

Currency	2013	2014	2015	2016	Total
SAR	163 500	203 997	89 117	486 675	943 289
EUR	78 445			203 200	281 645
USD			13 262	8 080	21 342
Iraqi Dinar	1 ML				1 ML
Turkish Lira			15		15
UAE Dirham				1 000	1 000

Source: Special Criminal Court

292. In addition and as an alternative to formal TFS, Saudi Arabia places individuals suspected of terrorist financing, to include FTFs, on a private watch–list, based on the CFT legislation. Provisional seizures on a person suspected of committing a terrorism-related crime were carried out at the decision of the investigating authority on the basis of article 18 of the LTCF.[15] The persons on the suspicion list are subject to a number of financial restrictions depending on the case, including freezes of accounts and prohibition of certain transactions. This list is used to a much greater extent than Saudi Arabia's 1373 list and is in response to their significant foreign terrorist fighter issue. The watch-list is circulated to all supervisory authorities, customs and border agents, as well as to FIs. Saudi Arabia did not provide statistics on the number of individuals on the watch-list or on the assets seized, but it is likely that it includes all FTFs and that it totals more than 3 000 people. The individuals placed on this list are not notified when placed on the list and cannot apply for de-listing and exemptions.

Consistency of measures with overall TF risk profile

293. CFT issues are considered a high priority within Saudi Arabia and authorities have a very good understanding of their TF risks. Saudi Arabia's National Risk Assessment on Terrorist Financing identified donations from private individuals and support for foreign terrorist fighters as the two major sources of terrorist financing. The PCCT advised that TFS did not typically seize a significant amount of fund and assets of FTF are largely seized by TF related investigations and prosecutions. The largest number of freezes occurs through the preventive watch-list which entails financial restrictions, but which also does not provide for legal procedures for de-listing, unfreezing, providing access to frozen funds, exemptions, and the protection of *bona fide* third parties.

294. The PCCT prefers to let Mabaheth and PP pursue prosecutions and apply financial restrictions instead of designations for terrorist financiers for a number of reasons. Given the high number of terrorist financing incidents in Saudi Arabia, the PCCT believes that designating all terrorist financiers and foreign terrorist fighters will lessen the impact of a designation. Saudi Arabian authorities reported over 1 000

15 Since November 2017, the freezing measures are based on article 9 of the CFT Law at the order of the Public Prosecution.

convictions related to terrorist financing incidents from 2013-2016 and the PCCT preferred to proceed cautiously with any public actions given the possible scale. The PCCT also cited a cumbersome and bureaucratic process for pursuing 1373 designations as opposed to judicial proceedings, leading to a tendency to prefer applying preventive measures through criminal investigations and prosecutions. Saudi Arabia cites the 2017 government reorganization and establishment of the State security Presidency as a possible avenue for streamlining their designation processes in order to make it less cumbersome. Further, the PCCT consists of a 5 person Secretariat and is responsible for many competing mandates, which limits its ability to respond to all requests in a timely fashion and capitalize on the potential of TFS to the greatest extent.

295. Saudi Arabian authorities noted they prioritise designation requests according to whether individuals have assets within Saudi Arabia, are Saudi citizens, and in response to third party requests. Saudi authorities do not pursue designations based on self-generated investigations.

296. Saudi Arabia could more proactively pursue nominations to the 1267 list given the significant threat of UN-designated groups that they identified and the presence of individuals affiliated to those groups on the Saudi 1373 list. Individuals and entities designated pursuant to UNSCR 1373 do not typically hold funds within the Kingdom, and Saudi Arabian preventive measures focus heavily on responding to self-financing crimes that support foreign terrorist fighters.

297. The absence of nominations to the UN as well as the lack of request for designation to foreign countries are not consistent with the risk profile of Saudi Arabia and may reflect a lack of strategy in disrupting the financing of terrorist groups through these tools. The timing and number of Saudi Arabia's 1373 designations also lends to questions over whether they are driven by TF risk or by other objectives. While the use of financial restrictions based on preventive watch-list lists may be at times an effective use to counter the financing of terrorism, there are uncertainties on whether these are proper tools, particularly because they may not always allow all interested parties to know about the restriction, in particular foreign countries where a potential designee holds bank accounts and other assets, not provide for legal procedures for de-listing, unfreezing, providing access to frozen funds, exemptions, and the protection of *bona fide* third parties.

Overall conclusions on IO.10

298. Saudi Arabia considers combatting terrorist financing a key priority and generally has strong implementation of UN terrorism-related TFS. Saudi Arabia has not independently nominated targets at the UN and initiated third party requests for 1373 designations abroad, which is not fully consistent with the risk-profile of the country. Saudi Arabia has co-sponsored designations at the UN Committees and has domestically designated more than 150 persons in Saudi Arabia. Saudi Arabia's 1373 designations are not public which hinders effective implementation. The largest number of freezes comes from financial restrictions imposed on a person through criminal procedures and watch-list mechanisms, which however do not provide for legal processes equivalent to the targeted financial sanctions and the FATF standards. Supervisory authorities communicate with FIs regarding their risks associated with TF. The measures taken by Saudi Arabia effectively mitigated the risk of NPOs being

misused for TF, although Saudi Arabia has recently introduced a risk-based approach to monitoring the activities of its NPO sector, based primarily on financial integrity.

299. **Saudi Arabia is rated as having a Substantial level of effectiveness for IO.10.**

Immediate Outcome 11 (PF financial sanctions)

300. Saudi Arabia prohibited all direct economic and financial relationships with Iran. There are also very little economic, financial, and demographic connections with North Korea. These restrictions have partially mitigated Saudi Arabia's proliferation financing risks. However, Saudi Arabia still faces the proliferation financing risks relevant to all major economies, including diversion and concealment of the true identity of the parties to a transaction, as well as those relevant threats given its geographic proximity to Iran and trade relations with nearby countries who trade with Iran and may deal in dual-use goods. Iranian pilgrims travelling to Saudi Arabia for the Hajj and Umrah are required to make tightly controlled ad-hoc banking arrangements to support their travel.

301. Saudi Arabia issued revised regulations in November 2017 during the on-site visit, making it impossible to assess the implementation of the new legislation. Accordingly this chapter will assess the effectiveness of the targeted financial sanctions regime under the general system previously in place. The absence of any cases or examples of PF TFS implementation also presents an assessment challenge.

Implementation of targeted financial sanctions related to proliferation financing without delay

302. Royal Order No. 7753/MB Dated 29/10/1427 H (2006) established the Chapter VII Committee, within the Ministry of Foreign Affairs, with the responsibility to review every resolution issued by the Security Council issued according to chapter seven of the United Nations' Charter, which includes overseeing the implementation of UNSCRs in relation to proliferation financing. To be in line with the requirements of PF related UN resolutions, revised implementing regulations were issued in November 2017. The new regulations have limited the scope of the Chapter VII Committee to proliferation of weapons of mass destruction.

303. The Chapter VII Committee meets monthly to review Security Council Resolutions issued under Chapter Seven of the UN and brings together most responsible agencies for implementing targeted financial sanctions related to PF.[16] The agencies include internal and external security personnel from Ministry of Interior, Ministry of Defence and Mabaheth, border control agencies (General Port Authority and Customs), a financial supervisor (SAMA) as well as Ministry of Justice, Ministry of Education, Ministry of Transport, and Ministry of Finance. The Committee is chaired by the Ministry of Foreign Affairs (MOFA).

304. The Saudi Arabian Financial Intelligence Unit (SAFIU) is a member of the Chapter VII Committee indirectly (as a part of the Ministry of Interior and more

16 It is noted that the implementing regulations identified the Chapter VII Committee as responsible for proposing designation to the UN Sanctions Committee, although no name has been proposed as yet.

recently the State Security Presidency) but is not a member on its own rights and takes part only on an ad-hoc basis SAFIU did not demonstrate that it was familiar with obligations in relation to TFS in proliferation financing. SAFIU analysts lack a clear understanding of the characteristics that would indicate a proliferation financing threat and SAFIU had not conducted any analysis related to potential violations of PF-related sanctions and related follow-up on possible proliferation financing at the time of the onsite.

305. Up to November 2017, sanctions for PF were implemented via a system of communications between relevant agencies.[17] The President of the Committee (MOFA) disseminated UNSCRs to Chapter VII Committee members. Royal Order No. 7753/MB did not specify how and how fast the dissemination should take place, and it is unclear how long it took for MOFA to disseminate the updated lists to Committee members.

306. Upon receipt of such an update and instruction from the MOFA, the Committee members who are supervisory authorities are required to send a circular to all FIs and DNFBPs, requesting that they check their client, transaction and beneficial ownership databases against the list and report back to them on the outcome of the screening within two weeks. In practice, only SAMA had developed a system to circulate these lists to individual FIs before the November 2017 law. In one instance, SAMA provided an example of a circular that was distributed to FIs 3.5 months after the UNSCR was adopted at the UN. It is not clear how long it takes for the other supervisors to inform the reporting entities of the updated lists. SAMA's as well as the CMA's sectorial AML/CFT rules require FIs to screen client databases against all UN sanctions lists on a regular basis, and to take relevant measures in case of a match. No match has ever been found.

Identification of assets and funds held by designated individuals/entities and prohibitions

307. There are no examples of any account being frozen or any transactions or services being prohibited in Saudi Arabia as a result of TFS for PF. Saudi Arabia has a new institutional framework to support implementation of targeted financial sanctions relating to proliferation of weapons of mass destruction – introduced in November 2017 – but does not have any examples of when it has been used.

308. There are no instances of assets frozen or seized due to WMD-proliferation related UNSCRs. No funds of any Iranian or DPRK individuals or entities have been frozen by FIs in response to United Nations Security Council Resolutions possibly as a result of the pre-existing absence of financial activity from both constituencies. There are also no examples of interagency co-ordination or collaboration to identify and detect possible violations of sanctions implementation related to proliferation financing. In addition, there are some weaknesses in updating the beneficial ownership information of legal entities and arrangements (see Immediate Outcome 4).

17 Since November 2017, the new regulations require that implementation of sanctions for PF be done automatically and without delay upon publication of UNSC Resolution (see R.7).

309. Customs and border officials are responsible for inspections at ports of entry, and some second-line borders officials have limited financial investigation training. The Saudi Arabian Customs Authority has participated in some training, including a workshop in 2013 on the Proliferation of Weapons of Mass Destruction. The Chapter VII committee has conducted ten investigations into vessels transiting Saudi Arabian waters, and customs officials with the Ministry of Commerce and Industry have participated in interdictions of dual-use goods at Saudi Arabian borders. The Saudi authorities intercepted and seized five ships in the last 2 years; however, there was no further financial investigation following the interdiction.

310. Iranian pilgrims may receive sanctions exemptions to travel to Saudi Arabia for the Hajj and Umrah. Iranian pilgrims are generally prohibited from traveling with cash and are directed to deposit funds into a specified account in Saudi Arabia, overseen by SAMA, before their arrival. For individuals unable to complete bank transfers, Saudi authorities will meet the pilgrims upon arrival in Jeddah or Medina, collect their cash, and immediately deposit it into a bank. Cash flow into Saudi Arabia during Hajj and Umrah dropped by more than 99% after this system was implemented. In 2016 there were around 60 000 Iranian pilgrims and in 2017 86 000. Mabaheth also monitors the pilgrims in country for the duration of their stay.

FIs and DNFBPs' understanding of and compliance with obligations

311. Financial institutions and DNFBPs have a weak understanding of TFS system in relation to PF. This is likely due in part to the lack of ties with Iran. The private sector is not educated and aware of the existing typologies related to PF, and in particular has little awareness of the risk of sanctions evasion or the relevance of establishing the beneficial ownership of parties to transactions. No guidance and training has been provided to the private sector regarding implementing TFS related to PF.

312. FIs and some larger DNFBPs have automated systems (World Check) to check for updates to UN lists, including WMD-proliferation related UNSCRs. In the event of any positive identification of an individual or entity on an UNSCR list, banks would freeze the account/transaction even before receiving instructions from SAMA. However, no individual or entity on the Security Council's list has ever been identified to hold assets in Saudi Arabia by the systems currently in place.

313. FIs reported undertaking enhanced due diligence processes for clients who engage in trade with Turkey, the United Arab Emirates, or other higher-risk jurisdictions as mentioned in Saudi Arabia's National Risk Assessment but do not have an understanding of the types of activities associated with proliferation financing.

Competent authorities ensuring and monitoring compliance

314. SAMA is responsible for ensuring that targeted financial sanctions defined in the UNSCRs related to PF are implemented without delay by banks and conducts periodic site visits to FIs. SAMA inspectors check FIs systems for sanctions screening during their on-site visits and can impose sanctions and fines. All supervisors are instructed to assess, as part of the onsite visit, the effectiveness of the supervised institution's controls to identify any business from persons listed by the UN, and to determine whether and how many such cases have been identified by the institution and whether they filed reports with the appropriate authorities.

315. Both SAMA and the CMA provided case studies that confirm that FIs systems for targeted financial sanctions are tested as part of onsite visits, but these are related to TF sanctions under UNSCR 1988 and 1989 lists, and not TFS related to PF. No violations related to PF have been found by supervisors.

316. SAMA has automated systems in place to check for any updates to the UNSCR lists, and to communicate any updates without delay to the private sector for implementation. Authorities performed a routine check to confirm that the system was operational. However, in practice, SAMA has disseminated circulars informing private sector entities about designations only after a considerable delay of at least 3.5 months.

317. Up until November 2017, written guidelines had not been provided to FIs or reporting entities. The Chapter VII committee had recently begun to enhance its outreach regarding PF vulnerabilities and requirements. The Ministry of Commerce and Industry oversees 28 chambers of commerce, which provide a venue for outreach to the private sector, but it is only utilized in the event that a sanctioned individual or entity appears in the MOCI database. As no match for PF has been found yet, the system was never used.

Overall conclusions on IO.11

318. Saudi Arabia has an interagency framework and co-ordination mechanism that oversees the implementation of targeted financial sanctions related to proliferation financing. This technical system was enhanced with the issuance of new Implementing Regulations in November 2017. Under the system up until November 2017, implementation without delay of TFS for PF was not demonstrated. There are no instances of assets frozen or seized and no examples of inter-agency co-ordination related to proliferation financing.

319. While Saudi Arabia has taken significant steps to limit its exposure to Iran and DPRK financial activity by cutting economic, financial and trade relations, the mechanisms in place to prevent sanctions evasion are weak. This remains a vulnerability especially given the regional proximity to Iran and regional trade of petrochemicals and dual use products. FIs and some DNFBPs are generally familiar with their obligations to implement TFS from a technical standpoint, but have a weak or non-existent understanding of TFS system in relation to PF. They also do not have a greater level of awareness regarding PF typologies, sanctions evasion risk or how to protect themselves from this type of activity.

320. **Saudi Arabia is rated as having a low level of effectiveness for IO.11.**

4

CHAPTER 5: PREVENTIVE MEASURES

Key Findings and Recommended Actions

Key Findings

- Major FIs in Saudi Arabia have a good understanding of the ML/TF risks they face, thanks to the supervision and outreach efforts made by the authorities, as well as the risk assessments conducted at the institutional level. Large-scale DPMSs also have a good understanding of their risks. The measures taken by Saudi Arabia in relation to NPOs have drastically reduced the risk of TF in the sector; however, NPOs continue to be treated as high risk by FIs and DNFBPs.
- Money exchangers and other DNFBPs do not fully understand their ML/TF risks or apply mitigating measures under a Risk-Based Approach.
- The awareness and implementation of AML/CFT obligations among reporting institutions has increased significantly thanks to vigorous supervisory measures taken by the competent authorities in the last two years.
- Money exchangers and many DNFBPs (in particular real estate agents and accountants) do not yet have a comprehensive and an in-depth understanding of their AML/CFT obligations, especially the reporting of STRs.
- Major FIs and large-scale DPMSs apply to a certain degree the AML/CFT preventive measures including CDD, record keeping and identification of beneficial ownership. However, STRs are not submitted in a timely way, and the low number of terrorist financing-related STRs, especially by the sectors identified as high-risk in the TF NRA, is a major concern.
- The new AMLL and CTFL adopted in November 2017 further strengthened the legal basis for AML/CFT preventive measures in Saudi Arabia; these Laws were however introduced too soon before the on-site visit to assess their level of effectiveness and implementation within FIs and DNFBPs.

Recommended Actions

- Saudi authorities should provide more information and guidance on TF risks and typologies to raise awareness among FIs and DNFBPs, especially the high-risk sectors, and enable them to better identify suspected TF activities.

- Saudi Arabia needs to increase the awareness, the understanding of AML/CFT obligations and the implementation of risk-based approach among money exchangers (class A and B) and most DNFBPs.
- Supervisors should take more vigorous measures, including supervisory actions, education and outreach, to urge non-bank FIs and DNFBPs to strengthen their transaction monitoring systems and ensure timely reporting of STRs by all reporting entities (accompanied by improvements in the FIU's systems).
- Saudi Arabia should provide guidance to FIs and DNFBPs that NPOs are low risk for TF due to the measures in place.

321. The relevant Immediate Outcome considered and assessed in this chapter is IO.4. The Recommendations relevant for the assessment of effectiveness under this section are R.9-23.

Immediate Outcome 4 (Preventive Measures)

322. Saudi Arabia has diverse financial and DNFBP sectors. The banking sector plays a predominant role in the financial sector. The exposure to ML/TF risks of FIs and DNFBPs varies significantly in Saudi Arabia. The ML & TF NRAs identified banks, class A money exchangers and dealers in precious metals and stones (DPMS) as high-risk sectors. Securities companies are identified as medium risk. Insurance companies (including saving and protection insurance), finance companies, class B money exchangers, lawyers, accountants, and real estate agents are identified as low risk. Tables 1.1 and 1.2 in Chapter 1 summarise the makeup of the financial and DNFBP sectors in Saudi Arabia.

Understanding of ML/TF risks and AML/CFT obligations

Financial Institutions

323. The risk-based approach was introduced into the financial sector in Saudi Arabia several years ago; the Implementing Regulations of the AML Law issued in 2012 set out a general requirement on risk management for FIs and DNFBPs, and SAMA required banks and money exchangers to: (i) periodically conduct ML/TF risk assessments based on detailed principles and factors (customer, geography, product and delivery channel) and (ii) to put in place adequate risk mitigating measures. Similarly, the risk-based approach was introduced in the securities sector in 2009 and enhanced afterwards. In 2015, a major update was introduced with more specific requirements and guidance. Financing and insurance companies, as well as class B money exchangers started to implement the risk-based approach in 2016.

324. Awareness among FIs about the results of the NRAs is well-established thanks to the outreach efforts and workshops made by the relevant authorities (SAMA and CMA). Financial institutions have in general a good understanding of the ML/TF risks identified by the NRAs. NRA results have been shared through workshops and meetings, but the results made available are mainly provided at a general level, without providing specific and detailed information on the patterns, typologies, and

methods used in major ML/TF activities within the Kingdom. This may limit the ability of FIs to identify suspicious ML/TF transactions.

325. The awareness of AML/CFT obligations is at a good level among most FIs, especially banks, financing companies and securities companies (APs).

326. Securities firms have a good level of awareness of the results of the NRAs and their relevant institutional risks. They apply the risk-based approach and have a good knowledge of risk mitigation measures. Supervisory actions taken by CMA in recent years have had a positive effect on the securities sector.

327. Financing companies are aware of the NRAs' outcomes and have adopted internal risk assessment mechanisms. These have allowed them to have a better understanding of ML/TF risks facing the sector. They participated in the NRA exercise and shared their knowledge on patterns and trends of ML/TF in their sector.

328. The insurance sector in Saudi Arabia is relatively new and represents about 2% of the financial sector. Life insurance is not common in Saudi Arabia for cultural reasons and represents only 3% of the whole insurance sector. Insurance companies know the results of the NRAs and have in place risk assessment mechanisms similar to other FIs under SAMA's supervision. Interviewed insurance companies are aware of their AML/CFT obligations to a certain degree.

329. The remittance sector in Saudi Arabia is composed of 12 remittance services providers, eight of which are associated with Saudi-licensed banks and the remaining four are class A money exchangers. As noted in the analysis of IO.1, since April 2011, Saudi authorities have implemented a remittance service framework, which includes ceasing to issue new Class A money exchange licenses. New remittance services providers can only be established in partnership with a Saudi-licensed bank. The four remaining Class A money exchangers continue to operate under grandfathered licenses issued prior to this policy change. Class A money exchangers can carry out domestic and cross-border money remittances businesses and are considered as high risk. When interviewed, they were aware of the results of the NRAs and have institutional risk assessment mechanisms in place - in part as a result of recent supervisory attention. However, the risk assessments carried out by class A money exchangers still need improvements as their understanding of ML/TF risks is mainly about those identified in the ML & TF NRAs, and they do not have a clear or independent understanding of risks they face at institutional level.

330. Money exchangers, both class A (remitters) and class B (currency changers), have an incomplete awareness of their AML/CFT obligations. This is a cause for concern since these are identified as high-risk sectors in the NRAs.

Box 21. Suspension of remittance license of three class A money exchange companies

Remitter #1

SAMA conducted an on-site inspection of a remitter in October 2016. The team found weaknesses in the control system, and the company's lack of

compliance with the instructions issued by SAMA regarding AML/CFT, as well as failure to follow the risk-based approach and the absence of a transaction monitoring system. In November 2016, a meeting was held with the representatives of the company to discuss the results of the inspection, where the company was requested to provide SAMA with the corrective action plan within 10 days.

In May 2017, the inspection team conducted the follow-up process, and it was found that the company still suffered from an inability to process findings as required. The company was requested to engage an independent and specialised consulting company approved by SAMA to ensure that the company implemented and finalised corrective actions. The consultant would then verify the remediation of all findings contained in the inspection report.

In September 2017, SAMA conducted an on-site inspection to follow-up on these issues. The team concluded that the company was not fully committed to correcting the observations in the form and with the speed required, and that this would negatively affect AML/CFT controls. Based on the inspection, it was decided to suspend the license for money transfer activity until all the observations have been corrected and approved by SAMA. On 25 September 2017, SAMA suspended the remittance license of the class A money exchanger, because of their failure to adequately address AML\CTF observations previously observed through on site supervision, in addition to the violation of the license issued by SAMA for remittances.

Remitter #2

SAMA inspected this money exchanger on 8-12 January 2017 and a number of deficiencies were identified, including a lack of compliance with regulatory requirements, weaknesses in technical systems, insufficient processes, shortcomings in many client files and processes, and weaknesses in the internal control system. A meeting was held with the representatives of the company at SAMA to discuss the results of the inspection.

On 29 January 2017, SAMA suspended the exchanger's remittance license, limiting the company and its branches to currency exchange only. The company was requested to provide SAMA with a corrective action plan within 10 days. In addition, the company had to assign an independent and specialised consulting company approved by SAMA to ensure that the company implemented and finalised the corrective actions and that would verify the remediation of all findings contained in the examination report.

Remitter #3

A third remitter was inspected from 19-23 March 2017. The inspection team found that the company had serious AML/CFT deficiencies, which required immediate intervention to ensure that no suspicious transactions could be executed. Based on the results of the inspection, it was decided to stop the money transfer activity until all the observations were corrected and

approved by SAMA, and on 18 April 2017, SAMA suspended the remittance license.

The company was requested to provide SAMA with a corrective action plan within 10 days. In addition, the company had to assign an independent and specialised consulting company approved by SAMA to ensure that the corrective actions were followed up and to verify the remediation of all observations contained in the examination report.

331. There are 69 class B money exchangers, which carry out currency exchanging business only and are considered as low risk. Class B money exchangers noted that they were recently informed about the results of the NRAs (one month before the on-site visit).

DNFBPs

332. Application of the risk-based approach among DNFBPs remains in its early stages and incomplete, largely because the requirement to follow a risk-based approach was introduced in mid-2016 by requirements set out by MOCI and MOJ. An exception to this are the large scale DPMSs, as noted below. In general, DNFBPs are aware of the results of NRAs due to numerous workshops carried out by competent authorities in early 2017.

333. Large DPMS (i.e. firms operating multiple shops dealing in jewellery, precious metals, and stones) appear to have a more in-depth understanding of the ML/TF risks identified in the ML and TF NRAs than other DNFBPs; they took them into consideration when assessing risks at the institutional level. They have adopted comprehensive risk assessments, identified high-risk areas (e.g. individual high-risk stores) and put in place measures commensurate with the risks.

334. Real estate agents have a relatively low level of understanding of ML/TF risks. The role of real estate agents is however limited to matching a seller's offer to a buyer's need. The real estate transaction is entirely carried out by public notaries in a specialised court under the Ministry of Justice. Public notaries follow a procedure that includes verification of (i) buyers and sellers' IDs as well as their background, (ii) the payment (exclusively by certified checks) and (iii) transfer of ownership. Transaction records are kept in the Ministry of Justice. Notaries do submit STRs on suspicious real estate transactions, as noted in the table below.

335. Large accounting firms interviewed demonstrated a reasonable understanding of the ML/TF risks and obligations. This was confirmed by MOCI and SOCPA as they focus their awareness raising and inspections work on the large/high-risk firms. One large accountancy firm stated that they have a risk assessment department and that an AML Officer is appointed in each branch of the company; AML/CFT policy based on the AML law is also circulated to all the company staff. They carry out a risk assessment at the start of a customer relationship and update it annually. Accountants in Saudi Arabia are mainly auditing firms and do not provide company formation services nor initiate transactions on behalf of their customers.

336. Lawyers interviewed showed an understanding of ML/ TF risks identified by NRAs and are aware of AML/CFT obligations, as part of efforts made by MOJ since 2016.

Application of risk mitigating measures

337. In general, risk mitigating measures are well established and implemented by major FIs and large-scale DPMSs.

338. Banks have conducted their own risk assessments which allow them to have a good knowledge of specific types of high-risk customers and products, and have developed relevant risk mitigating measures, including enhanced CDD and appropriate transaction monitoring. However, some banks do not update the customers' risk profiles based on ongoing monitoring or periodic reviews of account activity; this was confirmed by SAMA as one of the findings in their supervision.

339. When determining the risk category of the customer, some FIs rely on mandatory risk-classification requirements given by SAMA and/or applied in internal risk models, which require several classes of customer (e.g. PEPs, journalists, DPMS, real estate agents, and other classes of high-status individuals) to be treated as high-risk. In some banks these mandatory risk classifications mean that a large proportion of customers fall into the "high-risk" category. Similarly, NPOs continue to be treated as high risk, despite measures taken by Saudi Arabia which have drastically reduced the risk of TF in the sector. Banks do not generally perform a specific risk assessment of such customers based on each customer's detailed profile. While the relevant additional due diligence measures are applied to such high-risk customers, this approach potentially results in an excessive compliance burden on FIs, and may discourage them from fully understanding and mitigating the specific risks posed by their customers. SAMA should consider updating their guidance in this area to allow for a more graduated approach.

340. Securities companies (APs) and finance companies have adopted internal risk assessment mechanisms and have clear measures in place to mitigate the identified risks.

341. Large-scale DPMSs interviewed appear to have well implemented risk mitigating measures in place. Institutional risk assessments allow them to have knowledge of high-risk areas, including stores in high-risk regions and cash transactions, and applied enhanced measures accordingly.

342. Accountants and lawyers carry out risk assessment at the start of a customer relationship and update it annually. However, they do not have clear knowledge on identifying high-risk customers and the risk mitigating measures that should be consequently taken.

343. As stated above, the understanding of ML/TF risk by real estate agents is at a low level and risk mitigating measures are almost absent.

Application of CDD and record-keeping requirements

344. CDD requirements are generally well implemented within the financial sector, but deficiencies in this regard still remain (see tables in IO3). All prospective customers in Saudi Arabia, whether natural or legal persons, are required to be

physically present for verification purposes. The national ID system and associated database in Saudi Arabia (the shomoos) helps FIs and DNFBPs to carry out CDD. For individual customers, the online national ID system in Saudi Arabia allows banks and all the other regulated sectors to access the national ID information held by the MOI and to verify customers' identity. Information held in the national ID system includes names, ID number, date of birth, address, mobile phone number, picture, passport number, etc. For foreign workers in Saudi Arabia, a comparable database is used for the same purpose.

345. For legal persons, MOCI provides a platform for FIs to check basic information of the legal person in the commercial register (CR). Financial institutions also require the basic founding documents, as well as other documents that identify the beneficial ownership of the company.

346. For endowments (mainly waqf), banks and securities require a deed issued by the court that includes information of the settler, trustee, beneficiaries, etc. The identity of the trustee of an endowment is also required to be verified by banks and securities companies.

347. In general, interviewed FIs and DNFBPs are aware that if CDD cannot be completed, they should refuse or terminate the business relationship. According to SAMA, in 2016, 571 relationships were declined due to difficulties in complying with CDD requirements or concerns about the potential risk of ML/TF. Some of the interviewed securities firms, DMPS and lawyers also provided such cases.

348. There are 730 remittance centres in Saudi Arabia that are exclusively operated by domestic banks. Customers of these remittance centres are required to have a membership that is obtained after completion of a KYC process similar to that applied for opening a bank account.

349. Record keeping seems well-implemented; FIs and DNFBPs keep documents for 10 years, which goes beyond the requirement in the FATF standards. For FIs and large scale DPMS, digital systems are used to keep records. Real estate agents appear not to have clear awareness of keeping record as an obligation. However, given the limited role of real estate agents and the duplication of safeguards on real estate transactions through public notaries, this is not a major vulnerability.

350. Beneficial ownership is identified during the customer on-boarding stage and during the relationship. For natural persons, banks monitor transactions in the account to ensure it is used for the benefit of the account holder. For domestic companies, banks rely on legal ownership information obtained at the customer on-boarding stage and verified through commercial register information held by MOCI. For joint stock companies, shareholders who own more than 5% of shares should be identified. Banks interviewed indicated that the relationship managers visit their corporate customers in person and then update beneficial ownership information when needed or on an annual basis. For foreign companies operating in Saudi Arabia, when starting a relationship, information including ownership structure and identities of all shareholders will be required by the bank. Banks interviewed stated that identification of the beneficial owners is based on identifying the physical person behind any legal ownership. The same was confirmed by MOCI. Supervisors' findings after inspections show that some banks did not update beneficial ownership information after it had changed in the course of business relationship.

351. Other FIs including financing, insurance and securities companies also showed a good degree of implementation of CDD and KYC requirements. Insurance companies in Saudi Arabia are not allowed to use agents on life insurance business and have to establish a face–to-face business relationship with customers.

352. Class A money exchangers have in place KYC procedures. They identify and verify natural and legal customers' ID respectively through MOI and MOCI's systems. At the same time, customers who seek remittance services are also routinely required to provide justifications about the source of funds and the purpose of the transaction and remitters check whether the transactions are consistent with their customers' profiles.

353. Most DNFBPs interviewed have a general awareness of CDD requirements, but the level of understanding varies. The use of national databases to verify the customer's identity is sometimes limited in practice; real estate agents interviewed stated that verification of a customer's identity is not always performed given their limited role and reliance on Public Notaries within Ministry of Justice who are controlling and executing all real estate transactions in the Kingdom. They confirmed however that they do it as a first level of verification by contacting the Ministry when the transaction is very important. One real estate agent stated that they have access to national Shomoos system to check and verify their customers' IDs and such access would be generalised soon in the sector.

Application of EDD measures

354. Under the current legislative framework, FIs and DNFBPs in Saudi Arabia are required to take enhanced CDD measures in line with FATF standards' requirements, namely with respect to PEPs, wire transfers, correspondent banking relationships, high-risk countries, and whenever they identify a high ML/TF risk in relation to a specific customer, transaction or relationship.

355. Risk associated with PEPs appears well managed by FIs and major DNFBPs (lawyers, large scale DPMS). Requirements on PEPs are clearly set out in relevant rules and regulations, and instructions were given by competent authorities; this allows FIs and major DNFBPs to be well aware about the risks associated with PEPs. Financial institutions and DNFBPs are required by competent authorities to list all PEPs as high-risk customers and apply additional measures. Screening systems such as WorldCheck are widely used by the financial sector and major DNFBPs to identify PEPs. Some banks adopted a more conservative approach and listed professions such as journalists as PEPs or as high-risk customers. Large scale DPMS interviewed indicated that they carry out comprehensive training for employees and help them to identify PEPs. Other DNFBPs indicated that they face a challenge in identifying family members and close associates of a PEP.

356. Shortly prior to the on-site visit, over two hundred individuals - many of them PEPs - were arrested in connection with investigations into long-running and large-scale corruption, estimated to have stolen up to USD100 billion over the last ten years. Authorities confirmed that FIs filed STRs regarding a number of individuals involved in these cases. No more information was provided on how thoroughly FIs applied enhanced measures regarding these PEPs.

357. Correspondent banking relationships appear to be well managed. Interviewed banks have good awareness of risk associated with, and procedures in place to manage correspondent banking relationships. Banks tend not to maintain correspondent banking relationships with high risk countries and regions and take enhanced measures against those identified by FATF and local authorities.

358. Major FIs (banks, finance companies, security companies) took the risks associated by new technologies/products into consideration and applied relevant risk mitigating measures. New electronic payment methods including prepaid card, on-line payment, etc. are only offered to customers who already have an account. Interviewed banks also ensured that all these transactions are subject to transaction monitoring.

359. Financial institutions are aware of their risks and obligations with respect to UN sanctions and domestic sanctions lists. The awareness among DNFBPs is weak; however, large scale DPMS and lawyers understand their obligations to a certain degree and have adopted relevant measures. Financial institutions indicated that there is no major problem in obtaining UN lists since WorldCheck is widely used in the financial sector. SAMA and MOCI provide the relevant information and they also check UN website regularly for any updates and information. Financial institutions have a clear process to check a customer's name against UN sanctions lists at the on-boarding stage and while conducting transactions and are aware of the requirement to immediately freeze funds and assets. Supervisors including SAMA and CMA indicated that they included the implementation of sanctions' requirements into their inspection plans.

360. Financial institutions and DNFBPs have a good awareness of high-risk countries identified by FATF. Financial institutions obtain lists of high-risk countries through the AMLPC website - which is directly linked to the FATF website - and can easily consult it to check for updates. SAMA indicated that extra efforts were taken by some banks regarding countries in conflict zones and EDD measures were put in place in relation to those.

Reporting obligations and tipping off

361. Suspicious transaction reporting obligations are established for FIs and DNFBPs. In general, FIs have better awareness and more resources on suspicious transaction reporting than DNFBPs. The number of STRs received from SAFIU confirmed that the majority of the STRs were submitted by FIs, more specifically by the banks.

Table 26. Suspicious Transaction Reports

Year	2014		2015		2016	
Type of STR	**ML**	**TF**	**ML**	**TF**	**ML**	**TF**
FIs	1 967	77	3 252	140	5 723	140
DNFBPs	4	1	5	2	17	14
Government authorities	241	9	244	39	220	10
Individuals	28	39	33	51	42	204
Sub total	**2 240**	**126**	**3 534**	**232**	**6 002**	**368**
Total	**2 366**		**3 766**		**6 370**	

Table 27. Reporting Institutions

Reporting Institution	2014	2015	2016	2017
Banks	1906	3302	5755	5552
Finance companies				11
Insurance companies offering life insurance services	5	1	2	19
Insurance brokers				
Securities Services	71	38	65	130
Money exchangers (A)	62	51	41	110
Money exchangers (B)				
Real estate agents	1			3
Public notaries	11	9	10	9
Accountants				1
Lawyers	1	1	7	9
DPMS	1			13

362. The banking sector reported the highest number of STRs. Banks interviewed demonstrated having comprehensive monitoring systems and mechanisms for reporting STRs from generation of alerts to human analysis and issuing the report. Banks use ML/TF red flag indicators and typologies published by supervisors and adapt them to their own business and risk framework. AML units within interviewed banks are well resourced which allow them to fulfil their obligations. Banks adopted a graduated approach with different thresholds of transaction monitoring for different groups of customers.

363. Despite the high TF risks in Saudi Arabia, the number of TF-related STRs is relatively low, especially from banks, class A money changers and DPMSs which are all identified as high-risk sectors in the TF NRA. In addition, the number of TF investigations triggered by STRs is relatively low (see table in para 207 of IO10). The STR reporting system is not realising its full potential as a tool to identify and combat TF.

364. Other financial sectors also have clear awareness and mechanisms in place regarding transaction monitoring and reporting of STRs, but the number of STRs they reported is low, especially by finance companies and insurance companies. No information is available on how many cases have been initiated on the basis of STRs from these sectors.

365. DNFBPs report STRs, but the number is relatively low. Supervision authorities indicated that, thanks to the supervisory campaigns in mid-2016, awareness of reporting entities and the number of STRs reported increased. Please refer to the above table on the number of STRs reported by each sector.

366. The real estate agent sector has a low level of STR reporting. However, public notaries (which are responsible for executing real estate transactions) do report a greater number of STRs. Real estate agents and their supervisor (MOCI) both consider the ML/TF risks to the sector low. Taken together the level of STR reporting regarding real estate transactions seems proportionate to the risks.

367. Limited feedback on typologies and effectiveness of STRs has a negative effect on the private sector's ability to report suspicious transactions. Most FIs and DNFBPs interviewed expressed that feedback is received from SAFIU after an STR is reported, but such feedback is limited to confirming the receipt of the STR, thus there is a lack of information about the effectiveness of the STR.

368. FIs and DNFBPs are aware of the obligation on preventing tipping-off. However, the methods used to report STRs, for instance by fax, is not efficient and may also raise concerns about confidentiality issues. Assessors reviewed a number of cases where reporting entities failed to submit an STR promptly.

Internal controls and legal/regulatory requirements impending implementation

369. Most FIs, especially banks, have comprehensive internal controls in which AML/CFT obligations including CDD, record keeping, transaction monitoring are well embedded. AML/CFT compliance at group level (including overseas branches) was also covered while regular internal and external audit ensures its effective implementation.

370. For class A money exchangers, internal controls are weak, especially on TF, and this is one of the major reasons that led supervisory authorities to suspend remittance licenses of three Class A money exchangers (see para 10). As a result, these money exchangers took remedial actions to improve their internal controls, including by getting support of a consulting company.

371. Among DNFBPs, internal controls are not well established, except for large scale DPMS.

Overall conclusions on IO.4

372. AML/CFT preventive measures in Saudi Arabia are strong and well established. Thanks to vigorous supervisory measures taken by competent authorities, the level of understanding of ML/TF risk and awareness of AML/CFT obligations among reporting institutions improved significantly in the recent years, especially among DNFBPs. Reporting of STRs is however a major concern given the TF risk profile in Saudi Arabia and the low number of STRs reported by TF high-risk sectors.

373. Implementation of the risk-based approach among different sectors is uneven. Major FIs including banks, securities and financing companies have a good level of implementation of the risk-based approach, while other sectors, especially class A and class B money exchangers are applying the risk-based approach at a low level. Among DNFBPs, the understanding of ML/TF risks and implementation of the risk-based approach by large scale DPMSs is a strength; other DNFBPs are still at the beginning stage and need more efforts to understand the ML/TF risks and AML/CFT obligations.

374. **Saudi Arabia is rated as having a moderate level of effectiveness for IO.4.**

CHAPTER 6. SUPERVISION

Key Findings and Recommended Actions

Key Findings

- As noted in ch.1 and IO.4, the financial sector and DNFBP sectors in Saudi Arabia are relatively small, and primarily serve domestic customers. The remittances sector is an exception, with Saudi Arabia being the second-largest remittance market globally.
- Supervisors apply strong market entry controls and extensive fit and proper requirements. This system appears to be effective in preventing criminals from owning or controlling institutions.
- Saudi Arabia conducts intensive supervision of the higher-risk financial and DNFBP sectors, and in particular has recently done a great deal of outreach and engagement with regulated entities to communicate their new obligations and supervision arrangements, which appears to have been successful.
- Arrangements for risk-based AML/CFT supervision of FIs are becoming established, while for DNFBPs these arrangements have been introduced in mid-2016 for some sectors. For DNFBPs it is too early to reach a conclusion about its effectiveness.
- Indications are that the system in place for supervision of FIs achieves a substantial level of effectiveness: financial supervisors have a good understanding of the ML/TF risks based on the NRAs, and a sound model for risk-based supervision; and good communication and relations with their sectors.

Recommended Actions

- Sustain the changes that have been out in place in the last two years to AML/CFT supervision of the financial sectors.
- Continue to establish AML/CFT supervision of the DNFBP sectors, including by establishing a regular/permanent supervisory team for inspection of accountants;
- Ensure that the obligations introduced through the new AMLL and CFTL and their implementing regulations are quickly and properly implemented.
- Consider developing an even more granular ML/TF risk understanding of individual FIs, and update the risk analysis to capture the evolving ML/TF risks in the financial sector.

375. The relevant Immediate Outcome considered and assessed in this chapter is IO.3. The Recommendations relevant for the assessment of effectiveness under this section are R.26-28, R.34, and R.35.

Immediate Outcome 3 (Supervision)

376. The legal and regulatory framework of AML/CFT obligations in Saudi Arabia was reformed very recently. New AML and CFT laws were introduced in October 2017 (immediately prior to the onsite), which enacted most of the new requirements of the 2012 revisions to the FATF standards. At the time of the onsite, some of these had not yet been widely implemented - although many were already implemented, e.g. as a part of group-wide policies or risk-based measures.

377. The practical arrangements for supervision have also been subject to significant changes in the past years. SAMA is responsible for supervising the financial sector including banks, insurance companies, Money exchangers and finance companies, and has applied a risk-sensitive approach to supervision since 2011. SAMA reorganised its supervision function in 2013 (with the creation of a deputy governor post responsible for supervision) and again in early 2016 (with the establishment of a dedicated AML/CFT Department reporting to the deputy governor). This has significantly increased the resources and focus devoted to AML/CFT within SAMA, including through the use of a new risk model. Many elements are well-established and the current risk-based supervision model put in place in 2016 is in line with the FATF recommendations. However there has been only a limited time for the effects of the changes introduced in 2016 - in particular the most recent risk model - to be felt in practice.

378. Risk-based AML/CFT supervision of DNFBPs also started in 2016. The MOCI, MOJ and SOCPA supervise the DNFBPs (DPMS, lawyers, accountants and real estate agents) where AML/CFT supervision was introduced in the on-site inspections in the last quarter of 2016, using a model prepared in 2016 and based on information collected on the ML and TF risks in the different sectors. There has been sufficient time for DNFBP supervisors to conduct some outreach about the new obligations. Their main activity since mid-2016 was awareness-raising though onsite inspections to assess the level of compliance were also carried out.

379. Saudi Arabia's national risk assessment was completed in April 2017 and endorsed in August 2017; it forms the basis for risk-based supervision. It identifies the banking sector (97 % of the financial sector is dominated by Banks), money remitters, finance companies linked to local banks and DPMS as high-risk sectors for ML and TF. Some DNFBP sectors pose low risks: real estate agents have very limited role in real estate transactions (being controlled by public notaries in the court). Accountants and Lawyers do not have the right to act on behalf of their customers (performing financial transactions) and casinos and TCSPs do not exist in the Kingdom. Saudi Arabia is not a major financial centre: the financial and DNFBP sectors serve mainly domestic customers (with the exception of the remittance sector, which is significant due to the Kingdom's large population of migrant workers).

Licensing, registration and controls preventing criminals and associates from entering the market

Financial Institutions

380. SAMA and CMA, apply extensive fit and proper tests to all senior staff and shareholders of FIs, and have demonstrated that these tests are applied rigorously in practice, including through regular refusals to approve inappropriate appointments. This system appears to be effective in preventing criminals from owning or controlling FIs.

381. SAMA and CMA conduct fit and proper checks at the time of licence application and periodically throughout the licence period to ensure that the fit and proper criteria are always met. During the licensing process, they follow detailed due diligence processes; apart from obtaining self-declarations from applicants about meeting the fit and proper criteria, clearance from various agencies, including criminal records from police are obtained. In case of foreign banks, SAMA also obtains detailed reports from home supervisors and checks the policies and procedures followed by such banks.

382. All supervisors check by means of criminal records to assure that criminals and their associates do not own or hold a significant function in an institution. All investments are through banks and banks conduct due diligence exercise to ensure that only legitimate funds are involved in such transactions as well.

383. Fit and proper tests are be implemented rigorously: SAMA rejected 41 applications during the period 2014-2016 from banks, insurance companies, finance companies and money exchange companies; The most common reasons for rejections are lack of expertise and inappropriateness of the work plan submitted. Some of the main reasons for rejection of applications cited by SAMA are submission of inaccurate or misleading information, lack of expertise/appropriate qualification of candidates/Board of Directors, inappropriateness of work plans submitted, etc. With respect to foreign banks, reasons for rejection include name in the 'sanction list' and lack of internal policies and controls to prevent terrorism financing. SAMA maintained 53 applications during the period 2014-2016 i.e., those which are kept on hold waiting for the missing information to be provided before making a decision on the application.

Table 28. Statistics on licenses applications 2014-2016

Year	Sector	Licenses Granted	Applications Rejected	Applications Maintained*	Total
2016	Banks	1	1	2	**4**
	Finance companies	4	-	3	**7**
	Insurance companies	-	-	-	**0**
	Exchange companies	1	6	10	**17**
2015	Banks	1	-	4	**5**
	Finance companies	12	-	2	**14**

Year	Sector	Licenses Granted	Applications Rejected	Applications Maintained*	Total
	Insurance companies	-	-	-	**0**
	Exchange companies	11	6	4	**21**
2014	Banks	1	4	3	**8**
	Finance companies	15	-	13	**28**
	Insurance companies	2	-	-	**2**
	Exchange companies	11	24	12	**47**

Note: * Maintained applications are those kept on hold waiting to be completed.

384. CMA also applies a detailed process for issuing licences to APs to operate in the Capital Market. During the period 2014-2016, CMA received 5 applications, rejected 3 and granted 2 licences. Reasons for rejection include failure of fit and proper test due to previous violations of the CML. Similarly, eight applications for change of ownership during the same period were rejected while 11 applications were withdrawn.

385. Approvals of supervisors are also required for appointments to the leadership positions including to the Board of Directors in FIs. The fit and proper criteria include absence of any criminal record, adequate experience and expertise, etc. As per the information provided by SAMA, 47 applications for leadership positions in banks, insurance companies and money exchange companies were rejected during the period 2014-2016. 37 applications for leadership positions with APs were rejected by CMA or withdrawn during the same period.

DNFBPs

386. There are strict entry requirements for DNFBP sectors, with regulators having strong fit and proper criteria and detailed due diligence processes:

- For Lawyers, the Ministry of Justice (MOJ) obtains information through the Ministry of Interior (MOI) on the criminal background of the lawyer. The MOJ continuously receives information on lawyers for instance from Ministry of Interior and Courts, to ensure that the licensees do not violate the profession requirements. During the period 2015-2016, the MOJ rejected 27 applications of prospective lawyers and three lawyers were banned from further practicing.
- To operate, Dealers in Precious Metals and Stones should request the approval of the relevant supervisory authority, the Ministry of Commerce and Investment (MOCI), and that of other competent authorities such as the Municipality and the Public Security. To ensure that criminals do not enter the market, a new dealer should also provide 2 recommendation letters from dealers working in the field and endorsed by the Chamber of Commerce. No case of illegal dealers has been detected; there were a few cases of dealers opening a new branch without the required license, which were quickly detected through the regular inspections and sanctioned.

- The MOCI is the licencing authority for Real Estate Agents. To operate in this sector applicants should be of good character and without any criminal background for which declarations are obtained. The MOI maintains a black list of undesirable persons and MOCI checks this list while considering applications. MOCI has the right to withdraw the license from real estate agents who have been subject to adverse information obtained for instance from the FIU or law enforcement authorities.
- Saudi Organisation of Certified Public Accountants (SOCPA) under MOCI has the responsibility of regulating and supervising CPAs. The SOCPA applies conditions and procedures for issuing licenses to CPAs. During the last three years, 220 licences were issued and 12 license applications were rejected. Reasons for rejection were generally related to insufficient qualifications or experience.

Supervisors' understanding and identification of ML/TF risks

387. While the ML and TF NRAs were concluded in 2017, the process started two years before, thereby making supervisors sensitive about various ML and TF risks. Supervisors assessed the ML/TF risks of their respective sectors based on a number of tools and methods that also allow them to incorporate the results of the NRAs.

388. Financial supervisors' understanding of ML/TF risks in their sectors is comprehensive as it is based on the assessment of the risks faced by each financial institution using a Risk Matrix Tool, which has also provision to incorporate the results of the ML and TF NRAs completed in August 2017. The Risk Matrix Tool considers (i) *the inherent risk (based on the size and nature of the customer base, sectors and activities of the bank and associated businesses such as remitters etc.), (ii) the internal controls (based on supervisory findings), (iii) the residual risk (based on the degree to which risks have been mitigated) and (iv) the impact of the financial institution*. The *impact of the financial institution* on the sector depends on the size/share of the financial institution and its reputation. While assessing FIs, supervisors also use information received during meetings with FIs, information from previous inspections and inputs from agencies such as the FIU. This model seems to provide a sophisticated and sound basis for providing supervisors with a granular understanding of the risks faced by each institution, which could support targeted risk-based supervision. This model became fully operational as the basis for targeting on- and off-site inspections in the second half of 2016. Previous supervisory activity was risk-based, but used a less sophisticated risk model, focused primarily on the degree of risk posed by each sector as a whole.

389. CMA has also adopted a Risk Matrix Tool in 2016 similar to that of SAMA to assess and rate the entities under its supervision. The Risk Matrix Tool has also provision to incorporate the results of the ML & TF NRAs. When analysing the AML/CFT risk of the APs, CMA considers many indicators for the classification of the APs in the category high or very high risk including inherent and business risks), the impact of the AP (number of non-resident customers, number of offices, staff, customers, higher-risk customers, transactions, etc.), CMA's judgment on the internal controls (AP's risk assessment, AP's risk-based approach, MLRO, CDD, monitoring, STRs, etc.) and other indicators including the ongoing inspections.

DNFBPs

390. In the second half of 2016, the MOJ and the MOCI conducted a risk rating exercise for DNFBPs involving the use of questionnaires for data collection, outcomes from onsite visits and meetings with DNFBPs, inputs from some government agencies like the FIU and customs, as well as the results of the NRAs. This is being used as a basis for risk-based supervision. The MOJ used a questionnaire to determine the risks related to each lawyer based on four risk factors: customers, services provided, geography and delivery channel of the business performed. The high-risk category includes mostly the large law firms and those located in high-risk areas (near conflict zones).

391. The MOCI made risk-evaluations for the DPMS and the real estate sectors. DPMS's ML/ TF risks were assessed based on collection and analysis of information from different sources and authorities such as the Ministry's information centre, the General Customs Administration (data on import/export), the Council of Saudi Chambers, among others.

392. The SOCPA also conducted an assessment of the risks of CPAs based on the collection and analysis of information including the volume of accounting and auditing market, the volume of fees during one fiscal year, the type of business (auditing/consulting), the number of customers and the committed violations.

393. In Saudi Arabia, all financial statements are available on an online platform called 'Qawaem' which supports credibility and transparency. This also helps supervisors, especially in DNFBP sectors, to better understand the business of their supervised entities.

Risk-based supervision of compliance with AML/CFT requirements

Financial Sector

394. Financial supervisors started a full risk based supervision and monitoring of compliance with AML/CFT requirements which became operational in March 2016. Prior to that, AML/CFT supervision in the financial sector by SAMA and CMA was part of the general supervision procedure and risk-sensitive. In 2016, the FIs were risk rated for AML/CFT as per the Risk Matrix Tool, and supervisors started fully applying the risk based supervision. Priority for onsite inspections was given to high risk entities, some of which had more than one follow-up visit during last year. Extensive onsite supervision was performed since then, and 66% of FIs had been inspected by the time of the on-site with focus on the higher risk institutions.

395. Within SAMA, the AML Department (AMLD), is in charge of supervising AML/CFT compliance of FIs in SAMA, currently has 26 staff, working on offsite and onsite supervision, as well as preparing AML/CFT regulations and guidance. This has significantly increased the capacity and expertise of SAMA in AML/CFT.

Table 29. AML/CFT inspections made and number of staff involved since 2016.

Financial institutions (FIs)	No. of FIs	FIs visited	No. of Staff		Working Days
			AML	General	
Local banks	12	12	59	9	830

Branches of foreign banks	12	10	28	3	150
Money exchangers (A)	4	4	9	2	55
Money exchangers (B)	69	67	73	15	102
Finance Companies	34	11	32	7	192
Insurance Companies	24	17	51	0	183
Brokers	40	6	18	0	36
Total	**195**	**127**	**268**	**35**	**1548**

396. Since the start of full implementation of risk based supervision in 2016, SAMA has inspected 130 out of the 195 FIs under its supervision (66% of the FIs); it has inspected all the seven high risk entities (three banks and four money exchange companies, class (A), all the 22 upper medium risk entities, 29 of the 69 lower medium risk entities and 59 of the 97 low risk entities. In 2017, CMA made onsite inspection for the two APs which are rated as 'very high risk' (three other APs rated as very high were inspected in December 2016) and seven of the 10 APs which are rated as 'high risk". The 52 medium- and 19 low risk-rated APs have not been subject to AML/CFT-focused inspection by CMA. At the time of the onsite visit however, the CMA had held compliance meetings with seven of the medium risk rated APs. Box 21 gives examples of the impact of supervisory action on remittance providers

DNFBPS

397. AML/CFT focused supervision for DNFBP sector started in early 2017 though it mainly took the form of outreach programmes and campaigns for raising awareness about AML/CFT risks. Priority was given to high-risk rated entities: the frequency and intensity of supervisory visits to those firms was high. Being relatively new to AML/CFT focused inspections, the DNFBP sector was first subject to awareness-raising inspections, in order to make the entities aware of the newly-introduced AML/CFT requirements, including the need for CDD, identification and reporting of suspicious transactions, etc. During discussions with private sector, it was confirmed that meetings with the MOCI and the MOJ had given obliged entities a better understanding of the risks associated with ML/TF and had become much more sensitive to the AML/CFT requirements.

398. Supervisory visits to Real Estate Agents till 2016 were not focused on examination of ML/FT risks as such risks in this sector are considered as low. In part this is because the role of the Real Estate Agents in real estate transactions is very limited as such transactions also have to go to through Public Notaries (who are Government officials), foreigners have very limited access to the domestic real estate market and cash transactions are allowed only up to SAR 100,000. Nevertheless, AML/CFT obligations should apply to both notaries and real estate agents. The MOCI conducted 1,840 supervisory visits to REAs in 2015 (not AML/CFT focused though AML/CFT aspects were also looked into during such visits), and conducted 1,079 and 3,824 AML/CFT focused visits respectively in 2016 and 2017 (up to August).

399. The frequency and intensity of inspection of the legal profession is high. In 2017, the MOJ made supervisory visits to about 300 law firms. As per the planned inspection programme, high risk lawyers will be inspected 3 times per year, the medium risk lawyers twice per year and the low risk lawyers once per year. The 700 lawyers that were classified as very-low risk will be inspected randomly or if there is a special need.

400. For the DPMS sector, the MOCI has deployed a total of 75 inspectors specialized in AML/CFT and who are distributed over the different regions and major cities of the Kingdom. During 2017 and up to the time of the visit, supervisory visits were made to 15 high-risk rated entities, 14 entities which are rated as high moderate risk, 106 moderate-risk rated entities, 458 entities which are rated as low moderate risk and 181 low-risk rated entities. The duration and intensity of the inspections varies with the risk profile of the specific DPMS. Besides, 17 high risk entities were subjected to special extra visits by the dedicated inspectors in 2017. Breaches noticed mainly relate to non-compliance with control measures published by the Ministry in addition to failure to applying required CDD measures when applicable.

401. For supervision of accountants, there is no dedicated staff of supervisors. Onsite inspections are carried out by 2-3 members of SOCPA. In early 2017, SOCPA applied the risk based supervision whereby it conducted focused inspection of 8 of the 18 high-risk rated CPAs, 15 of the 87 CPAs rated as medium risk and 10 of the 70 ones rated as low-risk. During the period from 2014 to 2016 - before ML/TF focused approach was adopted- SOCPA had conducted 359 supervisory visits to CPAs. SOCPA selects its supervisors from a pool of experienced experts in the accountant firms to execute the inspections. It has used 40 full-time and part-time examiners during the last three years. Inspection teams consist of two or more persons depending of the size of the inspected firm. It may be advisable to have a regular/permanent supervisory staff to ensure that inspections are carried out in a consistent manner.

Remedial actions and effective, proportionate, and dissuasive sanctions

402. Supervisors of the financial and DNFBP sectors have adequate powers and are armed with a range of measures from issuing warnings to withdrawal of licences, as noted in the TC analysis of R.35. SAMA and CMA have imposed sanctions for violations of AML/ CFT rules by obliged entities. For the DNFBP sector, since that the focus on AML/CFT rules started in early 2017, cases of violations of AML/CFT rules were dealt with gradually. As noted above, the current supervisory regime of DNFBPs has not been in place for long enough to review a full cycle in which violations were identified, sanctioned, and remediated.

Box 22. Inspection and remediation action.

During the period 2011-2017, SAMA conducted four inspection visits to one of the largest domestic banks (in terms of customer base and volume of transactions). The visits revealed some discrepancies in the application of AML/CFT requirements. Accordingly, financial penalties were enforced against the bank amounting to SARs 2 820 000 (US$ 752 000).

The first and second visits were made in 2011 and 2012. The inspection examined, among other things, transaction monitoring systems where several weaknesses were identified. The bank was required to set corrective measures, including obtaining an advanced automated monitoring system, and hiring and training new staff to investigate alerts of suspicious financial transactions.

The third and fourth inspection visits were made in 2016 and 2017 and again reviewed the transaction monitoring system, looking at its efficiency and the

quality of its outputs. A number of observations were made by supervisors, including: raising the efficiency of monitoring through corrective measures aimed at the inclusion of the bank's activities; creating a mechanism to develop profiles for the automated system; and provision of sufficient resources to effectively deal with the alerts generated by the automated monitoring system (including the number and training of staff); and providing staff with tools to obtain the data required for conducting such operations.

These interventions have led to a significant increase in the Bank's capacity - from 19 investigators at the beginning of 2014, to 47 at the end of 2017, with corresponding improvements in training and tools.

403. Supervisors in the financial sector have been imposing sanctions to ensure that FIs are complying with AML/CFT laws and regulations. SAMA issued six sanctions on banks in 2014 for AML/CFT violations and 25 in 2015. In 2016, SAMA issued 26 sanctions on banks and money exchange companies, and 13 sanctions were issued up to August 2017. Table 30 below summarises the types of deficiencies identified in the banking sector, and the types of sanctions imposed.

Table 30. Banking sector deficiencies and sanctions

Year	Total	Type of AML/CFT Violation						Sanction imposed		
		CDD Measures	Failure to provide information	Monitoring systems	KYC rules	Internal Controls	Risk assess-ment	Notice	Fine **	Corrective Procedure
2014	6	3	1	1	1	-	-	4	5	6
2015	25	14	3	3	-	5	-	25	25	15
2016	26	24	-	-	-	12	1	26	26	-

Notes: * note that columns do not sum, since a single case may involve multiple violations and multiple sanctions.
*** Fines ranged from SAR 5000 to SAR 2,455,000 (EUR 1,000 to 500,000). The average fine was SAR 162,000 (EUR 35,000)*

404. With respect to insurance and finance companies, SAMA issued in 2017 respectively five and four sanctions. Similarly, CMA imposed fines on 5 APs in 2014 for violation of AML/CFT rules and altogether 16 in 2015 and 2016. After starting the ML/TF focused inspections in late 2016, sanctions were imposed on 11 APs as of October 2017.

405. During January – August 2017, SAMA suspended the licences of three of the four Money Exchangers class (A) for persistent AML/CFT violations despite the repeated warnings including summoning of Chairmen. These cases are set out in more detail in Box 21.

406. For lawyers, the MOJ initiated awareness campaign visits in 2016, which were followed up with supervisory visits during 2017 and wherever deficiencies were identified, law firms were requested to develop a corrective action plan in order to address the deficiencies within a specific timeframe. Further inspections are then made to ensure that corrective measures have been taken. It has been reported that

11 law firms which failed to fix their deficiencies have been referred to the Disciplinary Committee for considering further actions. At the time of the visit of the assessment team, decisions in this regard had not been taken.

407. The MOCI has a graduated approach to sanctioning its obliged entities, beginning with a written commitment to comply with the AML/CFT requirements upon the first violation. If the violation is repeated, the owner of the facility or its chief executive shall be summoned to the Ministry and heard, and a warning letter from the Minister will be sent. In case of further violations, the matter would be referred to the public prosecutor. In the DPMS sector, supervisors have so far been not opting to apply formal sanctions even in one case of repeated breaches of AML/CFT rules and supervisory instructions - though in this case the DPMS chain's owner was summoned to the Ministry to account for breaches. MOCI considers that this supervisory action led to prompt remediation. This is appropriate to the newly-established supervisory regime, but should transition to an established system with an expectation of sanctions for non-compliance.

408. Up to 2017 in the DNFBP sectors, AML/CFT rules were looked into as part of general control visits. Supervisors started a vigorous awareness campaign on AML/CFT issues from 2016 and this was followed by AML/CFT onsite inspections. Since AML/CFT focus is at initial stages, supervisors followed a graduated approach with respect to imposing sanctions; after the first round of onsite inspections, entities were asked to submit firm commitments to address the deficiencies identified. During the second round of inspections, wherever the deficiencies were not rectified/violations persisted, supervisors resorted to summoning the concerned entities, issuing warning letters, and in case of repeated violations, serious sanctions would be imposed. This appears to have had a positive impact and there was a huge improvement in this sector.

Impact of supervisory actions on compliance

409. Over the past years, deficiencies in implementation of AML/CFT laws/rules have come down considerably due to the persistent efforts of supervisors. Apart from increasing the frequency and intensity of supervisory interventions (including follow up visits to ensure proper submission of compliance reports/rectification plans) wherever required, information made available shows that supervisors are not hesitating to resort to sanctions including suspension of licenses in some cases. This was confirmed during discussions with private sector as well. Thus, for example, the case of suspension of money remittance facilities offered by three of the four Money Exchange Companies class (A) which were allowed to undertake this activity, gives a strong message to other entities in the kingdom that non-compliance with laws and regulations would not be tolerated.

410. SAMA has shown that the number of STRs filed by its regulated entities have increased considerably during recent years. In DNFBP sector also, especially DPMS, there was an increase in the number of STRs submitted last year, after the MOJ and the MOCI initiated an awareness campaign. This is set out in the analysis of IO.4 - in table 27 on page 114.

411. Details provided by SAMA and CMA show that there were vigorous follow up measures including follow-up visits after inspections to ensure that the FIs address their deficiencies and comply with the requirements. The table below (Table 5.)

shows that the follow-up process had a positive impact on the compliance by the entities under SAMA supervision. The follow-up actions indicate the extent to which these entities respond timely to address the shortcomings and to mitigate ML/TF risks.

Table 31**. Progress made by FIs in addressing deficiencies identified by SAMA inspections as of end of October 2017**

Financial Institutions	inspections	observations	Progress reports	Closed observations	Proportion closed	Follow up meetings to discuss action plans.	Follow up visits.
Local Banks	12	486	**18**	**377**	78%	7	4
Foreign Banks	10	190	**13**	**168**	88%	7	7
Finance Companies	11	336	**17**	**236**	70%	3	2
Insurance	17	381	**19**	**253**	66%	4	2
Brokers	6	74	**6**	**30**	41%	-	-
Money Exchanges (A)	4	154	**10**	**148**	96%	2	2
Money Exchanges (B)	67	859	**53**	**831**	97%	2	2
Total	**127**	**2 480**	**136**	**2 043**		**25**	**19**

412. During the discussions with DNFBPs, it was found that the actions of supervisors had a very positive impact on their AML/CFT policies and procedures as they became very well aware of the provisions of the law and have taken effective measures (training staff, monitoring transactions, filing STRs wherever required, etc.) to ensure that these are complied with. An owner of a very well reputed DPMS firm had been associated with the Ministry to conduct training programmes for the sector after being summoned for repeated violations/non-compliance. According to the supervisors, that had a very a positive effect on other dealers and brought out remarkable market discipline.

Promoting a clear understanding of AML/CFT obligations and ML/TF risks

413. There is a good co-operation between FIs, DNFBPs and their relevant supervisors. Supervisors prefer to communicate with regulated entities through regular workshops and meetings, which happen frequently and are well-regarded by industry representatives. Several workshops were also held in order to explain the AML/CFT obligations and the ML/TF risks that the reporting entities are exposed to.

414. Since the start of the AML system in 1995, SAMA has issued and regularly updated various AML/CFT rules for FIs to clarify their AML/CFT obligations. Various topics have been covered such as the ML/TF risk assessment, the risk-based approach, due diligence measures, reporting STRs to the FIU, the responsibilities of the Compliance Officer, staff training, and records keeping. Additionally, a number of workshops have been organised for the private sector.

415. Regular meetings of FIs and supervisors took place where information is exchanged between supervisors and obliged entities; during these meetings, supervised entities get a better understanding of the various supervisory issues and concerns and supervisors seize that opportunity to understand the developments in the market. On a monthly basis, SAMA participates as an observer in several committees attended by all FIs to develop and implement the latest policies and exchange experiences. Topics include the latest rules and regulations, latest FATF publications, ML/TF risks, NRA findings, etc.

416. Financial supervisors also conduct trainings and workshops for the benefit of the employees of FIs. It is also observed that after the conclusion of NRA, workshops were conducted by supervisory authorities to disseminate the findings of the NRA and make the entities sensitive to the AML/CFT risks. Further, supervisory authorities have been issuing instructions through circulars and manuals such as the Manual for Money Exchange Companies issued in 2015, which provides detailed and specific instructions.

417. For the DNFBPs, supervisors initiated an awareness campaign from mid-2016 and during the discussions with private sector, it was confirmed that this had helped them considerably in understanding and addressing AML/CFT risks. It was also pointed out that supervisors were always available whenever clarifications or advises were required.

418. In 2017, the MOJ conducted 3 workshops in co-operation with SAMA and the SAFIU that were attended by 60 Law firms. The MOJ also published a manual for Law firms that explains the AML/CFT requirements and ML/TF risks to which Law firms may be exposed.

419. The MOCI issued a guideline for all entities subject to its supervision and conducted several workshops to promote interaction and communication with the reporting entities and training them on the AML/ CFT requirements. In 2017, MOCI conducted six workshops for DPMS and three for REAs. Similarly, SOCPA held six training programmes for CPAs in 2017

Overall conclusions on IO.3

420. Saudi Arabia conducts comparatively intensive supervision of the higher-risk financial and DNFBP sectors in accordance with a risk-based approach, and in particular has since 2016 done a great deal of outreach and engagement with regulated entities to communicate their new obligations and supervision arrangements, which appears to have been successful. For DNFBPs, the outreach programmes/campaigns started in 2016, and AML/CFT focussed supervision started in early 2017. These arrangements are being further elaborated and enhanced for some DNFBPs and have to be further applied to all the obligations introduced in new laws.

421. The system in place for supervision of FIs achieves a substantial level of effectiveness: financial supervisors have a good understanding of the ML/TF risks based on the NRAs, a sound model for risk-based supervision and good communication and relations with their sectors. All these efforts have resulted in a significant improvement in compliance with the AML/ CFT requirements. For DNFBPs, the pace and intensity of recent activity is impressive, but it is too early to reach a conclusion about its effectiveness.

422. **Saudi Arabia is rated as having a Substantial level of effectiveness for IO.3**

6

CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS

Key Findings and Recommended Actions

Key Findings

- Saudi Arabian authorities have a basic understanding of potential misuses for ML of commercial legal entities, based on the NRA process. The NRA did not cover all legal persons/arrangements. There are many measures that contribute to mitigating the risk of legal entities and arrangements for ML/TF.
- Reliable basic information of most commercial entities is generally available to competent authorities and FIs/DNFBPs through the Companies Register. Commercial entities are required to submit legal ownership and other basic information to the Company Register, and to update it in case of change (with some exceptions up until November 2017); and public Notaries within MOCI verify the documents. Effective sanctions are applied by MOCI and SAGIA to ensure that information provided is accurate and updated.
- Basic information on businesses which are exempt from these requirements (Unlimited (silent) Partnerships and Islamic Partnerships) may not be available.
- Access to beneficial ownership information is also primarily through the Company Registry. Around 83% of the corporate entities have only natural persons as shareholders, which allows for the matching of the legal owners themselves with the beneficial owners presuming are no informal nominees (strawmen).
- Up to November 2017, however, Joint-Stock Companies and Limited Partnerships did not have to report basic or beneficial ownership information to the Company Register.
- Banks and other reporting entities also hold beneficial ownership information and maintain the necessary records when a legal person/arrangement has a customer relationship with them. Legal entities with a capital requirement are obliged to have an initial bank account in Saudi Arabia. Accuracy of and extent to which the information is up-to-date as some weaknesses still exist in banks' ongoing CDD procedures.
- SAFIU has trailed basic and beneficial ownership information; however the authorities did not demonstrate how they chase beneficial ownership information in more complex ownership structure inside or outside Saudi Arabia.
- Saudi Arabia applies controls on foreign ownership of companies, among other measures, that mitigate the risk of misuse of legal persons and arrangements to some extent. Foreign legal persons who want to invest in Saudi Arabia must obtain

a licence from SAGIA, who grants it after conducting verification on the ownership and control structure and financial standing of the foreign investors.

- Waqfs are well regulated and information on their ownership and beneficiaries is available with the Ministry of Justice and accessible to competent authorities. Foundations and Associations are strictly regulated and they are not allowed to send or receive funds from abroad.

Recommended Actions

- Saudi Arabia should conduct a more thorough assessment of the ML/TF risks related to the misuse of legal entities/legal arrangements, and take appropriate and proportionate mitigation measures, wherever required. Agencies such as the Ministry of Justice, FIU and LEAs should provide inputs on criminal typologies on the misuse of legal entities/arrangements.
- Saudi Arabia should cross-match the information available to the various authorities, including by completing the development of the common portal together with GAZT, MOCI, Ministry of Labour and the General Organisation for Social Insurance, to mitigate the use of strawmen.
- Saudi Arabia should introduce appropriate transparency measures for all businesses, including Unlimited (silent) Partnerships and Islamic Partnerships, and for all private waqfs in order to allow the identification of their beneficial owners.
- Saudi Arabia should monitor that the new legislation requiring beneficial ownership information to be maintained by certain companies and provided to MOCI is duly implemented and enforced in a way to ensure that the information is accurate and up-to-date. MOCI should ensure that the information on beneficial ownership available to it is made readily available or shared with all relevant stakeholders involved in the fight against ML/TF.

423. The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The Recommendations relevant for the assessment of effectiveness under this section are R.24-25.[18]

Immediate Outcome 5 (Legal Persons and Arrangements)

424. Different types legal persons and arrangements can be created and can operate in Saudi Arabia. Laws and regulation on commercial entities significantly changed in 2016. In November 2017, a Ministerial Resolution required Joint-Stock Companies not listed on the stock-market, Limited Partnerships and Limited Liability Companies to maintain an updated register of beneficial ownership and to provide it to the Ministry of Investment and Commerce. The effects of the Ministerial Resolution cannot be taken into account in the assessment of the effectiveness of the system for

18 The availability of accurate and up-to-date basic and beneficial ownership information is also assessed by the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes. In some cases, the findings may differ due to differences in the FATF and Global Forum's respective methodologies, objectives and scope of the standards.

transparency of legal persons and arrangements. The following is a breakdown of the entities and arrangements active in Saudi Arabia.

Table 32. **Legal entities in existence and legal arrangements created in Saudi Arabia (2013-2017).**

	2013	2014	2015	2016	2017
Unlimited liability company	2 952	3 580	4 132	4 371	4 502
Joint-Stock company	1 629	1 689	1 723	1 734	1 740
Limited-liability company	32 268	43 617	53 839	59 187	63 307
Limited Partnership	1 138	1 306	1 481	1 557	1 611
Unlimited (silent) partnership			Unknown		
Foreign companies	174	366	269	258	377
Associations	95	129	148	161	176
Foundations	630	659	720	844	943
Private Waqfs			6 000		
Public Waqfs			3 093		

Source: MOCI, MLSD, Ministry of Justice, General Authority for Waqfs, Ministry of Islamic Affairs.

Public availability of information on the creation and types of legal persons and arrangements

425. Information about the formation and basic features of commercial entities is available on the website of Ministry of Commerce and Investment (MOCI).[19] Information on the created legal entities is available online for joint-stock companies together with a basic description of activities, contacts and the incorporation date.[20] Additional information on legal entities (such as the names of the directors and legal ownership) and authenticated documents (such as deeds and bylaws) can be accessed for a fee from Saudi Arabia.[21] The process for obtaining and recording beneficial ownership for commercial entities is not explained.

426. Public and private waqfs are private contracts formed under Sharia law and the Law of Procedures before the Sharia Law, and since 2016 are subject to the oversight by the General Authority for Waqfs. Private waqfs must be approved by the Judge at the Ministry of Justice and registered at the General Authority for Waqfs. Public waqfs register with the General Authority for Waqfs (previously with the Ministry of Islamic Affairs). Information on the procedures to establish private waqfs are available on the Ministry of Justice (MOJ) website.[22] MOJ has assigned the work to guide the public about the procedures to be followed for setting up waqfs to certain offices. Before visiting the designated judges for setting up the waqf, people have to

19 http://aamal.sa.

20 http://eservices.mci.gov.sa/Eservices/(S(qwxzjglhomspjs33k0o3vuht))/Commerce/Corporations.aspx

21 http://aamal.sa.

22 https://www.moj.gov.sa/ar/Ministry/Courts/Pages/WaqafSteps.aspx.

go through these offices, that help them to prepare the drafts before submitting to the judge. Information about the waqfs created is not publicly available.

427. Foundations and Associations must register and provide information to the Ministry of Labour and Social Affairs, where a new online portal provides information related to individual NPOs and allows for the searching of information by name, region, size, income, expenditure, liabilities, assets, number of employees, number of volunteers, board members, services provided, and goals.

Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal entities created in the country

428. The Saudi authorities have not yet conducted a sufficiently detailed assessment of the risks associated with each type of legal person in the Kingdom. The assessment focused on the structural elements of the corporate system and the Saudi authorities consider the risks of misuse of legal persons for ML and TF to be very limited in the country in view of the historical, cultural and structural corporate background. The authorities submitted that the Saudi society does not use legal persons for management of private assets and legal persons are formed almost exclusively to carry out viable business (i.e. that complex corporate structures are unusual within Saudi Arabia). In addition, 83% of the companies are owned by natural persons, and access by foreigners to the Saudi corporate market is limited and controlled, with only about 3% of all Saudi legal entities being owned or controlled by a foreign legal entity. There is an understanding of risks related to trade-based money-laundering through companies. The authorities consider that any residual vulnerability is mitigated by the large number of controls and monitoring processes in place.

429. The Saudi authorities did not demonstrate that they have addressed how all commercial legal persons may be misused to perpetrate ML or TF and the conclusion that the historical, cultural and structural background would eliminate the current and future risk of commercial legal persons being used for ML/FT operations is not fully satisfactory. Even though a company conducts legitimate business, it may be misused to launder the proceeds of crime, particularly large proceeds generating crimes like corruption. Despite the fact that most companies are owned by natural persons, it may not be appropriate to rule out the possibility of individuals misusing the company by acting as frontmen for third parties. Lack of complexity is not the only, or even the main, typology of ML using legal persons and arrangements. No typology of misuse of legal person and arrangement was presented to the assessment team.

430. The Saudi authorities consider that the exposure of waqfs to the risk of misuse for ML/TF purposes is limited. This is mainly because of the registration and supervision mechanisms in place (see below), and because even private waqfs would be concluded for "good" purposes only, otherwise the judge would not register the waqf deed. In addition they have not detected any ML cases involving waqfs.

431. Waqfs can be created for both private and public purposes, and it is common practice to use waqfs for profitable private purposes, which include services such as

wealth management for high net-worth individuals,[23] as also confirmed by some representatives of lawyers met during the onsite visit. Any persons, including foreigners, can establish waqfs, provided that the property and the waqif (trustee) are in Saudi Arabia. Waqfs are usually used for real estate, but can be established for all sorts of assets, including to acquire ownership of legal entities in their own name. The Saudi authorities indicated that in the last 4 years 3 093 public waqfs were created, for a total size of assets worth about SAR 16 billion, with annual income of SAR 400 million; 6 000 private waqfs were created with unknown asset worth. The authorities indicated that there has not been a case of ML/TF involving a waqf.

432. Common-law trusts cannot be established under Saudi Arabia legislation. Even though there may be service providers (e.g. lawyers and accountants) who offer the service of establishing and managing a trust created under foreign legislation, the Saudi authorities indicated that they never came across foreign trusts being managed and established in Saudi Arabia. This issue has little materiality in Saudi Arabia.

433. Saudi Arabia assesses the ML/TF risks of Associations and Foundations to be low, due to the tight regulation, supervision mechanisms, and requirements for enhanced CDD in place which mitigate the threats (see Immediate Outcome 10).

434. To sum up, Saudi Arabia has not fully estimated the overall risk of misuse of these legal persons and arrangements for ML/TF and does not have a granular understanding of how they can be, and are being, misused for ML and TF purposes.

Mitigating measures to prevent the misuse of legal persons and arrangements

435. Notwithstanding the insufficient understanding of risk, Saudi Arabia implements many rules-based measures which ensure the transparency of legal persons and help to prevent the misuse of legal persons and arrangements. These are mainly based on the large number of information that must be disclosed to the authorities when creating a person or an arrangement.

436. At the time of registration of a commercial entity, basic information and documentation is disclosed to Company Register, which is part of MOCI. The documents received are reviewed and notarised by Public Notaries working at MOCI. Officers at the Company Register verify that all necessary documents have been duly provided and use the database of the Ministry of Interior (ABSHAR System) to verify the identities of legal owners and administrators who are natural persons and check the names against the list of persons who are prohibited in Saudi Arabia from practicing commercial and investment activities. A list of around 200 names was provided to MOCI by the Ministry of Interior and none of the names included in the list had tried to establish a legal entity. A company does not acquire legal personality until MOCI has completed the verifications and the registration, and a company is not allowed to carry out any business meanwhile. These are effective measures to ensure that real persons are registered and accuracy of information; they do not however limit the possibility of using strawmen as shareholders or as administrators. The Saudi authorities have indicated that the ABSHAR system (the database maintained by Ministry of Interior) can compare a person's lifestyle and living arrangements with his professional or business activities and that strawmen arrangements would likely

23 https://www.alkhabeer.com/WAQF.

be detected during the verification process conducted by MOCI. However, there is no evidence that any remedial action has ever been taken by MOCI or any other authorities on persons who may be acting as shareholders or directors on behalf of someone else. Unlimited (silent) partnerships do not have to register with MOCI.[24]

437. Updated basic information on commercial entities must be provided to the CR, except for joint-stock companies until November 2017. Verifications of the application for entries are performed by Public Notaries and CR officers, and changes take effect only after verification by the CR. Any change in ownership of commercial entities is to be registered with the CR, although the requirement on updating legal ownership of joint-stock companies and limited partnerships was introduced in November 2017 and its implementation could not be tested.[25]

438. Foreign investments are tightly regulated. Foreign legal persons who wish to carry out business in Saudi Arabia or acquire ownership of Saudi Arabia companies must obtain a licence from SAGIA. MOCI relies on the information provided by SAGIA for entering details in CR. As part of the application process SAGIA requires the provisions of a comprehensive set of information, including on the financial standing of the foreign legal person, the ownership and control structure of the foreign legal person, and copies of founding documents and agreements regulating the powers to bind the legal person. Certified documents have to be provided. SAGIA also undertakes a comprehensive screening and verification of each applicant's financial background, ownership and control structure, previous commercial activity, etc. and keeps records of all the documents and records obtained. Updates to beneficial ownership information on the foreign company would not be required to be provided to SAGIA. SAGIA had applied remedial measures in 45 cases between 2014 and 2016 against foreign investors for not providing accurate information and has rejected the application in a number of cases. These regulations on foreign investments provide safeguards on the transparency of foreign companies.

439. Information on the beneficial ownership of companies is also available to FIs and DNFBPs when the company has a relationship with them. Joint-stock companies and Limited Liability Companies are required to deposit 25% of their capital with a Saudi bank before completing registration with the Company Register. For the registration to complete, the Company Register must first receive a notification from the bank that 25% of the capital was paid in effect. This would guarantee that the Company Register is informed of the initial bank account of joint-stock companies, although the Company Register does not maintain updated information on all bank accounts used by Saudi Arabia commercial entities. A number of legal entities have to provide annual financial statements to MOCI (see below), which helps MOCI to determine the bankers of such entities. A number of Saudi Arabia entities may not

24 Unlimited (silent) partnerships do not have a direct obligation to maintain a register of shareholders, but the contract must specify the purpose, the partners' rights and obligations, the management, the distribution of profit and loss and other terms (CL, Art.23, 44 and 45). Partners in unlimited (silent) partnerships continue to be the owner of their shares, unless the partners agree otherwise (CL, Art.49).

25 Existing companies should update MOCI with legal and beneficial ownership information with a delay of maximum three months after the entry into force of the Ministerial Resolution of 14 November 2017.

have a bank account or a continuous relationship with a DNFBP in Saudi Arabia, and so the beneficial ownership of these entities would not be available in the country.

440. Banks complete the due diligence process by verifying the identities of the owners, etc., and also sources of funds by examining the documents and through field visits of their relationship managers. Continuous monitoring of accounts by banks helps to detect any abnormal transaction if there is a different BO. The Company Register, however, is not updated with fresh inputs from banks which notice such changes. The MOCI authorities indicated that the identity of the legal shareholders is verified through the use of databases maintained by the Ministry of Interior.

441. Joint-Stock Companies, Limited-liability Companies and foreign companies are required to submit certified financial statements to MOCI. This occurs via a certified public accountant that uploads the audited financial statements onto an online database ("Qawaem" system). Other legal entities are required to have financial statements verified by a recognised accountant and Saudi Arabia has indicated that Saudi Organisation for Certified Public Accountants has issued a circular requiring all accountants to submit financial statements to the Qawaem system. This database is accessible to MOCI, and produces automatic financial statements to the Tax Authorities. This measure helps to verify that the company has actual business activities and more generally to ensure transparency in financial dealings. The Saudi authorities have indicated that in a number of cases sanctions were imposed in previous years for late filing.

442. As per the guidance given by supervisory authorities, FIs have to place NPOs in high risk category and undertake enhanced due diligence which help to mitigate the ML/FT risks. NPOs are not allowed to either receive funds from abroad or sending cross border remittances (see Immediate Outcome 10).

443. Waqfs are supervised by the General Authority for Waqfs and the names of settlor, trustee, and where available the beneficiaries are recorded by the Courts. The settlor, or a representative, must be present when establishing the deed. Before approving a waqf, the Judge would verify that the settlor effectively owns the property, and that the terms of the waqf respect Sharia law and other obligations included in the Law of Procedures before the Sharia. Once approved, the waqf deeds are scanned and stored on a secured platform available to MOJ and other authorities. When waqfs open a bank account in their names, the banks must receive the documents certified by the Court. Public Waqfs are administered by the General Authority for Waqfs (previously by the Ministry of Islamic Affairs). Even though it is not clear to what extent the supervising Judge would monitor its use (other than by petition), these are strong risk mitigation factors. Waqfs can hold shares in commercial entities; however it is unclear how many waqfs are shareholders in Saudi legal entities.

444. The General Authority of Zakat (GAZT) maintains a database with information on legal entities, such as names of entities, names of shareholders, percentage of shares, addresses, nationalities, and other information relevant to determination and calculation of zakat and tax. The shareholders' information is verified by cross-checking MOCI data in case of companies being the shareholders and by cross-checking Ministry of Interior data (ABSHAR System) in case of individuals being the shareholders. The Saudi authorities informed that GAZT, MOCI, Ministry of Labour and the General Organisation for Social Insurance are working to have a common

portal where information on companies and shareholders will be jointly maintained and shared.

445. In sum, there are many measures in place that help to mitigate the risk of misuse. There is potential to make better use and cross-matching of the information available to the authorities to prevent misuses of legal entities and arrangements, including by identifying potential strawmen, and by making readily available to or share with all relevant stakeholders the information on beneficial ownership which should be submitted by JSCs.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons created in the country

446. Timely access to basic information is ensured for all competent authorities, particularly through the Company Register database. Access to accurate and current beneficial ownership information may be available through the Company Register in case the legal ownership information coincides with the beneficial ownership information or through FIs and DNFBPs.

447. Access to basic ownership of legal entities is generally easy for competent authorities, particularly given the large number of information that can be accessed through the Company Register database. The information available in the Company Register up to November 2017 was updated basic and legal ownership information on Limited Liability Companies and Unlimited Liability Companies. There are mechanisms to ensure that this information is accurate and current (described above).

448. The competent authorities indicated relying on the Company Register database for legal ownership and other basic information about commercial legal entities. There was indication from the authorities that basic and beneficial ownership information would be sought directly from the commercial legal entities, in particular for Joint-Stock Companies and Limited Partnerships which until November 2017 were not required to provide shareholder information to MOCI.

449. The competent authorities normally access beneficial ownership information through the Company Register database by following the chain of ownership. In practice, Saudi Arabia indicated that SAFIU received 100 STRs regarding legal entities between 2016 and 2017. In 85 of those cases, SAFIU was able to identify the beneficial owner through the Company Register as the shareholders were all Saudi natural or legal persons. In 14 of the 15 remaining cases, SAFIU obtained beneficial ownership information on the foreign owners from SAGIA, and in one case could not identify the beneficial owner. This is possible and effective where the full ownership chain is made of Saudi persons only, and assuming that there are no informal nominees (strawmen). In case there is a foreign person in the ownership chain (which accounts for about 3% of the legal entities), the information included in the CR database (obtained by SAGIA through the Saudi embassies) does not include beneficial ownership. As indicated above, SAGIA obtains ownership and control structure information before granting a business licence to a foreign company, although it does not necessarily receive updates of it.

450. Where the information available with MOCI is not sufficient, which according to the Saudi authorities is rare, the competent authorities rely on reporting entities to

obtain beneficial ownership information (particularly for Limited Partnerships and Joint-Stock Companies until November 2017, when a new provision obliged these types of entities to report legal and beneficial ownership information to MOCI). Initial beneficial ownership information is generally available with the Saudi bank with which the legal entity has the bank account. The relevant bank holding beneficial ownership information may be identified through a request by SAMA. There is however no obligation on Saudi companies to maintain a bank account in Saudi Arabia. Banks conduct a due diligence exercise, which starts by verifying the information on the companies maintained by the CR.

451. Updated information on the beneficial ownership is more problematic because the banks may not always be aware of the change in (legal and beneficial) ownership. Even though banks constantly monitor transactions in accounts, BO and CDD information is updated on a risk-based basis depending on the type of client, and they verify this by checking the CR. In two cases presented to the assessment team, however, the BO and CDD information available to the bank did not match the updated information available with MOCI. This shows that MOCI was able to obtain updated ownership information, but also that the FIs did not update their files in due time.

452. Ensuring the accuracy of BO information is possible for FIs and DNFBPs also when there is a foreign element in the chain of ownership and control. This is because verification of the foreign person is made through the information provided to SAGIA.

453. With regard to Associations and Foundations, all basic information is available with the Ministry. NPOs are treated as high risk customers, and banks continuously monitor the accounts and ensure that all information, including ownership information is up-to-date. Such information maintained by banks/FIs and Courts are available to the competent authorities.

454. The extent to which the various competent authorities pursue basic and beneficial ownership information is unclear. The Saudi authorities indicated that the FIU, directly or through SAMA, would request the CDD files on the suspect. The competent authorities have not presented cases where they followed-up ownership in complex structures involving entities located inside or outside Saudi Arabia. The Saudi authorities indicated there are few such complex ownership structures.

455. In sum, the authorities are generally able to access reliable basic and beneficial information from the Company Register in relation to Unlimited Liability Companies and Limited-Liability Companies, provided that no informal nominees would act as strawmen directors and shareholders. Information on foreign persons investing in Saudi Arabia would be accessible via SAGIA. Access to beneficial ownership of Limited Partnerships and Joint-stock companies until November 2017 could be done through reporting entities in case the company had a business relationship with them (and with the limitations highlighted in IO.4). Information on businesses which do not need to register like Unlimited (silent) Partnerships and Islamic Partnerships may not be available. The authorities did not demonstrate that they would chase cases of complex ownership structure.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal arrangements

456. Waqfs are registered with Courts and these are regulated and supervised by The General Waqf Authority. Court documents provide the details of endower (settler), beholder (trustee) and beneficiaries. As noted under R.25, these details do not go as far as having available beneficial ownership information on the waqf. These documents are to be maintained indefinitely. This information is available to all competent authorities through the electronic files saved on the MOJ website, which disclose the waqfs deed. The Saudi authorities indicated a case where indictments were brought against a waqf. The indictments were brought as a result of illegal transactions carried out by the management of the Waqf. At that time, the Waqf was not registered and the monitoring system of the money coming in or going out was not sufficiently maintained. In addition, the management (Waqif) did not respond or co-operate with the ongoing investigations. Moreover, there were a couple of lawsuits in foreign jurisdiction brought by the family of the victims whom were harmed as result of illegal transactions conducted by the management of the Waqf. The case was first initiated by financial intelligence communities and the outcome of the case resulted in prosecuting the beholders, terminating the waqf and transferring all its assets to a separate waqf.

457. In respect of those business which are not required to be registered with MOCI (i.e. Unlimited Partnerships and Islamic partnerships), ownership details may not be readily available.

Effectiveness, proportionality and dissuasiveness of sanctions

458. MOCI applies sanctions when it identifies irregularities during its verification. An application to the Company Register is rejected when it is not correct (there were 68 applications rejected in 2017). A Committee within MOCI was established in 2016 to deal with violations of the Company Law. Since 2016, the MOCI Committee studied 105 cases of misconduct and issued 46 sanctions. Since 2015, SAGIA cancelled the licences of 92 foreign companies (29 in 2015, 39 in 2016, and 34 in 2017) for different reasons, including a failure to provide accurate information and the lack of submission of financial statements. A new provision from November 2017 requires Joint-Stock Companies, Limited Partnerships and Limited Liability Companies to provide and maintain updated beneficial ownership information. The implementation and enforcement of this provision in practice will be seen in future assessments.

459. In respect of foreign companies and foreign owners, SAGIA has taken action in 45 cases which include monetary sanction, limitation or suspension of certain benefits granted to foreign investors and in some cases, cancellation of licences for providing inaccurate information. This appears to be adequate.

460. In relation to CDD and BO information, conducted by FIs and DNFBPs, bank supervisors' findings show that banks usually stop their inquiries having identified legal and beneficial ownership information, but do not ensure that this information is kept accurate and up-to-date. There have been sanctions for violations of CDD measures, which the Saudi authorities indicate included deficiencies in respect of beneficial ownership information (although this is not made clear, as described in Immediate Outcome 3).

461. In relation to waqfs, the Saudi authorities indicate that there was not case of misuse for ML. There are some cases of violations of the deed by the trustee (waqif), in which case the settlor complained with the competent judge who can remove the waqif or order a correction. Saudi Arabia has taken enforcement measures related to waqfs in respect of 39 cases in 2015, 50 cases in 2016, and 69 cases in 2017.

462. In relation to sanctions on Foundations and Associations, see Immediate Outcome 10.

463. In sum, the relevant authorities have applied effective, proportionate and dissuasive sanctions to persons involved in the registration process of legal entities and arrangements, particularly in recent years. It is not clear that supervisors apply sanctions in relation to violations of their obligations to obtaining and updating beneficial ownership information of legal entities and arrangements.

Overall conclusions on IO.5

464. Saudi Arabia has a system for regulating and monitoring legal persons and arrangements which is helpful in maintaining transparency and also in identifying beneficial owners. The Company Register maintained by MOCI provides the updated and accurate details of ownership of commercial entities. Designated Courts have such records in respect of Waqfs and conduct verification. NPOs are strictly regulated and they are not allowed to send or receive funds from abroad. The understanding of authorities of the risks of misuse of legal entities and arrangements does not yet seem to be sufficiently well-developed. Further, it is also not clear whether current and reliable BO information is available and accessible to competent authorities in respect of Limited Partnerships and Joint-stock Companies (until November 2017), and in respect of persons acting as strawmen directors and shareholders. It is not clear that effective, proportionate, and dissuasive sanctions have been applied by supervisors.

465. **Saudi Arabia is rated as having a Moderate level of effectiveness for IO.5.**

7

CHAPTER 8. INTERNATIONAL CO-OPERATION

Key Findings and Recommended Actions

Key Findings

- Saudi Arabia can and does respond to incoming requests for mutual legal assistance, but there appear to be delays in some cases. The outcome of international co-operation provided to other countries was not clear, in terms of investigations carried out on behalf of other countries and / or assets confiscated and repatriated.
- Saudi Arabia does not effectively seek international co-operation. The number of outgoing requests remains relatively low despite a recent significant increase. As a result, Saudi Arabia does not pursue opportunities to investigate and disrupt transnational criminal networks involved in corruption, supply of narcotics and in money laundering, or to confiscate the proceeds of crime.
- Some authorities favour direct or informal co-operation over formal MLA, with some success in combating predicate crimes, but the results achieved are uneven, particularly for ML and criminal proceeds.
- On terrorist financing Mabaheth prioritises international co-operation and relies primarily on intelligence co-operation. Case examples provided by Mabaheth illustrate that it has an effective approach to disrupt the threat of terrorist networks. Saudi Arabia also makes significant contributions through its leading role in global and regional alliances against terrorism and its financing.

Recommended Actions

- Saudi Arabia should review its mechanisms for receiving and co-ordinating international co-operation requests, to make sure that requests are actioned quickly and appropriately further improve the case management system used by the PCMLA to prioritise and track responses by domestic authorities to incoming MLA requests.
- Saudi Arabia should continue the recent upward trend of seeking MLA and should seek to more frequently utilize MLA and other forms of international co-operation to enhance the approach of its law enforcement and prosecution authorities so that their investigations prioritise following the money and disrupting criminal networks and facilitators inside and outside Saudi Arabia's borders.
- Saudi Arabia should consider establishing a specialised unit to recover the proceeds of crime from other jurisdictions.

- Authorities should take a strategic approach to bilateral agreements, using the NRA to focus on the most significant destination countries for proceeds of crime.
- While Mabaheth, Customs and occasionally other LEAs carry out direct and informal co-operation effectively, it is recommended that they complement their work by seeking extradition of criminals and recovery of assets.
- Authorities should consider expanding the remit of the *General Directorate of Narcotics Control* (GDNC) liaison offices to include co-operation against ML, TF, and proceeds of crime.

466. The relevant Immediate Outcome considered and assessed in this chapter is IO.2. The Recommendations relevant for the assessment of effectiveness under this section are R.36-40.

8

Immediate Outcome 2 (International Co-operation)

Providing constructive and timely MLA and extradition

467. International co-operation is important in the Kingdom of Saudi Arabian context given its economic, social and geographical features, as well as the ML and TF risks the country faces. The Kingdom of Saudi Arabia has a legal and institutional framework in place to provide MLA and extradition across a range of international co-operation requests. Information is exchanged in accordance with agreements, conventions or memoranda of understanding in place, or according to the principle of reciprocity (Basic Law of Governance (article 42), the AML Law (AMLL) and the Law of Terrorism Crimes and Financing (LTCF).

468. The central authority responsible for international co-operation and mutual legal assistance in Saudi Arabia is the Permanent Committee for Legal Assistance Requests (PCLAR) at the Ministry of Interior. It is presided over by the MOI undersecretary and is formed by representatives from 10 governmental authorities. The PCLAR receives requests addressed to the Kingdom by other States through the Ministry of Foreign Affairs by means of official diplomatic channels. The Committee's secretariat holds meetings on a weekly basis or whenever the need arises. Upon receiving a request, it is reviewed by an advisor of the Committee's secretariat. Responses are proposed, and the request is considered by the Committee for further action as necessary. It is not clear however whether the PCLAR has in place procedures that ensure the confidentiality of the process.

469. The Committee may directly accept requests for legal assistance from other States through written communication, including fax or e-mail, in accordance with paragraph (1) of Article 15 of the Manual on Legal Assistance and Asset Recovery Procedures. States may also consult with the Kingdom on how to submit a request for legal assistance and send a preliminary draft of that request to ensure that it meets the requirements of legal assistance in the Kingdom in order to facilitate the implementation of the request as soon as possible. The manual for legal assistance and asset recovery requests has been posted on the UNODC web site, with its address and means of communication. The Commission has already received direct access from countries such as the United States of America and China.

470. The Committee is currently discussing with a number of countries the conclusion of a legal assistance agreement. The draft agreement was sent to more than (24) countries in which several criteria were considered, including a) the number of applications issued or received by the Kingdom; b) Number of the nationality of that country in the Kingdom; c)/ neighbouring countries; d) Countries that require the Kingdom's interests to co-operate with them in the future.

471. In 2013 (later updated in 2017), guidelines on legal assistance procedures and redemption of assets were issued in order to clarify the legal framework of legal assistance, the competent central authority, the scope of legal assistance, the information to be provided in the legal assistance request, and the way of execution of the requests, etc. There is a prioritization mechanism for the PCLAR which is based on its internal procedures. After being examined by the committee – priority is given to serious crimes (terrorism, TF etc.) and any requests relating to the seizure of assets.

472. Saudi Arabia received 93 incoming MLA requests during 2016 and 96 in 2017[26], 2017 figures updated as set out in Table 1. A breakdown of these requests according to the type of crime is set out in Table 2. Requests were received from 31 different countries, with the largest numbers of requests coming from Turkey (35% of the total); Egypt (4%), UAE (4%), India, Pakistan, and Lebanon (3.5% each).

Table 33. Incoming MLA requests 2013-2017

Year	2013	2014	2015	2016	2017
Incoming requests	40	58	64	93	96

Table 34. Incoming and outgoing requests by case type 2016-2017

Case Type	2016		2017	
	Incoming	Outgoing	Incoming	Outgoing
Fraud	17	5	22	10
Cursing and insulting	11	2	16	8
Forgery	9	0	11	5
Customs evasion	4	0	2	1
Murder	3	0	2	0
Drugs	9	1	5	12
Notification of Judicial judgement	7	0	3	3
Terrorism financing	2	0	1	0
Terrorism activities	3	1	1	1
Sexual Assault	2	0	1	0
Money laundering	3	2	8	16
Blackmailing	3	2	1	4
Corruption			5	13
Bribery			3	9
Magic and sorcery	1	0	0	0

26 According to the - information received on 21-11-2017,

Case Type	2016		2017	
	Incoming	Outgoing	Incoming	Outgoing
Assets recovery	2	3	5	15
Robbery	2	3	5	4
Notification to attend court	2	1	0	0
Tax evasion	1	0	0	0
Other	12	3	5	0
Total	**93**	**23**	**96**	**101**

Table 35. Type of co-operation requested in the above cases - 2016-17

Type of co-operation sought	Cases
Taking Statements	45
Hearing testimony	11
Requesting information	37
Provisional seizure and recovery	3
Interrogation	26
Tracking Money	3
Requesting copy of judgements	14
Requesting Investigation	7
Requesting copy of investigation files	9
Other	14

473. In the last two years Saudi Arabia has received close to 100 MLA requests per year, involving a range of different criminal offenses, most notably fraud, insulting and cursing, drugs and forgery. Saudi authorities provided information on the time needed and actions taken to provide responses to a sample of incoming MLA requests in 2017 and 2016. Authorities generally respond quickly to requests (average response time is 2-3 months or more) and in most cases the requested information was provided following investigation and co-operation with national Authorities.

474. Feedback provided to FATF and MENAFATF by other countries on international co-operation by Saudi Arabia suggests that Saudi Arabia is, in general, responsive to MLA requests received. Some of the 17 countries that responded provided good feedback on the responses Saudi Arabian authorities provided. One country experienced delays up to 15 months for receiving information on a MLA request, and three MLA requests have been deemed to be refused by the Saudi Arabian authorities as no response was given at all. Another country stated that it received an answer after 8 months, with useful information. In one case, a country reported that the Saudi authorities refused a request because the subjects of the request were Saudi Nationals. In this case, a judge was sent to Saudi Arabia to try to resolve the pending case. In other cases, MLA requests were not executed as they did not follow the required legal formalities, but Saudi authorities provided assistance to the requesting country. .

Box 23. MLA by Saudi Arabia in response to a foreign request

French authorities submitted a legal assistance request (letter rogatory) on19/12/1437 AH (22/9/2016) , asking for French investigators to participate in the interrogation of a Saudi citizen, Y, who was accused of money laundering, bribery, influence peddling, misappropriation of corporate funds, and conspiracy.

A former French official, Mr. N, had received a payment of EUR 500 000 from Malaysia, ostensibly the proceeds of the sale of paintings, and intended to purchase an apartment with the funds. However, the paintings were found to be valued at only EUR 30 000. A false invoice for EUR 500 000 had been issued by a lawyer in Malaysia, and on investigation, the law firm was found to have received a EUR 500 000 payment from an account in Saudi Arabia two days before making the transfer to France. The Saudi account was controlled by a French resident, Mr. K. At this point in the investigation, French authorities sought assistance from Saudi Arabia.

On 17/2/1438 AH (18/11/2016), the PP approved the participation of French investigators. On November 22, suspects in Saudi Arabia were interrogated in the presence of the French investigators. No conclusions were reached at this point and the investigation remains ongoing.

475. For extradition requests, the authority responsible is the Public Prosecution (PP) regarding the cases of money laundering and associated predicate offences, and the Saudi liaison with Interpol, which acts as the primary communication channel. The PP receives incoming requests through Interpol, while the outgoing requests are received by the Bureau through the competent authorities in the Kingdom (principally the GSD/Police).

476. Between 2014 and 2017, the Saudi authorities received 228 extradition requests, of which 197 were completed, 31 were declined and 8 were declined and were otherwise charged. Cases submitted suggest that extradition can take up to 3 years to finalize as per some of the examples mentioned by the Saudi Arabian authorities

Box 24. Extradition of a non-citizen

In March 2017 a request was received to interview a UAE Citizen in connexion with fraud and money laundering charges in UAE. The accused was interviewed by prosecutors, and denied the charges, but agreed to be extradited to UAE authorities. An extradition request was then made and approved, and the extradition carried out within the following two weeks.

477. Saudi Arabia does not extradite its citizens and the authorities mentioned that they are able to prosecute their nationals instead once they confirm the charges against them. The Saudi Arabian authorities mentioned that they would extradite resident non-citizens when their crime is proven. The relevant charge should be referred to the PP and referred to the competent court. The person would then be prosecuted. Saudi authorities provided details of 31 cases in which extradition was

refused during 2013-18. In 28 of these cases extradition was refused because the person sought was a Saudi citizen. In seven of these cases, the individual was charged with offences in Saudi Arabia. An example of such a case is set out in Box 25 below. In some cases extradition of non-Saudi citizens has also been refused, for reasons of lack of reciprocity; and the existence of financial obligations on the accused in Saudi Arabia with government agencies, legal persons and individuals.

Box 25. Prosecution in Saudi Arabia for a foreign crime

On the date of 28/10/1437 AH (2 August 2016), a Saudi citizen visiting Kuwait assaulted and robbed a Kuwaiti citizen of KD41 (EUR110), and subsequently returned to Saudi Arabia. Based on co-operation between the Kuwaiti and Saudi authorities, the Saudi citizen was arrested in Saudi Arabia, tried, and was sentenced to seven months' imprisonment. A representative from Kuwait attended the court hearings.

478. Saudi Arabia received three incoming requests to trace, identify confiscate, or repatriate the proceeds of crimes committed in another country. In one case a request led to the identification and provisional attachment of assets in Saudi Arabia belonging to a foreign company manager, however these were not ultimately confiscated and repatriated since no judgement was reached in the requesting country.

Seeking timely legal assistance to pursue domestic ML, associated predicates and TF cases with transnational elements

479. Saudi Arabia has a legal and institutional framework which would enable it to seek legal assistance to pursue domestic cases with a trans-national dimension. The Permanent Committee for Legal Assistance Requests at the Ministry of Interior's mandate extends to both the incoming and outgoing requests. There is a process for sending requests to other countries; the committee receives the requests from the competent authorities in the Kingdom, analyses their content and sends them to the Ministry of Foreign Affairs for onward transmission through official diplomatic channels.

480. The Committee has taken several measures to improve the use of mutual legal assistance, held workshops with the Public Prosecutor's Office (PP). A number of ECU branches have also visited to exchange, sharpen and elicit ideas on this matter in the end of 2016. The manual was distributed in relation to the implementation of the law and work is in the process of arranging workshops for legal assistance with the concerned authorities during the year 2018.

Table 36. Outgoing MLA requests 2013-2017

Year	2013	2014	2015	2016	2017
Outgoing requests	15	23	25	23	101

Table 37. Outgoing requests by case type 2016-2017

Case Type	2016	2017
Fraud	5	10
Cursing and insulting	2	8
Forgery	0	5
Customs evasion	0	1
Murder	0	0
Drugs	1	12
Notification of Judicial judgement	0	3
Terrorism financing	0	0
Terrorism activities	1	1
Sexual Assault	0	0
Money laundering	2	16
Blackmailing	2	4
Corruption	0	13
Bribery	0	9
Magic and sorcery	0	0
Asset recovery	3	15
Robbery	3	4
Notification to attend a Judicial session	1	0
Tax evasion	0	0
Other	3	0
Total	**23**	**101**

Table 38. Type of co-operation requested by Saudi Arabia in the above cases - 2016-17

Type of co-operation sought	Cases
Taking Statements	28
Requesting information	33
Provisional seizure and recovery	19
Interrogation	15
Tracking Money	10
Requesting judgements	7
Requesting Investigation	3
Other	9

481. The number of outgoing requests made by Saudi Arabia is very low compared to the outgoing proceeds abroad. The number of outgoing MLA requests increased significantly in 2017 to 101 requests, compared to 23 in 2016 and a similar number in previous years. This increase followed the circulation of the *Legal Aid and Asset Recovery Procedures Manual,* and a number of workshops aimed at increasing awareness among prosecutors and law enforcement agencies. Tables 37 and 38 above list the predicate offences and the types of co-operation sought. Nevertheless, the number of requests remains low, and the crimes leading to requests do not correspond with the types of proceeds-generating crimes committed in Saudi Arabia, in particular those with a cross-border dimension. Some particular concerns are:

- *Narcotics trafficking*: this is the most significant proceeds-generating crime in Saudi Arabia, accounting for 31% of proceeds, and 4,097 criminal investigations in 2016.

However, there was only one outgoing MLA request relating to narcotics in 2016, and only 12 in 2017. Corruption is the second most significant source of proceeds, few number of MLAs was requested from foreign counterparts, mostly executed during late 2017;

- *Counterfeiting and piracy of products:* this is the third largest source of proceeds in Saudi Arabia, with 1,036 convictions in 2016, but leading to only 5 MLA requests;
- *Proceeds of Crime:* Saudi Arabia's NRA estimates that 70-80% of proceeds of crimes in Saudi Arabia are sent out of the country, implying a total of between SAR 8 billion and 40 billion leaves Saudi Arabia each year. Saudi Arabia made 15 outgoing requests for co-operation on asset recovery in 2017 and only three in 2016, and only 25 cases requested assistance with tracking money or provisional seizure of assets.
- *Money Laundering:* No outgoing MLA requests were sent relating to money laundering offences during 2015. Two requests for MLA relating to money laundering were sent during 2016, and 16 were made in 2017 (although some requests may relate to foreign ML activity but were classified according to the predicate offense committed in Saudi Arabia).

482. There is also an inconsistency between the countries to which MLA requests are addressed, and the countries which are identified in the NRA as the main destination countries to which the proceeds of crime are sent. The main destinations of outgoing MLA requests as indicated in the statistics from Saudi Arabia in 2016 and 2017 do not include any of the countries identified as the top three destinations for proceeds of crimes committed in the Kingdom. In one case this is because the country concerned is undergoing conflict. In other cases the reasons for the inconsistency are unclear. Although a perfect match is not expected, this mismatch does indicate that pursuing the proceeds of crime is not a high priority for Saudi's outgoing international co-operation requests.

483. Countering Terrorism and Terrorism Financing offenses are defined as high risk in Saudi Arabia, however, MLA outgoing requests for terrorism were only 2 during 2016. To a large extent this is because the Saudi authorities make use of other channels for international co-operation to deal with terrorism cases, in particular direct law enforcement co-operation or intelligence co-operation. While direct co-operation can be utilised as an effective tool in criminal matters, the use of MLA in relation to terrorist financing remains weak even when this is considered. The PCLAR acknowledged the fact that the number is low and that would be reviewed with a view to further increasing it.

484. The Saudi authorities mentioned that they undertook measures to improve the use of MLA; workshops with the PP were conducted, PCLAR visited a number of branches working in the ECU in order to brainstorm on this issue at the end of 2016 and a manual on legal procedures was distributed to law enforcement.

485. Outgoing extradition requests are made primarily through Interpol: In the case of persons, residing abroad, and wanted by the authorities of the Kingdom of Saudi Arabia, the Public Prosecution issues an indictment and an arrest warrant and request the extradition. These are filed with INTERPOL for international dissemination and inclusion in the red bulletin. When this person is arrested, the Public Prosecutor's Office pursues extradition proceedings. In the period 2014 - 2017,

Saudi Arabia made 212 outgoing requests for extradition. The persons sought were extradited to Saudi Arabia on 37 occasions.

Seeking other forms of international co-operation for AML/CFT purposes

486. The Kingdom of Saudi Arabia can use a wide range of other forms of international co-operation with its foreign counterparts in order to exchange various types of information including financial and law enforcement information for AML/CFT purposes. For crimes related to customs evasion, terrorism and terrorism financing, Mabaheth and the General Directorate of Customs showed a strong international co-operation especially with neighbouring countries.

487. The *General Directorate for Narcotics Control* (GDNC) regularly co-operates with counterparts from neighbouring countries, most notably Jordan, Egypt, which resulted in intercepting smuggled drugs from 2014-2016. The Directorate has co-operated with a number of peer authorities in neighbouring countries through conducting controlled deliveries, to tackle smuggling operations at destination countries and to identify smuggling methods. The Directorate has also opened 25 representative offices with liaison officers in relevant countries to speed up co-ordination and communication with their anti-drug and security centres. Saudi Arabia provided successful case examples of liaison leading to controlled delivery of captagon tablets; and raids on drug factories in other countries. While these show significant successes in upstream disruption of drug suppliers, they are focused on the physical supply of drugs, and do not attempt to target financial networks or criminal proceeds.

488. On countering the financing of terrorism, Mabaheth co-operates with about 83 countries. Data is received by the Ministry of Interior in the past and currently by the Security State Presidency (Mabaheth, PCCT and SAFIU) through several diplomatic and intelligence/security channels, or through states' liaison officers, bilateral visits or meetings. The information is often intelligence or secret financial intelligence intended mainly to stop a terrorist operation, the financing of terrorism, co-ordinate the classification or take a precautionary measure to prevent terrorist financing, activities by individuals or entities in accordance with Resolution 1373, joint action to classify names according to resolution 1267, information on individuals or entities and suspicions of terrorist activities or terrorist financing activities and information on foreign terrorist fighters. There are 21 offices abroad. Most co-operation is in relation to FTFs and returnees. The Saudi authorities provided information on cases of informal co-operation with counterparts in countries near conflict zones where would-be terrorist fighters were returned to Saudi Arabia. Assessors were provided with cases whereby there was effective police-to-police co-operation in returning and prosecuting a Saudi national who was suspected to travel to the conflict zone. Table 39 below provides the number of information exchanges between Mabaheth and foreign counterparts in recent years (not broken down by the nature of the offence or by cases).

Table 39. International Information Exchanges between Mabaheth and foreign counterparts

	Year	2013	2014	2015	2016
Number of Requests	**Incoming**	9,609	12,061	13,413	13,631
	Outgoing	17,637	17,030	19,842	20,782

Box 26. **Co-operation on terrorist financing**

After a bombing, Mabaheth collaborated with a foreign country (Kuwait) to identify the responsible and the facilitators. Three people were arrested in Kuwait, including a Saudi national who was extradited to Saudi Arabia. During interrogation, the Saudi national confessed that a vest was delivered to Kuwait in his brother's car; however, the owner was not aware of the purpose of the trip. The Saudi national confessed he paid SAR 10 000 to provide medical care to one of his brothers who was fighting in Iraq with ISIS. It is not known to whom the money was paid to as the cash was left in a bag to pick up. The Saudi national was convicted to 4 years in jail, 3 of which for attempting to travel to conflict zone, and 1 for paying SAR 10 000 for the purpose of supporting a foreign fighter.

489. The Saudi Arabia Financial Intelligence (SAFIU) joined the Egmont Group of FIUs in 2009 and conducts exchange of information through the secure website of the Egmont. By end of the first quarter 2017, SAFIU had concluded 28 bilateral memoranda of understanding with FIUs including India, Turkey, Bangladesh and Indonesia.

490. FIU co-operation can be conducted via direct contact between a SAFIU liaison officer and the liaison officer in another State. During 2016, there were 84 exchange of information requests on ML and TF by the liaison officer, and 98 exchange of information requests in 2017. Criteria for seeking to sign MOUs include the size of funds exchanged, the size of transactions, the numbers of cases or joint cases, the legal foundations of the other country, having a large number of foreign workers in Saudi Arabia, etc. However, Saudi Arabia has yet to sign MOUs with a number of key partners (both upstream and downstream of the Kingdom). Information requests are categorized by time whereby a request categorized as "immediate" would take around 2 business days to be answered and a regular case can take up to 60 working days (around three months in total) for financial analysis and investigations.

491. The Saudi FIU has access to a number of databases which should enable it to provide interim answers to the requests they receive in a relatively short time. Saudi Arabia authorities mentioned that the time period required to reply to any request depends on the quality of the information requested; if such information is related to the database of SAFIU and other databases directly accessed, the reply is sent within the minimal time period; if the request is related to financial information that requires co-ordination with the competent authority, the matter may take the maximum time period or exceed it in some cases. The SAFIU indicated that the main 10 countries they exchange information with: US, Bahrain, UAE, Lebanon, Jordan, Egypt, Kuwait, India, Philippines, and Bangladesh. These are largely consistent with the NRA analysis of the countries which are the main sources / destinations for

criminal proceeds. Regarding requests about TF, these are usually carried on by the relevant investigative authorities (i.e. Mabaheth).

492. International co-operation feedback suggests that some FIUs commended the information received from SAFIU, and most requests receive a response within 2-7 days, however, some countries have experienced delays up to 3 months for receiving answers from the SAFIU. The requests, as per the international co-operation partner contained not only information directly available to the FIU but also other kind of non-financial information (e.g. travel records of the requested subject).

Table 40. FIU incoming and outgoing exchange of information on ML and TF

2015	FT	ML	Total
International Outgoing	17	45	62
International incoming	362	169	531
2016	**FT**	**ML**	**Total**
International Outgoing	6	38	44
International incoming	110	135	245
2017	**FT**	**ML**	**Total**
International Outgoing	21	113	134
International incoming	61	59	120

493. As shown in Table 40 above, the number of outgoing international co-operation requests in the SAFIU has risen significantly in 2017 compared to 2016 and 2015. SAFIU sent 8 spontaneous disclosures to other FIUs.

494. *The Ministry of Interior:* 16 security agreements were concluded by the MOI in the last three years.

495. *The Saudi Arabia Monetary Agency (SAMA):* SAMA co-operates and exchanges information with counterpart authorities directly, by virtue of agreements and memoranda of understanding signed by the Kingdom or based on the principle of reciprocity. SAMA also receives many requests through the Permanent Committee for Legal Assistance Requests, as such requests are received by the competent department comprising the member of the Permanent Committee for Legal Assistance Requests - delegate of SAMA.

496. SAMA and CMA seek co-operation from home supervisors when considering requests from foreign FIs to begin operations in Saudi Arabia. They also seek due diligence reports from foreign supervisors when considering authorisation for appointments of senior management personnel who were previously employed in foreign jurisdictions. AML/CFT related co-operation takes place alongside co-operation on other aspects of prudential and conduct of business supervision, including co-operation with home supervisors through supervisory colleges to co-ordinate on the supervision of Saudi branches and subsidiaries.

497. *The Ministry of Justice:* the Ministry of Justice co-operates with the counterpart authorities in other states through bilateral agreements, whereas the Ministry has signed 10 bilateral agreements, memoranda of understanding, and executive programs, along with 9 multi-lateral agreements. The Ministry also signed 27 agreements and reference guides at the level of GCC countries. Furthermore, the

Ministry co-operates with the counterpart authorities as per a number of agreements. The content of such agreements covers judicial co-operation in civil, commercial and personal matters (including AML/CFT), including the exchange of judicial papers, communications, judicial assignments and the enforcement of foreign judgments in those matters

498. *The Ministry of Commerce and Investment (MOCI)*: the Ministry has signed an agreement with a number of countries. Examples reveal that there is direct co-operation with counterpart authorities through a number of incoming and outgoing inquiries, like the identification of the beneficial owner. The Ministry signed MOUs recently with Egypt, France, China, Malaysia, Turkmenistan, Japan and others.

499. *Customs:* The General Directorate of Customs frequently co-operates internationally and exchanges information, especially with States having common border with Saudi Arabia, including the GCC. The General Customs Authority has signed four bilateral agreements with each of the UAE, Qatar, Yemen, and Jordan, in addition to the Gulf agreement on the unified customs regulation. Furthermore, the General Customs Authority provided contact points with Arab and Gulf States, and communication is made directly through several means, including e-mail.

500. The General Directorate of Customs also exchanges information through the Regional Intelligence Liaison Office in the Middle East (RILO) established in the Riyadh in Saudi Arabia and related to the World Customs Organization, knowing that the office aims to facilitate the process of collecting, co-ordinating, analysing, and disseminating information among the States in the region. In 2014, this Bureau received about 60 reports, the most prominent of which had to do with Ivory from Elephant tusks where 187 pieces were intercepted in the country while in transit to/from Africa. Many of the requests relate to drugs "cocaine, heroin, narcotic pills", adulterated substances, cigarettes and other generic substances. In 2015, the Office received about 224 reports, most request related to narcotic substances, attempted smuggling and the remainder of its products related to counterfeited materials, cigarettes and other antidotes. In 2016, the Office received 384 reports most requests related to narcotic substances, counterfeit cigarettes and alcoholic beverages. Customs provided some cases where they intercepted captagon from neighbouring countries such as the UAE, Jordan, Qatar, Bahrain and Lebanon. Also, they were involved in a big operation with the US counterpart. The authorities mentioned that Customs and Mabaheth exchange information with counterparts relevant to Proliferation Financing.

Box 27. Customs co-operation with parallel financial investigation

The Middle East Regional Office for Information Exchange (RIE) received a report from the local Customs office of the Kingdom of Bahrain in mid-2014 stating that there were two consignments of captagon sent by air through DHL from Turkey transit via Haryn and its final destination was Riyadh. These two consignments are lighting tools (Chandeliers), containing an unknown quantity of Captagon tablets. Authorities were asked to pass the information to the Saudi Customs to intercept the shipment.

The two shipments were examined upon arrival at King Khalid International Airport in Riyadh, and found to contain 51 743 captagon tablets. Saudi Customs co-ordinated with the General Directorate of Drug Control to monitor the delivery of the consignments in order to catch its actual recipient. The Directorate monitored the shipments and caught its recipient and referred him to the competent court which sentenced him to two- year prison term and banned him from travel outside the Kingdom for a similar period of imprisonment and fined him with an amount of SAR 40 000.

Customs opened a parallel financial investigation during the investigation of the predicate crime. Information was collected from the FIU and the Public Prosecution, as well as Customs. However, the investigation did not identify evidence of money laundering, and the criminals were charged only with the predicate offence.

501. *The Capital Market Authority (CMA):* the CMA is a signatory of the International Organization of Securities Commissions (IOSCO) Multilateral Memorandum of Understanding Concerning Consultation and Co-operation and the Exchange of Information (MMOU). As a result, the CMA has answered requests received from members of the IOSCO in relation to Fit and Proper assistance (asking about registered employees background), and in relation to authorized persons asking for matters related to capital adequacy, unresolved complaints, systems and controls in place.

502. *The National Anti-Corruption Commission*: the commission co-operates at the international level with counterparties and international organizations as per with its mandate set forth in the Council of Ministers Resolution No. 165 dated on 28/5/1432 H concerning the organization of the Commission. Although the Commission receives reports on corruption, it does not seem that it can or has exchanged operational data.

International exchange of basic and beneficial ownership information of legal persons and arrangements

503. The Saudi authorities consider that the most relevant information is already publicly available: foreign authorities have free and public access to all registry information via the Ministry of Commerce and Investment's homepage. Additional information can also be requested from and will be freely shared by the MOCI if and as required.

504. As set out in the analysis of IO.5, foreign companies seeking to invest in Saudi Arabia are screened by and have to get an approval from SAGIA before they may become shareholders of a Saudi legal entity. The screening process includes seeking and verifying beneficial ownership information through documentation provided by the applicant as well as from foreign authorities. SAGIA keeps such information and Saudi Arabia authorities mentioned that they may share this information with foreign authorities upon request either directly or through SAFIU but have not provided any information on previous cases. Saudi Arabia authorities stated that they made outgoing requests for information on the basic or beneficial ownership of foreign legal persons and arrangements which may be connected to criminal or terrorist activity in Saudi Arabia.

Overall conclusions on IO.2

505. Saudi Arabia can and does respond to incoming requests for mutual legal assistance, but there appear to be some delays in same cases. It can and does respond to extradition requests regarding non-citizens and has demonstrated that it conducts prosecutions of Saudi citizens who cannot be extradited. The Saudi Arabian authorities do appear responsive to incoming requests for information though these appear to suffer from some delays. While the overall number of outgoing mutual legal assistance requests has witnessed a pickup in 2017, the numbers do not seem solid in 2016 and 2015. Some authorities, though, use informal co-operation channels on a very regular basis, but the outcome of these channels in terms of investigation, prosecution and confiscation/repatriation of proceeds is not clear. Saudi Arabia has established a large number of bilateral arrangements to facilitate co-operation but do not cover the most significant countries.

506. The Customs Agency, Mabaheth and the General Directorate on Combating Drugs showed examples of co-operation with foreign counterparts to disrupt criminal activities, but this is limited to identifying targets in Saudi Arabia, not exposing their wider networks in other countries. Saudi authorities do not follow the money outside the borders of the kingdom, and as a result they do not exploit opportunities to investigate and disrupt transnational criminal networks involved in the supply of narcotics to a lesser extent, corruption and in money laundering.

507. These are not only problems with international co-operation; it reflects the wider weaknesses in the investigation of money laundering and confiscation of criminal proceeds.

508. On terrorist financing, Mabaheth (General Investigation Department) clearly does prioritise international co-operation, inbound and outbound, and provided good examples of international law enforcement co-operation with their counterparts (Police-to-Police), especially in the conflict zones (ISIL dominated areas). Mabaheth relies primarily on intelligence co-operation (rather than MLA) which is effectively used to identify and disrupt terrorist threats and intercept FTFs. The use of such mechanisms may mean missing the opportunity to use criminal justice tools and powers to uncover and disrupt further elements of terrorist networks, either in Saudi Arabia or overseas.

509. **Saudi Arabia is rated as having a moderate level of effectiveness for IO.2.**

8

TECHNICAL COMPLIANCE ANNEX

Recommendation 1 – Assessing risks & applying a risk-based approach

Criterion 1.1 – Saudi Arabia conducted separate national risk assessments for money laundering and terrorist financing for the first time in April 2017, using a modified version of the IMF's risk assessment methodology, and based on a wide variety of information from different sources. The assessments were formally endorsed by the AMLPC and PCCT in August 2017.

Criterion 1.2 - Saudi Arabia has designated specific bodies with responsibility for each NRA. The Anti-Money Laundering Permanent Committee (AMLPC) is the designated authority to co-ordinate the process of the national risk assessment of ML, and the Permanent Committee for Combating Terrorism (PCCT) is the designated authority to co-ordinate the TF national risk assessment. Each of these bodies includes the most relevant ministries and agencies as members. A co-ordination group was setup to ensure consistency between the two committees. (*AMLPC Internal Regulation, Art.2; LTCF, Art.84)*

Criterion 1.3 - The current NRAs are the first conducted by Saudi Arabia, and there has been no opportunity to update them. The mandates of the two committees include updating the risk assessments periodically. There is no regular schedule set out for updating the assessments. (*AMLPC Internal Regulation, Art.2; LTCF, Art.84)*

Criterion 1.4 - The NRAs are classified and have not been made public, but have been shared with competent authorities - through their participation in the AMLPC and PCCT, and through high-level meetings and workshops with relevant authorities. The conclusions of both assessments were shared with the private sector through a series of workshops and meetings with regulated entities.

Criterion 1.5 - Some Saudi authorities apply a risk-based approach when allocating resources or setting priorities at agency level. Saudi authorities have taken extensive steps in recent years to address vulnerabilities and reinforce the national AML/CFT system, including revisions to the AMLL and LTCF in November 2017 and the expansion and reorganisation of competent authorities, in order to implement international obligations, address technical deficiencies, and respond to risks. Significant risk mitigation measures were taken in some areas before completion of the NRAs, based on agency-level understanding of the risks, including controls on NPOs, remittances, and cash (as set out in section 2.2.2 of this report).

Criterion 1.6 **-** Saudi Arabia does not permit any exemptions from the FATF Recommendations on the basis of low risk.

Criterion 1.7 - The AMLL requires FIs and DNFBPs to take enhanced due diligence measures to manage and mitigate higher risks when these are identified in their risk assessments, or in situations set out by authorities. Authorities require enhanced

measures in situations set out in the FATF Recommendations (e.g. PEPs, cross-border correspondent banking relationships), but no specific measures to mitigate risks identified through the NRA process have yet been put in place *(AMLL, Art.7)*.

Criterion 1.8 –The AMLL and its Implementing Regulation allow simplified measures to be applied where lower risk has been identified and there is no suspicion of ML. Simplified measures should be proportionate to the risk. The LTCF does not refer to simplified measures. SAMA and CMA have issued Rules on the LTCF which do permit simplified measures to be applied by banks and APs, but no such provisions apply to DNFBPs. The law, regulations, and rules do not define the nature of simplified measures or the scenarios in which they could be applied. *(AMLLIR, Art5/5; SAMA CFT Rules, third.7)*.

Criterion 1.9 - The AMLL and CFTL require FIs and DNFBPs to apply mitigating measures proportionate to their risks, and give general powers to supervisors of FIs and DNFBPs to ensure that FIs and DNFBPs are implementing their obligations, including regarding the assessment of risks and the application of a risk-based approach. *(AMLL Art.24, CFTL Art.82)*

Criterion 1.10 - The AMLL and CFTL require FIs and DNFBPs to identify and assess their ML risks; (a) document their risk assessments; (b) take into account a wide range of risk factors including those relating to its customers, countries or geographic areas, products, services, transactions and delivery channels, (c) keep their risk assessment up to date; and (d) provide risk assessments to the supervisory authorities. *(AMLL Art.5; CFTL Art.63)*

Criterion 1.11 - The AMLL and CFTL require FIs and DNFBPs to: (a) have policies, controls, and procedures to mitigate the risks, approved by senior management *(AMLL Art.14)*; (b) to monitor the implementation of these controls and enhance them if necessary *(AMLLIR Art 5/4)*; and take enhanced measures to manage higher risks *(AMLL Arts. 7, 11, 13)*.

Criterion 1.12 - The AMLL only permits simplified measures if lower risks have been identified, and there is no suspicion of ML/TF (*AMLLIR, Art5/5)*.

Weighting and Conclusion

Saudi Arabia has recently established a strong risk assessment process and comprehensively updated the legal framework to include the requirements of R.1. However authorities have yet to issue implementing regulations to the LTCF, and have not yet updated the guidance and information available to regulated entities following the NRAs and new laws.

Recommendation 1 is rated largely compliant

Recommendation 2 – National co-operation and co-ordination

Criterion 2.1 - Saudi Arabia has recently adopted a national Strategy on AML/CFT, and an associated draft AML/CFT Action Plan. The Strategy is high-level and general, but the Action Plan sets out more detailed objectives, and includes specific actions, responsibilities, and deadlines. It is also used to monitor the status of implementation and obstacles to completion of each objective. The Action Plan addresses issues

identified in the NRAs, but it is more focused on strengthening Saudi Arabia's broader AML/CFT system, and some of the risks identified in the NRA have yet to be addressed.

Criterion 2.2 - Saudi Arabia has created two main national committees on AML/CFT:

- The Anti-Money Laundering Permanent Committee (AMLPC) is responsible for national AML policies. The AMLPC's mission explicitly includes co-ordinating with the relevant authorities, and suggesting policies and measures to combat money laundering*(AMLPC IR Art.2.2)*
- The Permanent Committee for Combating Terrorism (PCCT) is responsible for co-ordinating policies to combat terrorism, including terrorist financing. The PCCT has a ministerial level counterpart - the Supreme Committee on Countering Terrorism (SCCT), which has a mandate to submit proposals on measures to combat terrorism. The revised LTCF, adopted on 1 November 2017, expanded the PCCT's responsibilities to explicitly include co-ordination on terrorist financing *(LTCF, Art.84)*.

Criterion 2.3 - The AMLPC's membership includes the ministries and agencies relevant to AML activities, and it can co-ordinate with the other non-members as needed. The committee is responsible for reviewing international standards and proposing any legislative, regulation or circulars to be adopted by the competent authorities. The AMLPC has taken steps to support operational co-ordination, including developing an *ML Cases Procedures Manual* and a *Mutual Legal Assistance Procedures Manual* to co-ordinate the process between various agencies during the stages of ML investigations and MLA proceedings. Co-ordination also takes place directly between authorities, e.g. through regular meetings of the FIU and supervisory authorities. (*AMLPCIR*)

The PCCT is responsible for co-ordinating policies that combat terrorism and its financing. The PCCT includes most of the relevant ministries and agencies, though the FIU is not a member of the main Committee (it is included via its parent authority, the State Security Presidency, and participates directly in some subgroups). The PCCT is responsible for policy co-ordination and operational co-ordination (e.g. regarding TF designations under UNSCRs 1267 and 1373). There is regular co-ordination between the PCCT and AMLPC. A further Permanent Committee has been established to facilitate interagency co-ordination on MLA requests.

Criterion 2.4 - Co-ordination and co-operation mechanisms on the counter-proliferation side, inter-agency co-ordination is done through the Committee Concerned with Studying the Security Council's Resolutions Issued Pursuant to Chapter Seven of the United Nations' Charter (Chapter VII Committee). This is responsible for implementation of all UN Chapter VII obligations, including the implementation of targeted financial sanctions related to proliferation (but not those related to terrorism which are dealt with by the PCCT), and has a mandate to take the necessary actions to apply the provisions of the UN Resolutions. The Chapter VII committee includes authorities relevant to WMD proliferation, (including the FIU through its parent authority, the State Security Presidency) and communicates with AML/CFT authorities as needed, including through regular meetings with the AMLPC and PCCT.

Weighting and Conclusion

Saudi Arabia has exceptionally strong and well-established co-ordination bodies for AML and CFT, which have shown their value. But there are two minor weaknesses: the Action Plan does not yet fully reflect the risks identified in the NRAs, and the FIU is not a direct member of PCCT or the Chapter VII Committee.

Saudi Arabia is *largely compliant* with R.2.

Recommendation 3 – Money laundering offence

In its 3rd round MER, Saudi Arabia was rated LC for Recommendation 1 and LC for Recommendation 2 on the scope of the money laundering offence. The sources of law at the time were *Shari'ah* and the Anti-Money Laundering Statute (AMLS). The main technical shortcomings noted in the previous MER where that there was a lack of clarity as to whether or not self-laundering and predicate offences committed aboard were covered under the law, and absent the specific criminalisation of terrorism financing, it was not possible to separate ML from TF and therefore fully assess ML independently.

Shari'ah provides the overarching legal framework in Saudi Arabia, and includes general provisions for the criminalisation of money laundering. Criminal law that deals with specificities, such as the specific provisions of anti-money laundering law, is covered in Statutes, which are complimentary to *Shari'ah* (See section 1.4). In October 2017, a new anti-money laundering law was issued by Royal decree (the AMLL), coming into force on 24 October. 2017. Implementing regulations were issued by Ministerial Resolution (AMLL IR) and came into force during the onsite visit on 10 November 2017. The 2017 AMLL superseded the anti-money laundering law issued by Royal Decree in April 2012.

Criterion 3.1 - ML is criminalised on the basis of the relevant articles of the Vienna Convention and the Palermo Convention. Knowingly converting, transferring or conducting any transaction of funds that are known to be the proceeds of crime; acquiring, possessing or using funds that are known to be the proceeds of crime; and concealing or disguising the true nature, source, movement, ownership, place, disposition, or manner of disposition, or rights with respects to funds that are known to be the proceeds of crime are all defined as money laundering offences (AMLL, Article 2).

Criterion 3.2 - Saudi Arabia applies an 'all crimes' approach under Shari'ah, with the dealing in monies that have been gained illegally is prohibited. The proceeds of crime are defined in the AMLL as the funds directly or indirectly obtained from a predicate offence, with a predicate offence defined as any act that constitutes an offence in Shari'ah or Statutory Law (AMLL, Article 1). All of the designated categories of offences defined by FATF are offences in Saudi Arabia (See FATF-MENAFATF Mutual Evaluation Report of Saudi Arabia 2010 for the relevant text from the Holy Quran and other Statutes, CFT law)[27]. The income tax law details the taxes required to be paid in

27 Further to the UNCAC review of Saudi Arabia conducted in 2017, Saudi Arabia has committed to amend the anti-bribery law so that all of the crimes listed required to be

Saudi Arabia (corporation tax and the taxes that apply to natural persons) and the fines due as punishment for failure to pay (or late payment) [Council of Ministers Resolution No.278, December 2004], meaning tax crimes according to the income tax law are also predicate offences for money laundering.

Criterion 3.3 – Saudi Arabia applies an 'all crimes' approach, with all criminal offences which generate proceeds predicate offences to ML.

Criterion 3.4 - The ML offence applies to funds, which are defined as assets, economic resources, or property of any value or type. The funds may directly or indirectly represent the proceeds of crime (AMLL, Article 1).

Criterion 3.5 - A conviction for a predicate offence is not necessary when securing a conviction for money laundering or establishing that property represent the proceeds of crime [AMLL, Article 4).

Criterion 3.6 - Predicate offences for Money Laundering extend to offences committed outside Saudi Arabia, if the act committed constitutes an offence in the State in which in which it was committed, and if it constitutes an offence under Shari'ah or Statutory Law in Saudi Arabia (AMLL, Article 1).

Criterion 3.7 - The money laundering offence can apply to a person who committed the predicate offence (expressly stated in AMLL IR Article 2/1 and implied in AMLL Article 2).

Criterion 3.8 - It is possible for intent or knowledge required to prove a money laundering offence to be inferred from objective factual circumstances (AMLL Article 4).

Criterion 3.9 - The penalties applied to national persons convicted of money laundering are applied under the AMLL and appear proportionate and dissuasive.

Natural persons convicted of ML are subject to imprisonment for a period of up to ten years and no less than two years, and/or a fine not exceeding 5 million Riyals (AMLL, Article 26). If information is provided that relates to another ML offence, the penalties may be reduced (1-7 years imprisonment and a fine of up to 3m SAR) [AMLL, Article 30]. If the offender has a prior conviction or the ML is accompanied by other serious offences, they are subject to a more severe range of sentences (3-15 years imprisonment and a fine of up to 7m SAR) [AMLL, Article 27]. Non-Saudi nationals are deported on completion of their sentences, and Saudi nationals are not allowed to travel outside Saudi Arabia after completing their sentence for a period equal to the duration of the sentence (AMLL, Article 28).

While there are more severe punishments provided for in Saudi Arabian law for some predicate offences (for example the death penalty is available for the illegal trafficking in narcotic drugs and psychotropic substances), the offences for ML under the AMLL appear broadly proportionate with many of the serious predicate offences such as bribery (up to 10 years imprisonment and/or a fine of up to 1m SAR), cybercrime (imprisonment of up to 3 years and/or a fine up to 2m SAR) and the counterfeiting of currency (imprisonment of at least 5 years and a fine of 300-500k SAR).

criminalised under UNCAC are criminalised in Statute (as opposed to the more general provisions in Shari'ah that criminalise some offences relating to bribery and corruption).

Criterion 3.10 - Legal persons are criminally liable for money laundering, with the act of money laundering defined on the same basis as an act committed by a natural person, and are subject to proportionate and dissuasive sanctions according to the AMLL. A legal person that is convicted of a ML offence is subject to a fine of no more than 50 million Riyals *and* no less than the equivalent of double the value of the funds that were laundered. A legal person may also be permanently or temporarily prohibited from engaging in certain licensed activities, may be ordered to close the offices that were involved in the money laundering activity, and may be ordered to liquidate the legal person's business (AMLL, Article 31).

The criminal liability of a legal person does not exclude the criminal liability of the chairman, members of the board of directors, owners, employees, authorised representatives, auditors or hired staff, or any other natural person who has acted in the legal entity's name or on its behalf (AMLL, Article 3).

Criterion 3.11 - The ancillary offences defined as a money laundering offences include: participation in; association with or conspiracy to commit; attempt; aiding and abetting; facilitating; and counselling the commission of an act of money laundering (AMLL Article 2).

Weighting and Conclusion

Saudi Arabia is compliant with R.3.

Recommendation 4 – Confiscation and provisional measures

The overarching framework for confiscation in Saudi Arabia is based on Shari'ah and provides the competent authorities with a general power to confiscate all proceeds of crime. The specific framework, consistent with the general powers provided in Shari'ah, is provided for in the AMLL and CFT Law, issued by Royal Decrees in October and November 2017 respectively, and gives the circumstances in which confiscation of laundered property should occur. Other statutes that relate to a particular predicate offence, for example the Law of Combating Narcotics and Psychotropic Substances, include provisions for confiscation that pre-date the AMLL and CFTL but are still in force in parallel to the AMLL and CFTL, although do not provide specific provisions that detail the circumstances around which the proceeds of crime may be confiscated.

In its 3rd round MER, Saudi Arabia was rated PC for Recommendation 3. The main technical deficiencies were the insufficient protection provided to some bona fide third parties, and the lack of clear powers to provisionally funds relating to predicate offences or TF. Other deficiencies related to effectiveness issues. Since the 3rd round MER, two new AML laws that include provisions for confiscation have been issued. The first came into force in April 2012, and a new AML Law (the AMLL) came into force replacing it in October 2017. Two new CTF laws that include provisions for confiscation have been issued. The first one came into force in December 2013, and a new law on terrorism and its financing (CTFL) came into force replacing it in early November 2017.

Criterion 4.1 - Under Shari'ah, it is not relevant who owns criminal property (criminal or a third party). The law permits the confiscation of property relating to the offence,

regardless of who holds is in possession of it. Therefore, the legislative framework for confiscation in Saudi Arabia is applicable to criminal defendants and third parties.

a. In the event of a conviction for a money laundering offence, the competent court must issue an order to confiscate the laundered funds (AMLL, Article 33). Funds are defined as assets, economic resources or property of any value of type, whether material or immaterial, movable or immovable, tangible or intangible along with documents, deeds, transfers, letters of credit and instruments of any kind, in line with the FATF definition of *property* (AMLL, Article 1).

b. Proceeds (including proceeds intermingled with funds acquired from legitimate sources) and instrumentalities of crime are subject to confiscation in the event of a conviction for money laundering or for a predicate offence (AMLL, Article 33). The proceeds of crime are defined as funds directly or indirectly obtained or acquired from or through the commission of a predicate offence, in line with the FATF definition of proceeds. The definition of the instrumentalities of crime includes anything used or intended to be used in a crime stipulated within the AMLL. As the crimes included within the AMLL include ML itself, proceeds of or the intended proceeds of ML is included, and therefore subject to confiscation (AMLL, Article 1). Articles 33 to 37 of the AMLL set out the process for confiscating laundered funds in Saudi Arabia. The definition of laundered funds includes any interest, profit or other income generated from such funds.

c. In the event of a conviction for terrorist financing, the competent court must issue an order to confiscate the proceeds, instrumentalities, and funds related to or intended to be used in a crime of terrorist financing (CFT Law, Article 58). This includes the financing of terrorism, terrorist acts or terrorist organisations (CFT Law, Article 1). The definition of the *proceeds of crime* and *funds* are in line with the FATF definition of proceeds and property respectively (CFT, Article 1).

d. In cases where confiscation is not possible because the funds are no longer available for confiscation or cannot be located in full or in part, the court shall order confiscation of any other funds owned by the offender in order to recover an amount that is equivalent in value (AMLL, Article 35).

Criterion 4.2 - Saudi Arabia has an 'all crimes' approach, whereby the proceeds of crime are defined as the funds directly or indirectly obtained from all predicate offences (See R.3). Therefore, the measures provided for in the AMLL apply to the crime of terrorism financing, as well as all other offences in Saudi Arabian law.

a. Criminal investigating officers (see R.30) are given the responsibility for criminal and administrative investigations aimed at identifying, tracing or securing the proceeds or instrumentalities of crime (AML, Article 49). All proceeds of crime must be subject to confiscation (AMLL, Article 33).

b. The Public Prosecution, based on a suspicion of money laundering or a predicate offence, may order the provisional seizure of funds that are or may become subject to confiscation. The order should be issued and executed without notifying the party concerned (AMLL, Article 44).

c. The competent court may invalidate or prohibit an activity, whether contractual or otherwise, if one or more of the parties knew or should have known that such an

activity could prejudice the ability of the competent authority to recover funds subject to confiscation (AMLL, Article 33).

d. Criminal investigating officers shall have the responsibility for searching, enquiring and gathering evidence in relation to the crimes within their jurisdiction (AMLL, Article 49) [See also R.31].

Criterion 4.3 - In the event of a conviction for a money laundering or predicate offence, the competent court shall issue an order to confiscate property without prejudicing the rights of third parties acting in good faith. Funds may not be confiscated if a third party can establish that he/she acquired the funds by paying a fair price or in return for the provision of services corresponding to the value of such funds or based on other legitimate grounds, and that he/she was unaware of their illicit origin (AMLL, Article 33). Any funds confiscated accrue to the Public Treasury, although remain bearing rights of any third parties acting in good faith – for example if the co-owner of property that is confiscated is an innocent party, the court will subsequently determine the share of the rights that they retain in property to reflect their original interest (AMLL, Article 36).

Criterion 4.4 - In April 2017, the General Commission for the Guardianship of Trust Funds for Minors, (in co-ordination with the Permanent Committee for Combatting Money Laundering), was established as the body responsible for managing the confiscated funds and assets in ML crimes and all predicate offences (Executive Order no.451, April 2017). Predicate offences include the crime of the financing of terrorism.

During the onsite visit, it was explained that the asset that is frozen is sometimes managed by the person under suspicion, or following a court order transferred to specific experts to manage, when the court deems it appropriate. However, further details of the mechanisms for the disposal of frozen, seized or confiscated funds, as necessary, have not been provided, including how the asset under supervision of the owner is protected.

Weighting and Conclusion:

The only shortcoming for R.4 is that it is not clear what mechanisms are in place for managing, and when necessary, disposing of property frozen, seized or confiscated, beyond the establishment of the General Commission for the Guardianship of Trust Funds for Minors as the institution responsible for undertaking these tasks.

Saudi Arabia is largely compliant with R.4.

Recommendation 5 – Criminalisation of TF

Saudi Arabia was rated PC for former SR II. The main deficiency was that Saudi Arabia did not have a standalone statutory law pertaining to terrorism financing (TF) but rather pursued cases of terrorism financing as money laundering cases. Since the last evaluation, Saudi Arabia established a separate TF offence with Royal Decree No. M/16 of 27 December 2013, the Law of Terrorism Crimes and Financing (LTCF), which came into force on 1 February 2014. This law was superseded by the new Law on Combating the Financing of Terrorism (CFT Law) passed on 1 November 2017 with Royal Decree No. M/21 12/2/1439 AH. Royal Order No. A/44 of 3 February 2014 is also relevant for TF offences.

Criterion 5.1 - Article 47 of the CFT Law criminalises the financing of terrorism as:

providing, raising, collecting, and receiving funds or allocating, transferring, converting, acquiring them, or calling for contributing such funds in any manner, directly or indirectly, from a legitimate or illegitimate sources with the intention that they should be used or in the knowledge that they are to be use wholly or in part for committing a terrorist offence, inside or outside the Kingdom or they are related to it or they will be used by a terrorist entity or a terrorist for whatever purpose, even if the crime has not occurred or the funds have not been used.

The CTF Law criminalises all the acts provided for in Articles 2.1(a), 2.1(b), 2.4 and 2.5 of the TF Convention, including the financing of all those activities mentioned in the annex to the TF Convention (CFT Law, art.1.3, art.1.4, and art.47).

It should be noted that the TF offence in Saudi Arabia also applies to acts that go beyond Article 2 of the TF Convention. This is established in Article 1.3 of the CFT Law, which defines "terrorist crime" as including:

Any act committed, individually or collectively, directly or indirectly, by a perpetrator, with the intention to disturb public order, destabilise national security or state stability, endanger national unity, suspend the Basic Law of Governance or some of its articles, undermine state reputation or status, cause damage to state facilities or natural resources, attempt to coerce any of its authorities into a particular action or inaction or threaten to carry out acts that would lead to any of the aforementioned objectives or instigate such acts; or any act intended to cause death or serious bodily injury to a civilian, or any other person, when the purpose of such act, by its 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.

This overly broad definition of a terrorist act, in turn, criminalizes the financing of activity not contemplated by the TF Convention, as it includes acts said to threaten national security or stability without further elaboration, conventional crimes, and non-violent acts of protest or dissent[28].

Criterion 5.2 - The CFT Law and Royal Order A/44 ensure that the TF offence extends to the financing of any funds or assets by any means to support a terrorist act, as well as to the funding of a terrorist group or individual even in the absence of a link to a specific terrorist act. The CFT Law criminalises the provision and collection of funds in any manner, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be use wholly or in part for committing a terrorist offence (Art.47).

Royal Order A/44 criminalises the support and the provision of any material support to an organisation designated as a terrorist organisation domestically, regionally or internationally (Article First.2). The CFT Law criminalises the provision and collection of funds "with the intention that they should be used or in the knowledge that they will be used by a terrorist entity or a terrorist for whatever purpose"

28 This is noted in the findings of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, on their country visit to Saudi Arabia, published on www.ohchr.org/Documents/Issues/Terrorism/SR/A.HRC.40.%20XX.Add.2SaudiArabiaMission.pdf

(Art.47). A "terrorist entity" is considered any group of persons, whether located inside or outside the Kingdom of Saudi Arabia that commits any of the acts set forth under the CFT Law (CFT Law, Art.1.6). A "terrorist" is any natural person, whether located inside or outside the Kingdom of Saudi Arabia, who Commits or attempts to commit or participate or organises or contribute to any crimes as set under the CFT Law, by using any means directly or indirectly (*ib.*).

Criterion 5.2bis - The TF offence in Saudi Arabia extends the travel of individuals who travel to a State other than theirs for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts; it also extends to providing and receiving terrorist training. This is mainly provided in Art.1.4 of the CFT Law which makes it explicit that the TF offence also applies to the "financing of travel and training of a terrorist individual outside his/her country." Whoever travels to another State for the purpose of committing a crime set out in the CFT Law may be sanctioned (CFT Law, Art.47).

Even before the introduction of the CFT Law in November 2017, there were provisions adherence to and providing *any material or moral support* to designated terrorist organisations (Royal Order A/44, Item First). It was also a TF offence to *arrange for training sites* and *knowingly provide any other means of support and financing as well as any act that constitutes a crime within the scope of the agreements* contained in Annex 1 of the TF Convention (LTCF, Art.1.b).

Criterion 5.3 - TF offences extend to any funds or assets whether from a legitimate or illegitimate source (CFT Law, Art.47). Funds are defined very broadly as "assets, economic resources or properties of any value or type, however acquired, whether material or immaterial, movable or immovable, tangible or intangible, along with documents, deeds, transfers, letter of credits and instruments of any form, whether inside or outside the Kingdom. This includes electronic or digital systems and bank credits that evidence ownership or interest therein, also all types of commercial papers, securities, or any interest, profit or other income generated from such funds" (CFT Law, Art.1.8).

Criterion 5.4 - An act would be considered as a TF offence even if the funds were not actually used to carry out or attempt a terrorist attack, or be linked to a specific terrorist act. This is explicitly provided in Art.47 of the CFT Law (see above).

Criterion 5.5 - The intent and the knowledge required to prove the TF offence can be inferred from objective factual circumstances. Inferring the intent, the knowledge or the purpose of committing a crime of terrorism or the crime of financing terrorism shM/16all be through the circumstances and the objective and factual circumstances of the case (CFT Law, Art.91).

Criterion 5.6 - There are proportionate and dissuasive sanctions for natural persons convicted for TF. The CFT Law provides for a host of sanctions for terrorist financing offences. Persons convicted for financing a terrorist crime may be sentenced to prison between 5 and 15 years (CFT Law, Art.47). Financing of recruitment is punishable with prison between 8 and 25 years (CFT Law, Art.35). Providing weapons, explosives, and forged documents, to terrorist entities and individual terrorists may be punished with prison from 10 to 30 years (CFT Law, Art.37). The provision of material support such as communications means, information, livelihood means, housing, medical care, transport shall be punished with prison from 10 to 20 years

(CFT Law, Art.38). None of the punishments prescribed under the CFT Law shall prejudice a more severe punishment based on the provisions of Islamic Sharia Law or other laws (CFT Law, Art.52). Aggravated sanctions may apply, including if the acts result in death. In addition to prison, travel bans may be imposed on Saudi citizens convicted for TF (CFT Law, Art.53). There is flexibility for judges to reduce and or suspend minimum sentences based on co-operation and/or remorse (CFT Law, Art. 56 and Art. 57).

These sentencings appear proportionate to other terrorism-related crimes. For example, joining a terrorist entity is punished with prison between 3 and 20 years (CFT Law, Art.33), and establishing or managing a terrorist organisation may be sentenced to prison from 15 to 25 years. Supporting a terrorist ideology, terrorist entity or a terrorist crime and expresses sympathy with it or promotes it shall be sentenced to prison from 3 to 8 years (CFT Law, Art.34).

Prior to the introduction of the CFT Law in November 2017, the law did not provide for specific sanctions for violation of TF offences. TF crimes were regarded as "major crimes requiring detention" and the sanctions were inferred from the AML Law (Royal Decree No. M/16, Second Item). As such, TF offences were punished the same way as ML, hence by imprisonment for 10 years and a fine of no more than SAR 5 million.

Criterion 5.7 - The CFT Law has introduced liability for TF offences committed by legal persons. Any legal person whose owners, representatives, directors, or agents have committed any of the offences set out in this law or contributed thereto shall be sentenced to a fine between SAR 3 million and SAR 10 million (between EUR 650 000 and EUR 2 150 000), if the crime has occurred in his name or for his own account (CFT Law, Art.49). This fine is without prejudice to the criminal liability of the natural persons. Courts may suspend the activity of the legal person on a temporary or permanent basis, or close the offices associated with the crime on a temporary or permanent basis, liquidate the business or appoint a judicial guard to manage funds and transactions.

Criterion 5.8 - It is an offence to attempt to commit a TF offence, instigate to commit such an offence, to participate as an accomplice, to aid and abet (CFT Law, Art.51).

Criterion 5.9 - TF offences are designated as ML predicate offences as Saudi Arabia adopts an all-crime approach to the offences underpinning money-laundering (AML Law, Art.1).

Criterion 5.10 - The TF offence established by the CFT Law applies to anyone who committed the TF offence in Saudi Arabia or abroad (CFT Law Art.47).

Weighting and conclusion:

Saudi Arabia is Compliant with R.5.

Recommendation 6 – Targeted financial sanctions related to terrorism & terrorist financing

In the 2010 MER, Saudi Arabia was rated PC for former SR III. The main deficiencies were that Saudi Arabia did not implement UNSCR 1373, and regarding UNSCR 1267,

their freeze actions did not apply to a broad range of funds, there were no communication mechanisms between non-bank FIs and DNFBPs, and there was no guidance for non-bank FIs and DNFBPs. There was also a lack of a clear monitoring and sanctioning procedures to verify implementation of freezing requests. Since the last evaluation, Saudi Arabia has taken several steps to address these deficiencies.

Criterion 6.1 -

a. The Permanent Committee for Combating Terrorism (PCCT) is the competent authority to propose persons or entities to the 1267/1989 Committee and the 1988 Committee for designation, as it is entrusted with the implementation of the UNSCR (1267/1989), (1988) and the subsequent relevant resolutions (CFT Law, Art.75). The formal decision to propose a designation to the UN Committees is made by the Head of the Supreme Committee for Combatting Terrorism in accordance with the powers granted to him by the CFT Law (Mechanism for the Implementation of the Security Council's Resolutions related to ISIL/Al-Qaeda (1267/1989/2253), s.4; Mechanism of Implementation of UNSCR 1988 (2011) and Successor Resolutions, s.4). With the issuance of the new CFT Law in November 2017 repealing the 2013 Law to Combat the Financing of Terrorism, the Head of the Supreme Committee for Combatting Terrorism moved from Ministry of Interior to State Security Presidency. The Ministry of Interior issued a telegram No. 109130 dated 23/1/2017 to circulate the mechanisms to the concerned parties in view of their effective implementation.

b. Saudi Arabia has mechanisms to identify targets for designation, based on the designation criteria of the relevant UNSCRs. The current applicable regulations were issued on 23 January 2017 through the Ministry of Interior Telegram No. 109130 which requires the Ministry of Interior to circulate and implement the mechanisms for (1267/1989/2253) related to ISIL, Al-Qaida, and associated individuals, groups, undertakings and entities listed on the Committee's consolidated list (1267/1989/2253), (1988) related to listed names and (1373) to the concerned parties in view of their effective implementation.

c. The implementing mechanism for UNSCR 1988 applies an evidentiary standard of proof based on *sufficient reasons* or *proper ground*. The mechanism for UNSCR1267/1989/2253 applies a proof standard based on *adequate causes* or *sound grounds.* The proposals for designation are not dependent on the existence of criminal proceedings.

d. and e. The implementation mechanisms for UNSCR 1988 (2011) and UNSCR 1267/1989/2253 clearly outline the necessary forms and procedures to follow and requires that as much pertinent information be provided, along with a justification statement, and clarifying whether Saudi Arabia initiated the request, and what information should be kept confidential and be provided. Standard forms for listing are used.

Criterion 6.2 -

a. Saudi Arabia has identified two different authorities within the Ministry of Interior (as of November 2017 the State Security Presidency) for implementing designations as set forth in UNSCR 1373 (Mechanism of Implementation of Security Council's Resolution 1373 (2001) and Successor Resolutions, s.8). Mabaheth (General Investigation Directorate) is responsible for designating Saudi or resident individuals and entities. The PCCT (as of November 2017 under the State Security Presidency) is

responsible for initiating designation requests based on foreign requests. The formal decision to designate individuals or entities based on foreign requests is made by the Ministry of Interior (as of November 2017 the State Security Presidency) after proposal by the PCCT.

b. Mabaheth has mechanisms in place for identifying targets and when suspecting a terrorist financing operation, must pursue a provisional seizure of funds without delay and without prior notice (within a few hours). Similarly, the Mechanism of Implementation of Security Council's Resolution 1373 (2001) and Successor Resolutions, provides the PCCT with the authority to examine, give effect to receive requests from other countries related to a proposed designation, and allows the PCCT to investigate and effect the designations.

c. The PCCT will review each request, acknowledge the submission within 3 days, and reply within 1-2 months. However, during the on-site the PCCT offered examples of when replies may take longer given political sensitivities that may delay the decision-making surrounding the request.

d. When deciding whether or not to make a designation, there is no clear reference to "reasonable grounds", although the regulations provide a thorough accounting of the types of information necessary to make a decision (Mechanism of Implementation (1373), page 5 "Local Evidence Standard, Local Listing Standards, and other considerations"). If the PCCT considers that a request from a foreign country for designation should be approved, it submits this proposal to the State Security Presidency and the Royal Highness for approval. The Saudi Arabian authorities indicate that designations originating from foreign requests should be based on a reasonable basis and grounds for listing, which they report as being connected with a terrorist organisation or terrorist activity, although this is not explicitly stated in the law. Proposals for designation are not conditional upon the existence of a criminal proceeding.

e. Saudi Arabia can request another country give effect to designations by submitting the standard form for 1373, although they have never done so. The form asks that as much detail as possible be provided. The PCCT is responsible for submitting requests via Mabaheth or MOFA for designation to a foreign country depending on whether the PCCT choses to go through official channels or any CFT counterparts.

Criterion 6.3 -

a. The PCCT is responsible for receiving and studying requests for designations at the UN Committees and from foreign countries based on UNSCR 1373. Mabaheth (General Investigation Directorate) is responsible for considering domestic designations based on national information. The implementation mechanisms establish the procedures necessary to collect and solicit identifying and supporting information for a designation. A number of relevant authorities, including Ministry of Foreign Affairs, the State Security Presidency, the Ministry of Interior, Mabaheth, collectively obtain and share information while developing designation recommendations. As the co-ordinating body, the PCCT oversees the designation process and requests specific agencies to solicit missing pieces of information.

b. "As appropriate", Mabaheth (General Investigation Directorate) and according to the classification party, shall take the possible measures to notify or inform the listed individual or entity. The notification will be accompanied by a narrative summary and

the description of the implications arising from the inclusion of their name on the list. The application of restrictive measures shall not be dependent on the notification procedure.

Criterion 6.4 - According to the implementation mechanisms for UNSCR 1267 and for UNSCR 1988, agencies shall immediately without delay (within a few hours) implement targeted financial sanctions without delay, and without prior notice (section 7). Any agency and authority concerned with the freezing of funds, including FIs and DNFBPs are required to continuously check UN lists via the UN website (section 9).

With regard to domestic designation, Mabaheth can apply provisional seizures of funds without delay (within hours) and without prior notice in relation to designees. In the case of domestic designations based on a foreign request, the Implementing Mechanism for UNSCR 1373 states that the relevant parties (e.g. FIs and DNFBPs) should implement the freezing procedures once the Minister of Interior has issued a general statement about the listing, in addition to publishing it on the Saudi press (page 15, section Second). The Guidelines for the Implementation of the Mechanisms relevant to the Security Council Resolutions on Countering Terrorism Financing specifically require to freeze funds without delay upon publication of a target. Restrictions such as travel ban and arms embargo should be applied without delay after a name is published (Implementation Mechanism for UNSCR 1373, pages 17 and 18).

Criterion 6.5 –

a. Saudi Arabia specifies the parties that are required to freeze without delay and without prior notice the funds and assets of designated persons as set forth in the implementation mechanisms outlined in UNSCR 1267/1989/2253[29] and 1373,[30] and not all natural and legal persons are included. For UNSCR 1267 and 1988, FIs are not specifically required by law to freeze funds, although in practice banks do implement sanctions. For requests considered by the PCCT, the parties involved are required to freeze assets, but there is no timeframe specified (e.g. without delay, or without prior notice). For requests considered by the GID (Mabaheth), the 1373 Implementation Mechanism specifies that the competent authorities shall require the relevant parties to freeze the funds/assets without delay and without prior notice 'when suspecting

29 The parties concerned with the freezing of funds for designated persons under UNSCR1267 and UNSCR 1988 are: Ministry of Interior, Ministry of Justice, Ministry of Commerce and Investment, SAMA, Capital Market Authority, Ministry of Finance (custom), Ministry of Social Affairs, Ministry of Transportation (the General Authority of Civil Aviation), the Saudi Port Authority, Communication and Information Technology Commission, DNFBPs, NPOs, Airline Companies working in Saudi Arabia.

30 The parties concerned with the freezing of funds pursuant to designations made under UNSCR 1373 are: Ministry of Interior (the Standing Committee Against Terrorism, General Investigation Directorate), Ministry of Justice, Saudi Arabian Monetary Authority, Capital Market Authority, Ministry of Trade and Investment, Ministry of Finance (Customs Department), Ministry of Labour and Social Development, Communications and Information Technology Commission, Financial Institutions, Designated Non-Financial Business or Profession.

any FT operation' (Section First, page 13). Saudi Arabia specified that this related to supervisory authorities who contact the FIs and DNFBPs.

b. The term, 'funds' is defined very broadly and covers the requirements on this sub-criterion. The definition of funds, in Article 1 (8) of the CFT Law includes 'assets, economic resources or properties of any value or type, however acquired, whether material or immaterial, movable or immovable, tangible or intangible, along with documents, deeds, transfers, letter of credits and instruments of any form, whether inside or outside the Kingdom. This include electronic or digital systems and bank credits that evidence ownership or interest therein, also all types of commercial papers , securities, or any interest, profit or other income generated from such funds. The Mechanism for Implementing the UNSCRs 1267 and 1373 require competent authorities to issue freezing orders to FIs to freeze funds and assets.

c. Saudi TFS mechanisms do not specifically prohibit nationals and persons within the jurisdiction from making any funds and other assets available to designated individuals and entities. Saudi Arabia partly mitigates this by criminalising TF in a broad sense. The Royal Order No. A/44 criminalises the act of providing any form of material or moral support to a terrorist organisation, classified locally, regionally, or globally. Given the broad definition of funds, this extends to prohibiting anyone in Saudi Arabia from making assets or economic resources available to designated persons, entities owned or controlled directly or indirectly by designated persons, and persons acting on behalf of designated persons.

d. Page 5 of the 'Mechanism of Implementation of UNSCR 1988 (2011), 'Work Mechanism' states that authorities, which includes CMA, MOCI, PCCT, SAMA, FIs, DNFBPs, NPOs, shall check the consolidated webpages of the Security Council Committees on a daily and continuous basis to ensure that they take note from a new inclusion, deletion, or a data modification. CMA and SAMA published in March 2017 guidance for FIs to implement targeted financial sanctions. MOCI also published guidance in November 2017 for real estate agents and DPMS. Other DNFBPs did not receive guidance.

e. Financial institutions and DNFBPs are required to report to competent authorities (PCCT or Mabaheth) any assets frozen or actions taken in compliance with the prohibition requirements (Implementation Mechanism for 1267, s.9, Implementation Mechanism for 1988, s.9). There is no similar provision requiring FIs and DNFBPs in the Implementation Mechanism for 1373. In the case of APs, CMA issued a circular on 6 March 2016 requiring APs to implement UNSCRs.

f. There are measures which protect the rights of *bona fide* third parties acting in good faith. Any party listed on the UN Committee's consolidated list (1267/1989/2253), as well as in the domestic lists under UN 1373, may file grievance cases whether inside or outside the Kingdom against any issued resolutions, according to the text of the Board of Grievances, as well as crimes of terrorism and its financing in Articles. Pursuant to the mechanism of implementation of UNSCR 1988 (2011) and the relevant subsequent resolutions, those listed on the consolidated list of the Committee (1988), may submit a request to the PCCT to take necessary actions concerning the request, for example and without limitation, notification of the procedures that may be followed at judicial level. Article 71 of the CFT Law exempts FIs, DNFBPs and NPOs from criminal liability resulting from execution of duties,

unless established that the actions were maliciously carried out to harm the person subject to the transaction.

Criterion 6.6 –

a. The Mechanisms for Implementation of the UNSCR of the Security Council Committee (1267/1989/2253) as well as the Mechanisms for the implementation for 1373 include procedures for submitting de-listing requests and unfreezing the funds or other assets of persons and entities which no longer meet the criteria for designation.

b. The UNSCR 1373 Mechanism includes a 'Guidelines to Eliminate the Name and Life the Freezing' which provides detailed guidelines on how to remove a name by submitting a request to the Board of Grievances for their review and consideration.

c. An individual, entity, or country, can file a request for lifting the designation classification to the Ministry of Interior or the Ministry of Foreign Affairs, 'as appropriate.' Saudi Arabian authorities define 'as appropriate' to mean 'as in the appropriate way,' based on where the individual is present For example, the individual should apply directly to the Ministry of Interior if the person is a citizen or resident, but to the Embassy of the Kingdom if located outside the country, which would then refer the request to the Ministry of Interior. It is not clear that this would be a sufficiently independent authority to review the designation given that MOI implements the designation itself.

d. Parties are entitled to file a grievance by lodging a request to the PCCT which will take all necessary procedures regarding the request, including co-ordinating with the petitioner, preparing the requisite report, and communicating a final decision regarding the request.

e. There are no procedures for informing designated persons and entities of the availability of the UN Office of the Ombudsperson to accept de-listing petitions, although in practice, Saudi Arabia has engaged with the Office of the Ombudsman in practice for de-listing requests.

f. Parties are able to submit grievance requests for designations under 1267, 1988, and 1373. The PCCT communicates with any designated person and inform him/her about the procedures for removing the name from the list and for lifting the seizure of part of the funds. However these procedures are not publicly available.

g. Competent authorities are required to immediately and without delay (within a few hours) and without prior notice, take all necessary actions to lift sanctions imposed once removed from an UNSCR list. According to Saudi authorities, the Consolidated List of the Council Committee will be updated immediately without delay (within hours) and without prior notice, in accordance with UNSCR 1267.

Criterion 6.7 - The Mechanism of Implementation of UNSCR 1988 (2011) and Successor Resolutions accounts for freezing exemptions provided appropriate conditions are met and in accordance with procedures set out in UNSCR 1452 (page 6). The Mechanism of Implementation of UNSCR 1988 (2011) authorizes the ability to lift sequestration over part of the funds for human living purposes or additional purposes (page 16).

Weighting and conclusion

Saudi Arabia has implemented a law establishing the legal enforcement regime for asset freezing related to terrorism and terrorist financing. However, it is unclear whether the measures in place ensure that the sanctions will be without delay in all cases. Not all natural and legal persons in Saudi Arabia are required to freeze the funds and assets of designated persons. Saudi TFS mechanisms do not specifically prohibit nationals and persons within the jurisdiction from making any funds and other assets available to designated individuals and entities, although the criminal legislation in part mitigates this issue. The procedures for de-listing and unfreezing the funds are not clear.

Saudi Arabia is Partially Compliant with R.6.

Recommendation 7 – Targeted financial sanctions related to proliferation financing

Criterion 7.1 – Royal Decree 7753/MB dated 29/10/1427 H (20 November 2006) grants the legal basis for Saudi Arabian authorities to implement targeted financial sanctions related to the prevention, suppression, and disruption of weapons of mass destruction. Royal Decree 7753 establishes the Chapter VII Committee and delegates to the Committee the implementation of these sanctions. The Chapter VII Committee is responsible for preparing reports and distributing them to representatives in the Committee for implementation. The "Mechanism to implement the Security Council Resolutions Issued by Chapter VII of the United Nations" was issued in November 2017. This mechanism requires any person including FIs and DNFBPs to freeze without delay and prior notice the funds belonging to, owned, held or controlled, wholly or jointly, directly or indirectly, by any person or body designated by Sanctions Committee or United Nations Security Council in accordance with a relevant UN Resolution (Art.3).

Criterion 7.2 **–** The Chapter VII Committee, established by Royal Decree 7753/MB, has the legal authority to implement and enforce targeted financial sanctions related to the prevention, suppression and disruption of the proliferation of weapons of mass destruction and its financing. The Committees Duties include taking necessary action concerning the Kingdom's implementation of the Security Council's resolutions in relation to proliferation financing. The legislation focuses on receiving information from each agency represented on the committee and preparing reports on those activities for the Kingdom for reporting to the UN Security Council. The Committee consists of representatives from the Ministries of Foreign Affairs, Defence and Aviation, Interior, General Intelligence, Commerce and Industry, Justice, Finance/Customs Authority, Civil Aviation, Sciences and Technology, Higher Education, and the General Ports Authority. Since November 2007, the Committee includes SAMA. These entities cover some relevant agencies which are responsible for implementing targeted financial sanctions in relation to PF, and it is unclear how the relevant FIs/DNFBP supervisors missing in the Committee would implement the relevant obligations.

(a) Article 3 of the Mechanism to implement the Security Council Resolutions Issued by Chapter VII of the United Nations, requires all persons, FIs, and DNFBPs to freeze without delay and without prior notice funds by any person designated by the

Sanctions Committee or the UNSC. Funds are defined broadly as covering "other assets" (Implementation Mechanism, Art.1; AML Law, Art.1)

(b) The freezing obligations extend to funds and other assets belonging to, owned, held or controlled, wholly or jointly, directly or indirectly, by designated persons, as well as any funds derived or generated (Implementation Mechanism, Art.3). The freezing obligations are not limited to those that can be tied to a particular act, plot or threat. They also extend to funds of any person acting on behalf of or at the direction of a designated person or body and of entities owned or controlled by a designated person or body, including through illicit means (*ib.*).

(c) Saudi Arabia has existing mechanisms in place to ensure that any funds and assets are not made available by their nationals or by any other persons or entities for the benefit of the designated person, unless licensed, authorized or otherwise notified in accordance with the relevant UNSCSRs. The Saudi Authorities may authorize the release of certain funds if certain conditions are met (Implementation Mechanism, Art.6-10).

(d) The Chapter VII committee is responsible for communicating with all competent authorities concerned applying procedures regarding the implementation of these UNSCRs (Implementation Mechanism, Art.2). The Committee is in charge of circulating the resolutions by the Security Council pursuant to Chapter VII, and requires each authority represented in the Committee to report about the procedures taken regarding the application of the resolution (Royal Decree 7753/MB, 'Mechanism of the Committees Work'; and Implementation Mechanism, Art.2). There is no indication regarding the timing with which the resolutions should be distributed following UN listings and there is no information provided regarding obligations that FIs or DNFBPs must follow. The Committee must report on those actions taken to the King, for compilation into a report to the UN Security Council. There is no information provided regarding what these reports must entail or how quickly they must be compiled and submitted to the UNSC. Financial institutions and designated non-financial businesses and professions shall have in place procedures set out by supervisory authority to implement the provisions of UN Resolutions (Implementation Mechanism, Art.11); however at the time of the on-site visit no supervisory authority had yet published such procedures.[31] Only SAMA had issued circulars explaining to the supervised entities their obligations.

(e) Financial institutions and designated non-financial businesses and professions shall report to the competent committee through the supervisory authority any funds frozen or actions taken in compliance with the provisions of UN Resolutions (Implementation Mechanism, Art.12). In the absence of procedures for implementation, it is unclear whether this obligation would cover the reporting of attempted transactions.

(f) There are measures to protect the rights of *bona fide* third parties acting in good faith when implementing the obligations under Recommendation 7, (Implementation Mechanism, Art. 15).

Criterion 7.3 – The Chapter VII Committee is responsible for communicating the application of necessary procedures with all competent authorities (Implementing

31 SAMA published detailed procedures in March 2018.

Mechanisms, Art.2). FIs and DNFPBs subject to the supervision apply the UNSCRs and are monitored in their implementation by their supervisors (Implementing Mechanism, Art.11 and 12). Any person, FI, or DNFBP who fails to comply with UNSCR obligations is subject to sanctions (Implementing Mechanism, Art.13).

Criterion 7.4 –

(a) Saudi Arabia's implementing regulations (Articles 14 and 15) provide the legal basis for any person affected by freezing measures to petition for a de-listing request to the Committee.

(b) The Committee, upon request of any affected person, may direct that a specific freezing measure be amended or lifted if it is established that the person or body whose name triggered the freezing measure is not the same as the designated person or body. Individuals designated by the UNSC may submit a petition to the competent committee (the Chapter VII Committee) for referral to the Ministry of Foreign Affairs and the United Nations for consideration. The mechanism to apply for a de-listing request is however not made publicly available.

(c) The competent committee may authorize the release of certain frozen funds if they have determined that the exemption conditions (in line with UNSCRs 1718 and 2231) have been met, and following the Sanctions Committee's approval (Article 10).

(d) Under Article 2 of the Implementing Mechanism, the Committee should communicate all necessary procedures with the competent authorities without delay. The implementing regulations do not specify the timing of this communication to the private sector, what this communication entails and do not specify that this should be done immediately upon taking such action and which authority is responsible for providing guidance.

Criterion 7.5 –

(a) The implementing mechanisms (Article 5) allows the payment to the frozen account of interest or other earnings that were concluded or arose before the date of designation, provided they continue to be frozen. Financial institutions are required to notify the competent committee about these transactions without delay.

(b) The Chapter VII Committee may authorise a payment by a person or body designated by the Sanctions Committee or United Nations Security Council in accordance with a relevant UN Resolution where such payment is due under a contract or agreement that was concluded by the designated person, or an obligation that arose for that person, before the date on which that person was designated (Implementing Mechanism, Art.7). The authorisation to release certain funds may be granted when the Chapter VII Committee has determined that the funds shall be used for a payment by a person or body designated by the Sanctions Committee or United Nations Security Council in accordance with a relevant UN Resolution. This is not fully in line with the standard in that the payment should not be made to a designated person. Nevertheless, the mechanism requires that the payment does not relate to a contract for any of the items, materials, equipment, goods, technologies, training, assistance, financial assistance or services, investment, brokering or other services or activities referred to in a relevant UN Security Council Resolution; and the payment is not in breach of the freezing measures established by the relevant UNSCRs. Prior to

granting authorization under this Article the Chapter VII Committee shall notify the Sanctions Committee of the proposed course of action.

Weighting and conclusion:

Saudi Arabia has implemented a law establishing the legal enforcement regime for asset freezing related to proliferation financing. The Implementing Mechanism issued in November 2017 requires that the freezing occurs immediately after the designation by the UNSCR. The Permanent Committee is responsible for communicating with all competent authorities concerned regarding the implementation of these UNSCRs. Supervisory authorities should provide procedures to FIs and DNFBPs regarding the obligations of the authorities to ensure compliance, although at the time of the on-site visit these had not been issued. It is unclear how the relevant FIs/DNFBP supervisors missing in the Committee would implement the relevant obligations.

Saudi Arabia is Partially Compliant with R.7.

Recommendation 8 – Non-profit organisations

In its 2010 MER, Saudi Arabia was rated LC on former Special Recommendation VIII. Saudi Arabia did not review the adequacy of domestic laws and regulations that relate to NPOs. Saudi Arabia also did not identify the elements and types of NPOs that were at risk of being misused for TF by virtue of their activities or characteristics. In addition, it was unclear what the terms and legal basis were for the record keeping requirements related to NPOs. The requirements of R.8 have evolved significantly since 2010.

Since the 2010 MER, Saudi Arabia has issued the Civil Society Associations and Organisations Law dated1 December 2015, repealing the Charitable Associations and Organizations Regulations. Saudi Arabia also issued the Implementing Regulations of the Civil Society Associations and Organisations Law. The Ministry of Labour and Social Development is the authority in charge of the affairs of all Associations and Organisations. Previously, associations and organisations were supervised by two separate ministries – the Ministry of Social Affairs (which then was merged into the Ministry of Labour and Social Development) and the Ministry of Islamic Affairs, Dawah and Guidance.

An Association is defined as including any non-profit group comprising natural or corporate persons, or both, for philanthropic or co-operative purposes; for a religious activity determined by the Ministry of Islamic Affairs, Dawah and Guidance; for social, cultural, health environmental, educational, instructional, scientific, vocational, creative, youth, tourist activities, or similar activities; or any activity relating to consumer protection or any other civil activity as determined by the Ministry; whether through material, moral, technical or other support.

A civil society Organisation is any non-profit entity established for a definite or indefinite period, by one or more natural or corporate persons, or both, for public benefit or the benefit of a specific group; and funded by the founder(s)' allocation of funds, endowments, grants or bequests. Family and private funds shall be considered as civil society organizations.

Non-profit organisations (NPOs) are defined in the AML Law as those entities which are legally authorized to collect, receive or disburse funds for charitable, religious, cultural, educational, social or co-operative purposes or for any other purposes (Art.1; Implementing Regulations, Art.40). NPOs subject to the obligations set forth in the AML Law (see R.3 above).

Criterion 8.1 –

- *Sub-criterion 8.1.a.* In 2017 Saudi Arabia began analysing information derived from compliance visits of NPOs to identify those organization within the sector that pose the highest risk. Indicators of risk used centred primarily on indicators related to financial integrity.
- *Sub-criterion 8.1.b.* The Saudi Arabia NRA on TF indicates that the risk of TF *within the NPO sector is low on the basis of information on crime statistics,* international co-operation requests on FT, and domestic terrorism and terrorism financing cases. It should be noted that since 2004, all NPOs have been prohibited from raising or disbursing funds internationally. With the new legislation, only Saudi citizens can establish an NPO. No specific information however was provided with respect to how Saudi Arabia identified the nature of the threats posed by terrorist entities to the NPOs which are at risk nor as to how terrorist actors abuse those NPOs.
- *Sub-criterion 8.1.c*. Legislative changes were made with the new Civil Society Associations and Organizations Law and the Implementing Regulations and authorities stated that some of the revisions were taken directly in response to identified risk of misuse of NPOs for TF, for example the expanded range of supervisory sanctions granted to MLSD and an enhanced financial reporting obligation for NPOs under the new law.
- *Sub-criterion 8.1.d*. Saudi Arabia's risk-based supervision and inspection model (see criterion 8.1.a.) which focuses on governance and organisational structure, projects and operations, and financial accountability and transparency is an ongoing process.

Criterion 8.2- The Civil Society Associations and Organizations Law clearly articulates the rules under which organisations are formed and the way in which they may operate.

- *Sub-criterion 8.2.a.* The new Civil Society Associations and Organizations Law clearly articulates the rules under which organizations are formed and the way in which they may operate. These rules promote accountability, integrity, and public confidence in the administration and management of NPOs.
- *Sub-criterion 8.2.b.* Saudi Arabia mentioned a number of ongoing initiatives to undertake outreach and educational programmes to raise awareness among NPOs and the donor community about the potential vulnerability of TF, including awareness sessions, training programs for Chief Executives, and the "Enhanced Support Programme".
- *Sub-criterion 8.2.c*. Saudi Arabia mentioned a number of ongoing initiatives to undertake outreach and educational programmes, which results in a manual covering governance

and structure, project and operational and financial accountability. The manual was distributed to the NPOs. These initiatives address specifically TF risk and vulnerabilities.

- *Sub-criterion 8.2.d*. The new Civil Society Associations and Organizations Law has Articles which pertain to the administration of an Association's Revenues and Article 21 addresses accounting and banking best practices.

Criterion 8.3 – Strict regulatory requirements are placed on all NPOs including the obligation to report suspicious transactions to the Department of Financial Intelligence. Each organization currently receives four audit visits every year with a year-end report from the 500 inspectors employed throughout Saudi Arabia. Beginning in 2017 MLSD began developing a risk-based tool by analysing information from these visits to determine those organizations that are most at risk. The indicators developed are primarily focused around financial integrity. A total of 2.4% of the organizations were identified as high risk and were therefore subjected to both desk audits and an additional four compliance visit per year (eight in total).

***Criterion* 8.4** –

- *Sub-criterion 8.4.a.* The Ministry of Labour and Social Development actively monitor compliance of NPOs with the requirements of the Civil Society Associations and Organisations Law, which includes compliance with the requirements of R.8.
- *Sub-criterion 8.4.b.* The Civil Society Associations and Organizations Law provides for a range of proportionate and dissuasive sanctions for organizations and/or persons acting on their behalf (Art.23). The Ministry of Labour and Social Development may suspend or dissolve an Association or Organisation, or merge it with another entity, if: it deviates from its objectives; commits serious violations of the Civil Society Associations and Organisations Law, the Implementing Regulations or its charter; disposes of its funds for other than designated purposes; violates the provisions of Sharia, public policy or morality, or commits any act undermining national unity (Civil Society Associations and Organisations Law, Art.23 and 35). If violations of the Implementing Regulations and bylaws are found, the Ministry will warn the entity providing a timeline for remedy and then may suspend any of the members, remove the board of directors, dissolve the entity or merge it with another one (Implementing Regulations of the Civil Society Associations and Organisations Law, Art.87). The funds may also be provisionally seized by the State Security and the Specialised Criminal Court (CFT Law, Art.9). Persons funding terrorism can be sentenced in accordance to the provisions of the CFT Law (see R.5 above).

Criterion 8.5 – SA has all the tools, access and training to address risk within its NPO sector.

- *Sub-criterion 8.5.a.* The Ministry of Social Affairs maintains a register of Associations and Organisations. Any governmental body without any legal restrictions can obtain the data available to the Ministry of any association or organisation. Financial and demographic data and information on each NPO is available to all through the National Platform for

NPO.[32] The Ministry of Labour and Social Development keeps track of all exchanges of information related to NPOs. It can participate as needed in the national committee for combatting TF.

- *Sub-criterion 8.5.b.* Saudi Arabia has investigative expertise and capability to examine those NPOs suspected of TF activities. The authority in charge of TF investigation is Mabaheth, whose expertise includes specialised financial investigators. Saudi Arabia indicated that the Ministry of Labour and Social Development is in the process of conducting training programs to supervisors in financial crimes.
- *Sub-criterion 8.5.c*. NPOs are required to maintain information on their administration and management (Implementing Regulations, Art.40), and to provide it without delay to the State Security Presidency or the investigators (CFT Law, Art.6). The Ministry of Labour and Social Development can examine and obtain any document and register of NPOs (including financial and programmatic information), upon request or on its own behalf, to verify compliance with the NPO Law, Implementing Regulations, and bylaws (Implementing Regulations, Art.86). Investigators can obtain this information through a request to Ministry. The Ministry is in the process of implementing an automated exchange of information mechanism with other government agencies.
- *Sub-criterion 8.5.d*. The Ministry of Labour and Social Development is the focal point in Saudi Arabia for all inquiries relating to NPOs and co-ordinates with other authorities when necessary. Competent authorities have the powers to access information related to NPOs that may be involved in or misused for TF activity (CFT Law, Art.6; NPO Law Art.23 and 35; Implementing Regulations of the NPO Law, Art.86) and they have mechanisms to exchange this information domestically. If the Ministry of Labour and Social Development identifies suspected financial irregularities and offences during supervision and control mechanisms, the Ministry shall notify the FIU directly and expeditiously (Implementing Regulations, Art.40(2)).

Criterion 8.6– The competent authorities in Saudi Arabia may exchange information with counterpart authorities in other countries with which Saudi Arabia has valid agreements or treaties, or on the basis of reciprocity (CFT Law, Art.72). Under the Civil Society Associations and Organizations Law the Ministry of Labour and Social Development is the authority in charge of the affairs of associations and organizations in accordance with the provisions of this Law.

Weighting and conclusion

With the passage of the Civil Society Associations and Organisations Law, Saudi Arabia has further refined the legal framework on how NPOs (as defined by the FATF Standards) are formed and operate. The rules under the law are highly restrictive. Saudi Arabia conducts 4 compliance visits for each NPO with an additional 4 compliance visits for those deemed to be at higher risk. While the risk assessment tool used to identify those organizations most at risk of TF, does contain indicators of TF

32 This information is available in Arabic at https://dp.mlsd.gov.sa.

abuse it is primarily a heath check assessment tool based on financial integrity. In addition, there are organisations within Saudi Arabia, such as organisations under the oversight of the Ministry of Islamic Affairs that do meet the FATF definition of an NPO but are not yet subject to oversight by MLSD.

Saudi Arabia is Largely Compliant with R.8.

Recommendation 9 – Financial institution secrecy laws

The Kingdom of Saudi Arabia was rated LC on financial institution secrecy laws in its last mutual evaluation. The main deficiencies were the limitations on the sharing of information between domestic and foreign banks relating to correspondent banking and wire transfers, as well as lack of explicit exemptions to confidentiality provisions to allow sharing of AML/CFT information between institutions, internationally and domestically.

Criterion 9.1 - The supervisory authorities in Saudi Arabia have access to, or could obtain relevant information from, FIs, DNFBPs, and NPOs (*Art. 24 of the AMLL and article 82 of the LCFT*). They are also authorized to share this information with domestic and foreign counterparts.

Saudi Arabia has secrecy/confidentiality provisions (such as Art. 19 of the Banking Control Law, Art. 12 of the Law on Supervision of Cooperative Insurance Company, Art. 15 of the Finance Company Control Law) which may have wide scope. However, the AMLLIR has a provision (Arts. 9/ &, 10/11) which allows FIs to provide relevant information regarding wire transfer and correspondent banks.

Weighting and Conclusion

Saudi Arabia is Compliant with R.9.

Recommendation 10 – Customer due diligence

Saudi Arabia was rated PC on former R5. The main technical deficiencies assessed in the 3rd round ME were: lack of controls on numbered accounts; no requirements for ongoing due diligence; missing requirements for insurance companies when CDD cannot be completed, and lack of requirements to apply CDD to existing customers.

Criterion 10.1 - The AMLL (*Art. 6*) prohibits the maintenance or opening of an anonymous account or an account in an obviously fictitious name or a numbered account. Similar prohibitions apply to other sectors through the relevant rules (*Art. 4.3.1 of the RBME, Art. 14 of RIC, Art. 3.2 of the RFC and Art. 8.1 of the RAP).*

Criterion 10.2 - The AMLLIR (*Article 7/1*) mirrored the requirements of criterion 10.2.

Criterion 10.3 - Financial institutions are required by the AMLL to identify customers (natural person, legal person or legal arrangement), and verify the customer's identity using reliable, independent source documents, data or information. (*AMLL, Art. 7; AMLLIR, Art. 7/2*).

Criterion 10.4 - The AMLLIR (*Art. 7/2/b*) requires FIs to verify that any person purporting to act on behalf of a customer is so authorized, and identify and verify the identity of that person in line with subsection (a). Several sectorial regulations including paragraph 4.4.3 of RBME, paragraph 2.6.3 of MRMCB, etc. repeated the above provisions.

Criterion 10.5 - The AMLL (*Art 7*) sets out general requirement on FIs to apply due diligence measures to their customers. The AMLLIR (*Art.7/2/c*) requires FIs to identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owners, using information and data obtained from a reliable source. Specific measures on identification of beneficial ownership are also provided in the IR. Such requirements are also provided in sectorial rules for banks, money changers, insurance companies, financing companies and securities companies.

Criterion 10.6 - The AMLLIR (*Art. 7/2/d*) stipulates that FIs should understand and obtain additional information on the purpose and intended nature of the business relationship, as appropriate. Sectorial rules for banks, money changers, insurance companies, financing companies, security companies also provided such requirements.

Criteria 10.7 - The AMLLIR (*Art. 7/6*) sets out detailed provisions on on-going due diligence which covers requirement of criterion 10.7. Other sectorial rules for banks, insurance companies, financing companies and security companies also have in place relevant provisions.

Criterion 10.8 - The AMLLIR (*Art. 7/2/d*) stipulates that FIs should understand and obtain additional information on the purpose and intended nature of the business relationship. Para e of same article stipulates that FIs should understand the ownership and control structure of legal person and legal arrangement. Other sectorial rules for banks, money changers, insurance companies, financing companies, security companies also have in place relevant provisions.

Criterion 10.9 - The AMLLIR (*Art. 7/2/a*) sets out detailed requirements on sources of information should be obtained and verified by FIs for legal persons and legal arrangements. Other sectorial rules including RBME, MRMCB, RIC, RFC and RAP also set out requirements in this regard.

Criterion 10.10 - The AMLLIR (*Art. 7/2/c*) sets out a provision which requires FIs to identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owners, using information and data obtained from a reliable source. For a customer that is a legal person, a financial institution or designated non-financial business and profession shall identify and take reasonable measures to verify the identity of the natural person who ultimately owns or controls 25% or more of the legal entity's shares. Where no controlling ownership interest exists as stipulated in the previous para (1), or there is doubt whether the controlling shareholder is not indeed the beneficial owner, the identity of the natural person exercising control of the legal person through other means; or, as a last means, the identity of the natural person who holds the position of senior managing official, and verify it. Other sectorial rules also have in place relevant provisions.

Criterion 10.11 - The AMLLIR (*Art. 7/2/c*) sets out provision which requires FIs to identify legal arrangement, and take reasonable measures to verify the identity of the

endower, beholder, the beneficiaries or classes of beneficiaries, and any other natural person exercising ultimate effective control over the legal arrangement.

Criterion 10.12 - The AMLLIR (*Art. 7/4*) provided due diligence requirement for beneficiary of saving and protection insurance policy and other investment related insurance policy. These requirements are commensurate with requirements of criterion 10.12. The Articles 15, 16 and 18 also covered relevant requirements.

Criterion 10.13 - The AMLLIR (*Art. 7/5*) stipulates that a financial institution, when determining whether enhanced due diligence measures are required in relation to a specific policy, shall take into account risk factors relating to the beneficiary of the policy and, if the financial institution considers that a beneficiary poses a higher risk, shall in all cases identify and verify the identity of the beneficial owner of the beneficiary at the time of payout.

Criterion 10.14 - The AMLLIR (*Art. 7/1*) stipulates that FIs shall undertake due diligence measures before establishing a new business relationship or opening a new account, and before carrying out transaction for occasional customer, and before carrying out a wire transfer with occasional customer. The AMLLIR (*Art. 7/1*) mirrored the requirement of the criterion 10.14.

Criterion 10.15 - The AMLLIR (*Art. 7/3*) mirrored the requirement of the criterion 10.15.

Criterion 10.16 - The AMLLIR (*Art. 7/7*) mirrored the requirement in criterion 10.16.

Criterion 10.17 - The AMLLIR (*Art. 7/14*) stipulates that financial institution shall determine the extent and depth of application of due diligence measures under Article 7 of the Law based on the types and levels of risk posed by a specific customer or business relationship. Where the risk of money laundering is higher, financial institutionn shall apply enhanced due diligence measures consistent with the risks identified. Other sectorial rules including RBME, MRMCB, RIC, RFC and RAP also set out requirements in this regard.

Criterion 10.18 - The AMLLIR (Art. 7/14) stipulates that financial institution shall determine the extent and depth of application of due diligence measures under Article 7 of the Law based on the types and levels of risk posed by a specific customer or business relationship. Where the risk of money laundering is lower, a financial institution or designated non-financial business and profession may conduct simplified due diligence measures provided there is no suspicion of money laundering, in which case simplified due diligence shall not be permitted. The simplified measures shall be commensurate with the lower risk. Other sectorial rules including RBME, MRMCB and RAP also set out requirements in this regard.

Criterion 10.19 - The AMLLIR (*Art. 7/8*) mirrored the requirement in criterion 10.19. Other sectorial rules for banks, money changers, financing companies, insurance companies, security companies also set out requirements in this regard.

Criterion 10.20 - The AMLLIR (Art. 7/9) mirrored the requirement in criterion 10.20.

Weighting and Conclusion

Saudi Arabia is compliant with R.10.

Recommendation 11 – Record keeping

In its 1st MER, Saudi Arabia was rated as compliant with R.10.

Criteria 11.1 - The 1st paragraph of the article 12 of the AMLL stipulates that FIs shall, for all domestic or international financial transactions as well as commercial and monetary transactions, keep all records and documents for a period of no less than ten years from the date of concluding the transaction or closure of account. Other sectoral rule including RBME for banks and money changers, RIC for insurance companies, RFC for financing companies and RAP for authorized persons also include relevant requirements.

Criteria 11.2 - The AMLL require FIs to keep all records obtained through due diligence measures, account files and business correspondences and copies of personal identification documents, including the results of any analysis undertaken, for at least ten years after the business relationship has ended or a transaction was carried out for a customer is not in an established business relationship. (*AMLL Art.12/2)*

Criteria 11.3 - The AMLL stipulates that records kept by FIs shall be sufficient to permit reconstruction of transactions and shall be maintained in a manner so that they can be readily made available to competent authorities upon request. (*AMLL Art.12/4)*

Criteria 11.4 - The AMLL stipulates that FIs shall keep records for a period of ten years and make them available to competent authorities upon request. (*AMLL Art. 13/4)*

Weighting and conclusion:

The AMLL obliged FIs, DNFBPs and NPOs to keep record documents for 10 years, which goes beyond requirement of FATF recommendation.

Saudi Arabia is compliant with R.11.

Recommendation 12 – Politically exposed persons

Saudi Arabia was rated PC on former R6 in last round mutual evaluation. Deficiencies noted in the last MER include incomplete definition of PEP, and inadequate requirements for financing companies and insurance companies.

Criteria 12.1 - The AMLL provides that FIs shall use appropriate systems to determine whether a customer or beneficial owner is or has become assignee with a prominent public function in the Kingdom or a foreign country; or with a senior management position in an international organization and if so, apply additional measures as prescribed by the Implementing Regulation. (*AMLL, Art.8)*

Article 8/1 of the IR of the AMLL provides that the person is or has become assignee with a prominent public function in the Kingdom or a foreign country; or with a senior management position in an international organization is consider as "politically exposed person (PEP)". This article also indicates that PEP includes heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, and important party officials,

directors, deputy directors, and members of the board or equivalent function, of any international organization.

Requirements established from (a) to (d) of Criteria 12.1 were covered in article 8/5 of IR of AMLL.

Criteria 12.2 - Article 8 of the AMLL and article 8/1 of its IR covered both foreign and domestic PEPs.

Criteria 12.3 - Article 8/2 provides that relevant obligations extend to family members and close associates. Article 8/3 sets out a definition of family member of a politically exposed person as any individual who is related to a politically exposed person by blood or marriage up to the second degree. Article 8/4 sets out a definition of close associate of a politically exposed person as any natural person who is known to have joint beneficial ownership of a legal entity or legal arrangement or who is in a close business relationship with the politically exposed person, or who has a beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of a politically exposed person.

Criteria 12.4 - Article 8/6 of the IR of the AMLL stipulates that FIs shall take reasonable measures to determine whether the beneficiaries or the beneficial owner from the saving and protection policy or any other investment insurance policy, before the payout of the policy prior to the exercising of any rights related to the policy, are PEPs, if so, the FI shall inform the senior management before the payout or prior to the exercising of any rights related to the policy, and conduct enhanced scrutiny on the business relationship, and consider making a suspicious transaction report.

Weighting and conclusion:

Saudi Arabia is compliant with R.12.

Recommendation 13 – Correspondent banking

Saudi Arabia was rated LC in last round of mutual evaluation on correspondent banking. The deficiency noted in last MER is that some banks did not seem to be implementing adequate due diligence towards correspondent relationships. This issue is now part of the effectiveness assessment.

Criteria 13.1 - The AMLL stipulates that FIs shall apply appropriate risk mitigation measures. Article 9/1 of the IR of the AMLL mirrored requirements in Criterion 13.1. (*AMLL, Art.9)*

The RBME (updated in 2012) defines correspondent banking and require banks and money exchangers to fully understand and appropriately document all the details of the respondent bank's management and nature of the business prior to opening any account. Banks should also determine from any available information (e.g., internet) whether the correspondent bank has been subject to any money laundering or terrorist financing investigations or regulatory action. Banks should also obtain certification of AML/CTF compliance for all correspondent relationships, which should include information including bank's basic information, AML/CFT supervisory framework of home country, policies and procedures of AML/CFT, KYC and STR, as

well as other relevant information. Correspondent bank accounts shall not be opened before the approval of the compliance officer in addition to that of the chief executive officer/director. Banks and money ex-changers are required to document the responsibilities of AML/CTF. (*RBME, paragraph 4.6.10)*

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. (*CDD Rules article 300.2.5*)

The MRMCB also sets out requirements on foreign correspondent banking covering the requirements of the Rec. 13. (*MRMCB art. 4.2)*

Criteria 13.2 - The RBME prohibits banks from dealing with any payable through account (RBME Art 13.3 (4.6.10), # (8)).

Criteria 13.3 - The article 9 of the AMLL stipulates that FIs shall not enter into or continue a correspondent relationship with a shell bank or a respondent institution that permits its account to be used by a shell bank.

Weighting and conclusion:

Saudi Arabia is rated Compliant for R.13.

Recommendation 14 – Money or value transfer services

Saudi Arabia was rated LC on former SRVI in last round of mutual evaluation.

Criteria 14.1 - All persons carrying out MVTS business are obliged to be licensed as a bank or class A money exchangers. All natural or legal person which carry out bank business are required to be licensed in accordance with this law, except legal persons licensed in accordance with other laws or special decree and licensed money changers (*BCL, Art.2*)

The Rules Governing Money Changing Business(*Decision of the Minister of Finance No. 1357 dated 01/05/1432H,*), sets out grandfathered rights for previously registered businesses to continue operating, as well as licensing procedures. .

Criteria 14.2 –The article 23.1 of the BCL stipulates that any person who carry out banking business without a license shall be liable to imprisonment for a term not exceeding two years and to a fine not exceeding RIs 5000 for every day the offenses continues or to either of these penalties.

According to the article 23 of RGMCB, SAMA shall undertake the prosecution against those who contravene the provisions of these Rules before the Committee referred to in Article 22 above for enforcement of the penalties set forth in the Banking Control Law.

Criteria 14.3 - The article 24 of the AMLL stipulates that supervisory authorities shall have the relevant powers and duties to carry out their mandate.

Article 25 provides that if supervisory authorities find FIs fail to comply with any provision of this Law, its Implementing Regulation or relevant decisions or circulars,

or any violation referred from other competent authority, the supervisory authority may impose one or more of measures set out in this article.

Criteria 14.4 and 14.5 - Banks and class A money changers are the only types of entities operating as MVTS providers in Saudi Arabia, and money changers do not use agents (only branches).

Weighting and conclusion:

Saudi Arabia is compliant with R.14.

Recommendation 15 – New technology

In its 1st MER, Saudi Arabia was rated largely compliant with R.8. The 2012 FATF recommendation set out new requirements which go beyond the former R8.

Criteria 15.1 – The AMLL stipulates that FIs shall include an assessment, prior to their use, of the risks associated with new products, business practices and technologies. Article 5/2 of the IR sets out the requirements on risk assessment relating to risk arising from the nature of products, services and transactions offered and the delivery channels for products and services. Sectoral rules for banks, money exchangers, financing companies, authorized persons detail specific requirements in this regard. (*AMLL, Art.5).*

At country level, the risk identification and assessment of new technology is absent in both NRAs provided.

Criteria 15.2 - The article 5 of the AMLL stipulates that FIs shall include an assessment, prior to their use, of the risks associated with new products, business practices and technologies.

The article 5/2 of the IR of the AMLL sets out requirements on risk assessment relating to risk arising from the nature of products, services and transactions offered and the delivery channels for products and services.

Weighting and conclusion

The Kingdom of Saudi Arabia has established comprehensive requirement for risk assessment at institutional level. However there is a gap regarding risk assessment at national level.

Saudi Arabia is largely compliant with R.15.

Recommendation 16 – Wire transfers

Saudi Arabia was rated PC on former recommendation SR VII. The major deficiency was that beneficiary FIs should be required to adopt effective risk-based procedures for identifying and handling wired transfers that are not accompanied by complete originator information. In Saudi Arabia, only banks and class A money changers carry out wire transfers.

Criteria 16.1 - The article 10 of the AMLL stipulates that FIs that provide wire transfer activities shall comply with all measures on wire transfers as set out in the IR.

The article 10/1 of the IR of the AMLL provides that Article 10 of the Law shall apply to cross-border wire transfers and domestic wire transfers in any currency, including serial payments and cover payments, which are received, or sent or processed by a financial institution in the Kingdom, including credit or debit or prepaid card, mobile phone or other digital or IT prepaid or post-paid device that are used to effect a person-to-person transfer of funds.

The article 10/2 of the IR of the AMLL provides that originator information shall include: (a) the full name of the originator; (b) the originator account number where such an account is used to process the transaction or in the absence of an account number, a unique transaction number that permits traceability of the transaction; and, (c) the originator's address, or customer identification, or date and place of birth. Beneficiary information shall include: (a) the full name of the beneficiary; and (b) the beneficiary account number where such an account is used to process the transaction or in the absence of an account number, a unique transaction number that permits traceability of the transaction.

The article 10/3 of the IR of the AMLL provides that financial institution that orders a wire transfer shall include required and verified originator information and required beneficiary information with each wire transfer.

Criteria 16.2 - Article 10/4 of the IR of the AMLL mirrored requirements of 16.2.

Criteria 16.3 -Saudi Arabia does not set out a *de minimis* threshold for wire transfer and apply the same requirements to all wire transfers.

Criteria 16.4 - Saudi Arabia does not set out a *de minimis* threshold for wire transfer and apply the same requirements to all wire transfers.

Criteria 16.5 - Article 10/5 of IR of AMLL provides that, for domestic wire transfers, the obligations set out in Article 10/3 shall apply unless the ordering financial institution is in a position to make all required originator and beneficiary information available to the financial institution ultimately receiving the wire transfer or competent authorities by other means, in which case the ordering financial institution may only include the account number or a unique transaction reference number that permits the transaction to be linked with the relevant originator or beneficiary information. The ordering institution shall make the required and verified originator and required beneficiary information available within three business days upon receiving a request for such information from the financial institution ultimately receiving the wire transfer or a competent authority.

Criteria 16.6 - See Criteria 16.5.

Criteria 16.7 - The 2nd paragraph of article 10 of the AMLL provides that financial institution shall record all originator and beneficiary information and keep the records, documents, data, and files in accordance with the article 12.

Criteria 16.8 - The article 10 of the AMLL stipulates that financial institution that is unable to obtain required originator or beneficiary information shall not permit the execution of the wire transfer.

Criteria 16.9 - The article 10/7 of the IR of the AMLL stipulates that, for cross-border wire transfers, a financial institution processing an intermediary element of the payment chain shall ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it, and shall keep all wire transfer

information including originator and beneficiary information in accordance with article 12 of the Law.

The paragraph 9 of article 5.1.2 of the RBME requires banks and money changers to make sure that all information related to the remitter and accompanied with wire transfer should be inserted with the transfer.

Criteria 16.10 - The article 10/8 of the IR of the AMLL provides that where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, the intermediary financial institution shall keep a record for ten years of all the information received from the ordering or other intermediary financial institution.

According to article 5.1.2 (10) of the RBME, and Article 3.2 (24) of the MRMCB, in the cases where technical restrictions prevent sending full information on the originator accompanying a foreign transfer with a domestic transfer related thereto (during the period necessary for the adaptation of the payment systems), the financial intermediary institutions receiving the transfer shall keep a record stating all the information received from the financial institution sending the transfer for a period of 10 years based on the AML/CFT rules issued by SAMA, taking into consideration the commitment for a period not exceeding (72 working hours) to respond to any inquiry received from the correspondent bank or the concerned authorities.

Criteria 16.11 - Article 10/9 of the IR of the AMLL stipulates that financial institution ultimately receiving or processing an intermediary element of a wire transfer shall have in place and apply procedures for (a) identifying wire transfers that lack required originator or beneficiary information; (b) determining, on a risk basis, when to execute, reject, or suspend a wire transfer that lacks required originator or required beneficiary information; and (c) taking appropriate risk based follow-up action which may include restricting or terminating the business relationship.

There is also general requirement provided by paragraph 4 of article 5.1.2 of the RBME for banks and money exchangers to ensure that full information is included.

Criteria 16.12 - See Criteria 16.11.

The paragraph 8 of article 5.1.2 of the RBME requires banks and money changers to take effective measures in case of wire transfers not accompanied with full information of originator. Above mentioned measures include: (1) to obtain missing information from the correspondent bank or the company providing transfer services and this applies to all local and international banks; (2) to reject the transaction and return the remittance in case of correspondent bank does not respond; (3) in case of suspicion in such a transaction and if correspondent bank does not respond, the case should be reported to the Financial Investigation Unit. The paragraph 18 of the article 3.2 of the MRMCB for money changers put in place similar provisions.

Criteria 16.13 - Article 10/10 provides that financial institution ultimately receiving a cross-border wire transfer shall take reasonable measures to identify cross-border wire transfers that lack required originator or beneficiary information. Such measures may include post-even monitoring or real-time monitoring where feasible. If the identity has not been previously verified, a financial institution ultimately receiving the transfer shall verify the identity of wire-transfer sender's information and maintain this information in accordance with Article 12 of the Law.

Criteria 16.14 - The Kingdom of Saudi Arabia does not set out a *de minimis* threshold for wire transfer and apply the same requirements to all wire transfers.

Criteria 16.15 - See Criteria 16.11. Based on article 10/9 of the IR, both ordering FIs and beneficiary FIs are obligated to (a) determining, on a risk basis, when to execute, reject, or suspend a wire transfer that lacks required originator or required beneficiary information; and, (b) taking appropriate risk based follow-up action which may include restricting or terminating the business relationship.

Criteria 16.16 - In Saudi Arabia, all persons carrying out MVTS business are obliged to be licensed as a bank or class A money changer, which are also obliged to implement requirements set out for wire transfers. Money changers do not use agents (see criteria 14.4).

Article 14/3 of the IR of the AMLL provides that where the anti-money laundering requirements of a foreign country are less strict than those imposed under the Law and this Implementing Regulation, financial institution shall ensure that its branches and majority-owned subsidiaries operating in that foreign country apply measures consistent with the requirements under the Law and this Implementing Regulation.

Criteria 16.17 – As banks and money changers are only two types of institutions carrying out MVTS service, its obligation on reporting suspicious transaction could cover part of requirement in this criteria. There is no explicit requirement however on institutions to file STR in any countries affected and make relevant information available to the FIU.

Criteria 16.18 - Articles 5.1.2. (19) of the RBME and 3.2. (32) of the MRMCB require banks and money exchangers check the names of originators and beneficiaries of wire transfers against lists of individuals and entities subject to asset freeze and take appropriate actions.

Weighting and conclusion

The only deficiency identified is the lack of requirement on institutions to file STR in any countries affected and make relevant information available to the FIU. This is a minor shortcoming.

Saudi Arabia is largely compliant with R.16.

Recommendation 17 – Reliance on third parties

Saudi Arabia was rated LC on former R 9 in last round mutual evaluation.

Criterion 17.1 - The AMLLIR (*Art. 7/10*) allow FIs to rely on another financial institution or designated non-financial business and profession to perform identification and verification of the customer; identification and verification of the beneficial owner; and to take the necessary measures to understand the nature and intended purpose of the business relationship.

The AMLLIR (*Art. 7/11*) provides that, if FIs rely on third parties as stated above, they shall do the following: (a) immediately obtains all necessary information as required under article 7 of the Law and this Implementing Regulation; (b) take measures to satisfy that copies of identification data and other relevant documentation relating to

the due diligence measures will be made available , and without delay; (c) ensure that financial institution or designated non-financial business and profession relied upon is regulated, supervised for and has measures in place for compliance with due diligence and record keeping requirements in line with the requirements stipulated under the Law and this Implementing Regulation. (d) take into account information available with (AMLPC) and the Directorate of Financial intelligence with regard to high-risk countries identified. The ultimate responsibility of all requirements stipulated in this law and its implementing regulation relay on the requesting financial institution and designated non-financial business and profession.

Criterion 17.2 - See criterion 17.1.

Criterion 17.3 - The AMLLIR (*Art. 7/13*) stipulates that financial institution relies on third party that is part of the same financial group may consider that the financial institution or designated non-financial business and profession relied upon meets the requirements on due diligence and record keeping requirements in line with the Law and this Implementing Regulation, the implementation of such policies is supervised at the group level by a competent authority and any higher country risk is adequately mitigated by the group's policies and controls.

Weighting and conclusion

Saudi Arabia is compliant with R.17

Recommendation 18 – Internal controls and foreign branches and subsidiaries

Saudi Arabia was rated LC for both former R15 and R22. Deficiencies identified with respect to technical compliance are the independence and adequate resourcing of the audit function not explicitly provided for in case of insurance and securities companies.

Criterion 18.1 - The AMLL (*Art. 14*) require FIs to have in place and effectively implement internal policies, procedures and controls against money laundering aimed at managing and mitigating any risks identified as clarified in Article 5. The policies, procedures and controls shall be proportionate to the nature and size of the FI and DNFBP's business and shall be approved by senior management. FI and DNFBP shall review and enhance them as needed. Financial institution are also required to apply its internal policies, procedures and controls said in (A) of this Article, to all of its branches and majority-owned subsidiaries.

The AMLLIR (*Art.14/1*) stipulates that the policies, procedures and internal controls shall be proportionate to the nature and size of the FIs business and shall address the following: (a) due diligence measures as required under this law and its Implementing Regulation, including risk management procedures for utilization of a business relationship prior to completion of the verification process; (b) transaction reporting procedures; (c) appropriate anti-money laundering compliance management arrangements, including appointment of an anti-money laundering compliance officer at the senior management level; (d) adequate screening procedures to ensure high standards when hiring employees; (e) ongoing employee

training programs; and (f) An independent audit function to test the effectiveness and adequacy of internal policies, controls and procedures.

Moreover, other enforceable means including RBME, MRMCB, RIC, RFC and ARP set out detailed requirements for banks, money changers, insurance companies, financing companies and authorized persons.

Criterion 18.2 - See criteria 18.1. In addition, the AMLLIR (*Art. 14/2*) stipulates that financial group shall implement a group-wide program against money laundering, apply the internal policies, controls, procedures to all of its branches and majority-owned subsidiaries and ensure effective implementation thereof by all branches and majority-owned subsidiaries. In addition to the issues set out in subsection 14/1, a group level policy shall address also the sharing of information between all members of the group; the provision of customer, account and transaction information to group-level compliance, audit or anti-money laundering functions; and the safeguarding of confidentiality and use of the information exchanged.

Criterion 18.3 - The AMLLIR (*Art. 14/3*) stipulates that where the anti-money laundering requirements of a foreign country are less strict than those imposed under the Law and this Implementing Regulation, financial institution shall ensure that its branches and majority-owned subsidiaries operating in that foreign country apply measures consistent with the requirements under the Law and this Implementing Regulation. If the foreign country does not permit the proper implementation of such measures, financial institution shall inform the Saudi supervisory authority of this fact and take any additional measures necessary to appropriately manage and mitigate the money laundering risks associated with its operations abroad. The financial institution shall comply with any instructions received from the supervisory authority in this regard.

Weighting and conclusion:

Saudi Arabia is compliant with R.18.

Recommendation 19 – Higher-risk countries

Saudi Arabia was rated PC in this regard. The technical deficiencies noted in the last MER were: (a) the absence of counter measures; (b) insufficient guidance regarding what is required of institutions with respect to identifying those countries that do not sufficiently apply the FATF Recommendations.

Criterion 19.1 - Article 11 of the AMLL stipulates that FIs shall apply enhanced due diligence measures proportionate to the risks involving business relationships and transactions with a person from a country that was identified as high risk by the FI or DNFBP or the Anti-Money Laundering Permanent Committee. The AMLPC has issued a list of high risk countries on its webpage that includes all FATF listed countries and is updated after every plenary (through a direct link to the FATF website).

Several sectoral rules including RBME, RIC, RFC and RAP also have in place similar requirements.

Criterion 19.2 - The AMLL stipulates that FIs shall apply the countermeasures prescribed by the Anti-Money Laundering Permanent Committee with respect to high

risk countries and the AMLPC has issued a list including all FATF designated countries and updates that list after every plenary *(AMLL, Art.11).*

Criterion 19.3 - The financial sector under the supervision of SAMA is kept aware of high risk countries by disseminating circulars after each of the FATF meetings and which include the high risk countries and the way to deal with them. Circular was also sent to all financial sectors focusing on the importance of keeping abreast of relevant websites including the FATF website.

Weighting and conclusion

Saudi Arabia is compliant with R.19.

Recommendation 20 – Reporting of suspicious transactions

Saudi Arabia was rated Largely Compliant with the Recommendation 13 in its MER published in 2010.

Criterion 20.1 - The AMLL (*Art. 15.1*) obliges FIs (defined in Article 1-5 as any institution in the Kingdom engaging in one or more banking activity, money transfer, currency exchange, investment, securities, insurance and financing) to notify the FIU immediately upon suspicion or in case of any reasonable grounds to suspect that the money or some of it represents the proceeds of criminal activity (defined as any activity constituting a crime punishable by Sharia or law) or is associated with or related to money laundering whereas Article 70.2 of the CFTL obliges the aforementioned entities if they believe that funds or parts thereof are related or linked to or be used for financing of terrorism, including attempts to initiate such a transaction amounts. Furthermore, Article 15.2 from AMLL and Article 70.2 from CFTL obliges financial institutions to provide the FIU with any required additional information after notifying the FIU of the suspicious transaction related to money laundering or terrorist financing. The Implementing Regulations (IR) of the Law provides that reporting can be made as a result of suspects or has reasonable grounds to suspect that any of the complicated, high-volume, or suspicious transaction that relates to money laundering, the AMLIR as well in Article 15.2 state that a financial institution, designated non-financial businesses and professions, or NPO shall implement indicators of suspected acts of money laundering. These indicators shall be updated on a continuous basis according to the development and diversity of methods used to carry out such acts, while complying with the publications of supervisory authorities in this regard.

SAMA Rules governing AML/CFT specify that the covered FIs, i.e. banks and currency exchangers are required to mandate their employees to do the following (Article 4.8.1):

1. If an employee suspects that a money laundering transaction is taking place, he/she should immediately report it to the bank or money exchanger's internal MLCU or designated Compliance Officer.

2. Attempts of suspicious transactions, which have been identified as suspicious but were foiled before occurrence, must be reported.

3. Banks and money exchangers should make available, to the appropriate authorities all documents, statements and related transactions.

Article 4.8.2 of the said Rules provides for the details of the reporting mechanism. Such details come to replicate that in the IR. A new requirement was added to "*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*."

The Insurance Supervision Department at SAMA issued the Anti-Money Laundering and the Combating Terrorist Financing Rules in 2013. Paragraph 42 tackles reporting and mandates insurance companies to immediately notify FIU about any complex, huge, or unnatural activity or transaction, any suspicious transaction in terms of its objectives, any activity or operations that is or might be related to financing a criminal activity, terrorism, terrorists or terrorist organizations. The company must submit a copy of the notification to its insurance control department. The Insurance Rules urged insurance companies to file suspicious reports regardless of their relation with any other cases. Also, sending a follow-up STR was encouraged.

Likewise, Paragraph 7 of the Rules issued to financing companies provide for prompt reporting to the FIU regardless of the amount.

Criterion 20.2 - Article 15 of the AMLL and 70 of the CFTL require FIs to report all suspicious transactions including attempted transactions regardless of the amounts. See above criterion.

Weighting and conclusion

Saudi Arabia is compliant with R.20

Recommendation 21 – Tipping-off and confidentiality

The Rating of Recommendation 14 in the MER published in 2010 was compliant

Criterion 21.1 - The Article 16.2 of the AMLL & Article 71.2 of the CFTL stipulate that "Financial institutions, DNFBPs, and NPOs as well as their Members of Board of Directors, Directors, Members of its executive or supervisory management, and employees shall be protected from any liability toward the reported if they report their suspicions to the Directorate in good faith" the AMLIR echoes that FATF methodology that The protection under Article 16 of the Law shall include protection from any criminal, civil, contractual, disciplinary or administrative liability and applies also in situations where the financial institution or designated non-financial business and profession or its employees or directors did not know precisely what the underlying criminal activity of the reported transaction was and regardless of whether illegal activity actually occurred.

Criterion 21.2 - Article 16.1 of the AML LAW and Article 71.1 from CFT LAW stipulates that " FIs, DNFBPs, and NPOs as well as their Members of Board of Directors, directors, Members of its executive or supervisory management, and employees are prohibited from disclosing to a customer or any other person the fact

that a report under this Law or related information will be, is being or has been submitted to the Directorate, or that a criminal investigation is being or has been carried out. This shall not preclude disclosures or communications between directors and employees or communications with lawyers or competent authorities

Article 4.8.3 of SAMA AML/CFT regulations reiterate the confidentiality of the STR process as they provide that 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. AML/CFT regulations on insurance as well provide for this confidentiality, as intermediaries should "treat all data and information acquired about the insurance company and clients with utmost confidentiality, and take appropriate measures to maintain the secrecy of confidential documents in their possession"

Article 29 of LTCF helps maintain the confidentiality of information regarding the reporting, inquiry, investigation or trial procedures, or of data related thereto, in respect of any of the crimes set forth in this Law information. Such information may not be disclosed except for the use of the competent authorities.

Weighting and conclusion

Saudi Arabia is rated compliant with R.21

Recommendation 22 – DNFBPs: Customer due diligence

The rating of Recommendation 12 in the MER published in 2010 was Non-Compliant.

Criterion 22.1 - DNFBPs in Saudi Arabia are set out in Article 1/3 of the AMLL Implementing Regulations and include all the required categories of activity. Casinos, in their entirety, are prohibited as they are against Sharia law. Notaries are civil servants who work for the government.

TCSPs are not recognised as a separate profession in Saudi Arabia, but they are partially included in the requirements through the application of the AMLL to "*attorneys or any person providing legal or accounting type services in the exercise of professional activities, when they prepare, execute, or conduct a transaction for customers in relation to any of the following activities: ... iii. Establishment, operation, or management of legal persons or legal arrangements and the organization of related subscriptions; or iv. Sale or purchase of commercial companies.*" (AMLLIR, Art.1/3). Some activities remain outside the scope of the AMLL, including providing a registered office; and acting as a trustee or nominee, but those are not admissible activities in Saudi Arabia.

Criterion 22.1 (a) - Saudi Arabia prohibits Casinos and gambling as they are contrary to Sharia law.

Criterion 22.1 (b, c and d) - The AMLL and its regulations set out the same CDD requirements for FIs and DNFBPs. Based on the detailed assessment of R.10, above, Saudi Arabia applies all the relevant requirements to DNFBPs (*AMLL Art.7; AMLLIR Art.7/1, 7/2*)

Criterion 22.1 (e) - TCSPs are not recognised as a separate profession in Saudi Arabia, but they are partially included in the requirements through the application of the AMLL (please refer to 22.1 above). Services relating to the formation and operation of a waqf are provided by lawyers, and as such they would be covered by the AMLL.

Criterion 22.2 - Record keeping obligations are set out in Articles 12 of the AML Law, its IRs, and Article 65 of the LTCF. Based on the detailed assessment of R.11, above, Saudi Arabia applies all the relevant requirements to DNFBPs.

Criterion 22.3 - Based on the detailed assessment of R.12, above, Saudi Arabia applies all the relevant requirements to DNFBPs

Criterion 22.4 – The requirements relating to new technologies are provided for under Article 5/6 of the AMLLIRs. Based on the detailed assessment of R.15, above, Saudi Arabia applies most requirements to DNFBPs, but the same minor shortcoming identified under R.15 also applies to DNFBPs: that there is a gap regarding risk assessment of new technologies at national level.

Criterion 22.5 - Based on the detailed assessment of R.17, above, Saudi Arabia applies all the relevant requirements to DNFBPs.

Weighting and Conclusion

There is one minor deficiency regarding the risk assessment of new technologies:

Saudi Arabia is largely compliant with R.22

Recommendation 23 – DNFBPs: Other measures

The rating of Recommendation 16 in previous MER was Non-Compliant.

Criterion 23.1 a to c - Designated non-financial businesses and professions, must immediately and directly report such transactions to the Financial Intelligence Unit when suspect or have reasonable grounds to suspect that funds or parts thereof are proceeds of a criminal activity or are related to money laundering, financing of terrorism, acts of terrorism, terrorist organizations, terrorist financiers, or if such funds - regardless of their amounts - will be used in acts of money laundering, financing of terrorism, acts of terrorism, terrorist organizations or terrorist financiers, including attempts to initiate such transactions. Both MOCI and MOJ manuals support this reporting requirement. (*AMLL, Art.15, CFTL, Art.70)*

Criterion 23.2 - Based on the detailed assessment of R.18, above, Saudi Arabia applies all the relevant requirements to DNFBPs. (*AMLL Art.14).*

Criterion 23.3 - Based on the detailed assessment of R.19, above, Saudi Arabia applies all of the relevant requirements to DNFBPs *(AMLL, Art. 11, CFTL, Art.66).*

Criterion 23.4 - Based on the detailed assessment of R.21, above, Saudi Arabia applies all the relevant requirements to DNFBPs. **(**AMLL Arts.11, 28; CFTL Art.20).

Weighting and conclusion

Saudi Arabia is compliant with R.23

Recommendation 24 – Transparency and beneficial ownership of legal persons

Saudi Arabia passed a Companies Law (CL) on 4 December 2015, effective on 2 May 2016, which has replaced the previous Company Law 1965. The commercial entities that can be created in Saudi Arabia under the current CL are the following:

- Unlimited liability company
- Joint-stock company
- Limited liability company
- Limited partnership
- Unlimited (silent) partnership[33]

Foreign companies can establish business as companies operating in Saudi Arabia, whether through a branch, office, agency or any other form; and companies having a representative office in Saudi Arabia to direct or co-ordinate activities they conduct outside Saudi Arabia (CL, Art.194). Foreign companies are considered an extension of the parent company, and their activities are limited to providing technical information and assistance regarding the foreign company's products to its Saudi distributor(s) and to end users of the products, studying and reporting on the market and conducting research.

The Law on Civil Associations and Foundations (NPO Law) allows for the creation of **Civil Society Associations** and **Civil Society Organisations** (comprising Family and Private funds).

Criterion 24.1-

In addition to the relevant legislation, there are mechanisms that publicly identify and describe information on legal persons that can be created in Saudi Arabia. The CL and the NPO Law identify and describe the different types, forms and basic features of legal persons in Saudi Arabia, as well as the process for the creation of legal persons and for obtaining and recording basic information. A website, available from Saudi Arabia only, provides information on the registration and establishment process for each type of entity, and the general features of each legal entity. The MLSD presents on its website, available only from Saudi Arabia, information about the creation and features of Associations and Civil Society Organisations (https://dp.mlsd.gov.sa). A

33 Unlimited (silent) partnerships are contracts which have legal effects only between partners and do not constitute a separate entity vis-á-vis third parties. Unlimited (silent) partnerships are not legally disclosed to third parties, are not subject to public identification and do not enjoy legal personality (CL, art.43). In case a third party is disclosed the existence of the partnerships, the rules applicable to Unlimited Liability Companies apply (CL, Art.48). In addition, partnerships may be formed under Islamic jurisprudence (Islamic Partnerships) without separate legal personality. These partnerships are not considered for the purposes of R.24, though they are considered under Immediate Outcome 5 as legal arrangements.

website (www.aamal.sa) is being developed and presents information in relation to commercial entities in Arabic.

Beside relevant legislation (see below c.24.6), there is no publicly available mechanism that would identify and describe the processes for obtaining and recording beneficial ownership information.

Criterion 24.2 -

The NRA for ML addressed the exposure of commercial legal persons to misuse for money laundering. The authorities have a high-level understanding of how the measures in place to register companies and verify the ownership would prevent the exposure of legal entities to money-laundering. However, their assessment of the ML/TF risks associated with all types of legal persons created in Saudi Arabia does not sufficiently address how all commercial legal persons may be misused to perpetrate ML or TF (see Immediate Outcome 5). The NRA for TF did consider the risk associated with legal persons, including NPOs, and concluded that the risk is low. With regard to NPOs, the risk associated with ML is also considered to be low in the light of the requirements imposed on the sector.

Criterion 24.3 -

Commercial legal entities are required to be registered in the Company Register, within the Ministry of Commerce and Investment (Law of Commercial Register (LCR), Art.3 and 6; and CL, Art.43). Registration must be performed by the manager of the legal entity within 30 days of the date on which the articles of association/incorporation are recorded by the notary public.

When registering with the Commercial Register, Saudi legal entities must deposit a copy of the articles of associations and bylaws. The type of information included in the articles of association varies from each entity; in general, they include basic information related to the entity. The Company Register must also receive and record basic information about the entity, such as the entity name and legal type, the address of the head office, the names of the managers and the names and address of the general partners in Limited partnerships and Unlimited liability partnerships (LCR, Art.3). Entities acquire legal personality upon registration in the Commercial Register (CL, Art.14).

Foreign companies[34] must register information on the branch or office in Saudi Arabia with the Commercial Register within 30 days of the date of its opening (LCR, Art.6). They must obtain a licence from the Saudi Arabian General Investment Authority (SAGIA) and SAGIA will provide the Commercial Register with a copy of the licence as well as a certified copy of the articles of incorporation and articles of association (CL, Art.196). The content of these documents will depend on the laws of the jurisdiction of incorporation.

Basic information about legal entities registered with the Commercial Register can be accessed by the public (LCR, art.11).

34 Companies operating in the Kingdom, whether through a branch, office, agency or any other form; and companies having a representative office in the Kingdom to direct or co-ordinate activities they conduct outside the Kingdom.

Civil Society Associations and Civil Society Organisations must obtain a licence from and register with the Ministry of Social Affairs (NPO Law, art.6 and 34). An application for registration of a Civil Society Association must be made to the Ministry containing a copy of the charter (NPO Law, art.8). The charter of an Association must contain basic information such as, name of the entity, internal governance structure, number of the managers ("board of directors"), main office, as well as names and addresses of the founders, purpose of the association, and members' rights and duties. The names of the directors must be communicated to the Ministry, including updates (NPO Law, Art.31). Civil Society Organisations should be registered with the Ministry of Social Affairs as this is required to maintain a register for organisations, in accordance with the relevant Regulations setting fort the registration procedures and required data (NPO Law, art.34). The names of the "board of trustees" (management) should be notified to the Ministry (NPO Law, art.31).

Criterion 24.4 -

Joint-stock companies are required to maintain a register of shareholders, indicating the shareholders' names, places of residence, numbers of shares and paid amounts (CL, Art.109). The preparation of the register of shareholders can be outsourced. Transfers of ownership are valid vis-á-vis the company or a third party from the date of entry into said register. Companies must report to the Commercial Register the type, value and number of shares upon incorporation and following any amendment thereto (CL, Art.65(2) and CRL, Art.4). The register of shareholders must be kept in at the company's address in Saudi Arabia (Ministerial Resolution, art.7).

Limited liability companies must maintain a special register of names of partners, number of shares owned by each and actions taken thereon (CL, Art.162). The articles of association must include the name and address of the partners, the amount of capital in cash or in-kind, address of the head office, and names of the supervisory board (CL, Art.156). The articles of association and any amendments must be communicated to the Commercial Register (CL, Art.158). The company must also notify the Ministry of Commerce and Investment of any ownership change (CL, Art.162). Change in ownership takes legal effect after registration in the Commercial Register. The register of partners must be kept in Saudi Arabia (Ministerial Resolution, art.1).

Unlimited Liability Companies are required to keep information under 24.3 as well as information on their owners (partners who are natural persons). The articles of incorporation of Unlimited Liability Companies must include the name and address of all partners, the names of any director as well as the company's capital and the equity of each partner (CL, Art.23). Any change to ownership must be approved by all other partners (CL Art.19). Unlimited liability companies must inform the Commercial Register of any change to the articles of incorporations or the ownership (CL, Art.19 and 22).

Limited partnerships are required to maintain a register of partners, including limited partners, and other basic information about the partnership. Limited partnerships are required to provide the Commercial Register with the information on the general partners upon incorporation and following any amendment (CLR, Art.3 and 4), but not limited partners. Limited partners can transfer their shares to any other partner in the limited partnership, and may also transfer the shares to a third party with the consent of the general partners (CL, Art.41).

Foreign companies do not have to maintain ownership and other basic information in Saudi Arabia under the CL. The relevant obligations to maintain such information would depend on the requirements of the jurisdiction of incorporation.

Civil Society Associations and **Civil Society Organisations** are required to maintain the information under 24.3, as well as the names of the founders and the members (NPO Law, art.21, 30, 37).

Criterion 24.5 -

The merchant, the manager of the company or the liquidator of legal entities must update any amendment to the information already provided to the Commercial Register within 30 days of the date of amendment. This includes amendment to basic information about all the entities registered in the commercial register as well as legal ownership information on Limited liability companies and Unlimited Liability Companies. Other commercial entities must update the information they hold.

The Ministry of Commerce and Investment is the competent authority to supervise the implementation of the CL (CL, Art.220), except for joint-stock companies that are listed on the stock market for which the supervising authority is the Capital Market Authority (CL, Art.219). Within the Ministry of Commerce and Investment, the General Administration of Companies Department (GACD) is responsible for verifying the information provided to the Commercial Register. Among others, Saudi Arabia indicates that the GACD verifies the identity of the owners and managers via security verification system and passport control, and the capital deposited by the company and the percentage of each shareholder/partner in the company. For Associations and Organisations, supervisory authorities are designated to approve their establishment and monitor their activities (NPO Law, Art.5).

Criterion 24.6 -

Saudi Arabia uses various mechanisms to obtain or determine the beneficial ownership of legal entities, although these may not be sufficient to ensure the availability of beneficial ownership information as defined by the FATF in all cases.

The Ministerial Resolutions issued on 14 November 2017 require Joint-Stock Companies not listed on the stock-market, Limited Partnerships and Limited Liability Companies to maintain a register of beneficial ownership and to provide it to the Company Register. The register should record identifying data regarding all natural persons to whom the ownership of the company belongs indirectly, as well as these data for all natural persons who engage in the management of legal persons having shares in the legal entity, whether the ownership of the legal person is direct or indirect (Ministerial Resolution, art.3 and 8). This requirement is coherent with the FATF definition of Beneficial Owner. The individual owners of the company/partnership are responsible for providing the company/partnership with this data, as well as with any update within 10 days (Ministerial Resolution, art.4 and 9). The register should be sent to the Company Register within 15 days following incorporation and within 15 days following any amendment thereto (Ministerial Resolution, art.5 and 10).

The Company Register within MOCI receives information on the legal owners of Unlimited Liability Companies, whose partners can only be natural persons (CL, Art.17). The company itself holds basic and legal ownership information. Where there

is no straw man involved, the information on legal ownership would be sufficient to identify the beneficial owner of those companies. When any company registers with MOCI, Public Notaries (who are government officials) must authenticate the articles of associations and any amendment, adding a verification measure to control and ownership information. Foreign companies must apply for a business licence to SAGIA before conducting business in Saudi Arabia, and SAGIA requires the provision of ownership and control structure. For foreign investors, Saudi Arabia indicated that SAGIA compiles information about the investors through the applicant itself and foreign Saudi embassies, and parts of the collected information is made available to the Commercial Register.

Beneficial ownership information would be available with FIs and/or DNFBPs if and when a legal person establishes a relationship with a reporting entity. The identification of the beneficial owner of these legal persons should occur through implementation of the CDD measures, which require reporting entities to identify and take reasonable steps to verify the beneficial ownership of legal entities (see analysis in c.10.3, 10.5, and 10.10). Joint-stock companies and limited liability companies are obliged to have a bank account in Saudi Arabia at the time of incorporation to prove that their capital/share equity has been paid (CL, Art.59, 64, 65, and 157). For Joint-Stock Companies listed on the stock-exchange market, all investors must have an account with an Authorised Person, who is a reporting entity and subject to CDD requirements in relation to the investor. Civil Society Associations and Civil Society Organisations must deposit cash received in a bank account (NPO Law, Art.21), although the AML/CFT legislation does not provide guidance on who is the beneficial owner of these entities. Other legal persons do not have an obligation to have a continuous relationship with a reporting entity in Saudi Arabia.

In sum, beneficial ownership information for Joint-Stock Companies not listed on the stock exchange, Limited Partnerships and Limited Liability Companies is required to be maintained by the entity and provided to the Company Register with effect from November 2017. Investors in Joint-Stock Companies listed on the stock-exchange market must always rely on an Authorised Person who must identify the beneficial ownership information of that person. Civil Society Associations and Organisations must have a bank account in Saudi Arabia and the BO would be identified by the relevant financial institution, although the AML/CFT legislation does not provide guidance on who is the beneficial owner of these entities. Foreign companies must provide ownership and control structure information to SAGIA when applying for a business licence. For Unlimited Liability Companies, the availability of beneficial ownership information would be available to the Company Register where there is no straw men involved and to FIs/DNFBPs when they have a relationship with any of them.

Criterion 24.7 -

Joint-Stock Companies not listed on the stock-market, Limited Partnerships and Limited Liability Companies should maintain a register of beneficial ownership and provide it to MOCI (Ministerial Resolution, art.3 and 8). The individual owners of the company/partnership are responsible for providing the company/partnership with this data, as well as with any update within 10 days (Ministerial Resolution, art.4 and 9). The register should be sent to the MOCI within 15 days following incorporation

and within 15 days following any amendment thereto (Ministerial Resolution, art.5 and 10).

When the availability of beneficial ownership is ensured through the relationship with a FI/DNFBP, which is compulsory only for investors in Joint-Stock Companies listed on the stock market and for Civil Society Associations and Civil Society Organisations, the beneficial ownership information will be updated in accordance with the risk-profile of the client or in the process of scrutinising transactions (see c.10.7). This would mean that the beneficial ownership information would be updated depending on the intensity of the reviews conducted by the reporting entity, but would not necessarily be as up-to-date as possible as required by c.24.7.

Criterion 24.8 -

Saudi Arabia has identified mechanisms that ensure that companies co-operate with the competent authorities to the fullest extent in determining the beneficial owner in most cases. Managers of all entities are responsible in front of the competent authorities for the entity's actions and activities and must give access to the representatives of the Ministry of Commerce and Investment and/or to the Capital Market Authorities all relevant information (CL, Art.220 and 221). Even where the managers are not in Saudi Arabia, the company must have an office in Saudi Arabia and would be able to provide assistance to the authorities. For Joint-Stock Companies not listed on the stock-market, Limited Partnerships and Limited Liability Companies, the beneficial ownership information should be kept in the register at the company's office in Saudi Arabia (See above). Even where there is no obligation for entities to hold, and for managers to know, beneficial ownership information of the entity, the managers will be obliged to identify the FI/DNFBP, in Saudi Arabia or abroad, who should hold it.

Financial institutions and DNFBPs are obliged to provide information on their clients (including BO information) to the AML/CFT supervisory authorities, who will then be able to transmit it to the FIU, investigative authorities, and judicial authorities (AMLL, Art.10). However, except for investors in Joint-Stock Companies listed on the stock market and Civil Society Associations and Civil Society Organisations, there is no obligation on other legal entities to have a continuous relationship with an FI/DNFBP, neither in Saudi Arabia nor abroad.

CMA would be able to obtain information on all the investors in Joint-Stock companies listed on the stock exchange market from the Authorised Person. Unlimited Liability Companies, Joint-Stock companies, and Limited Liability Companies must have their accounts audited annually by a licensed auditor (a DNFBP), who should collaborate with the authorities if needed.

Criterion 24.9 -

All persons, authorities and entities mentioned under R.24 must maintain documents and records of the legal persons. The CL does not specify for how long legal entities must keep information about the entity and ownership information. Liquidators must keep all documents and information related to the entity for ten years after liquidation (Explanatory Note No. 10/100/2 of the Committee of Job Ethics at SOPCA, of 22/5/1999). Commercial entities must keep "commercial books" (original day book, inventory book, and the ledger), together with all correspondence and

documents that are related to the business/entity for ten years (Regulation of the Commercial Books, Art.8). MOCI must also keep all documents for ten years.

Information, including CDD and BO information, held by FIs/DNFBPs must be kept for ten years (AML Law, Art.6 and LTCF, Art.39).

Criterion 24.10 -

The Ministry of Commerce and Investment has direct access to all information available in the Commercial Register. The Ministry of Commerce and Investment also has the powers to obtain information from commercial legal entities for the purpose of monitoring compliance with the provisions provided in the CL, including the powers to inspect the company and its accounts (CL, Art.221). The Capital Market ***Authority*** has these powers to access information from companies listed on the stock market.

Supervisory, law enforcement, investigative, and FIU authorities can access information from the Commercial Register only through the GACD within the Ministry of Commerce and Investment. The information in the Commercial Register should be available online to the public as soon as the website www.aamal.sa is fully operative. They can obtain information directly from legal entities in accordance with their powers, as described in R.31.

The Ministry of Labour and Social Development is responsible for overseeing the activities of Associations and Organisations and for monitoring them administratively and financially (NPO Law, Art.4 and 5). The Regulations specify relevant rules (see R.8).

Criterion 24.11 -

Joint-stock companies can only issue nominal shares (CL, Art.105), therefore bearer shares are not permitted under the current Saudi legislation.

Criterion 24.12 -

The commercial legislation in Saudi Arabia does not provide for the concept of nominee shareholding or nominee directorship, but nothing prevents shares from being held by a nominee (e.g. on behalf of someone else) or directorship positions from being controlled by someone else. The CL recognises the rights and responsibilities of the legal owners and of the managers indicated in the relevant corporate documents. A nominee relationship could then be only created through a separate private contract between the nominee shareholder/director and the other party. It is unclear whether this contract would indicate the details of the parties involved.

Criterion 24.13 -

Chapter 11 (notably articles 211, 212, and 213) of the CL provides for penalties for violations of the provisions of the CL. Any person who intentionally includes false information in the company's articles of association/incorporation or other documents is subject to imprisonment for maximum one year and a fine of a maximum of SAR 1 million (approximately EUR 220 000) (CL, Art.212(f)). Any person who fails to publish the company's articles of incorporation or fails to enter it in the commercial register in accordance with the Law, or to register any amendments is subject to a penalty of SAR 500 000 (approximately EUR 110 000) (CL, Art.213(n)).

There are penalties for failure to keep the register of shareholders of JSCs and register of partners of LLCs (CL, Art.211(r), and the company is liable towards the shareholders/partners and there are penalties up to SAR 500 000 for failure to grant access to the company's documents (CL, Art.213(j and m)) and for irregularities in distributing dividends (CL, Art.213(a)). Penalties up to SAR 500 000 can also be applied to any person who fails to comply with regulations and resolutions related to the company's business and activities (CL, 213(n)). These provisions together ensure that there are sanctions on legal and natural persons who do not maintain the basic and legal ownership of commercial entities.

Joint-Stock Companies not listed on the stock-market, Limited Partnerships and Limited Liability Companies must maintain beneficial ownership information and provide it to MOCI (see c.24.6 above). The shareholders of the entity are responsible for providing and updating this information to the entity. The entity is then responsible for providing the BO information to MOCI. There are sanctions for failing to provide this information to the entity and/or to the MOCI (CL, Art.211(r)).

There are sanctions for persons who do not provide the Ministry of Commerce and Investment with access to documents and information regarding commercial entities. Fines up to SAR 500 000 can be applied to any person who neglects to perform his duty to provide the Ministry with the documents set forth in the Law (CL, Art.213(k)).

In case of recidivism, the penalties for the offences and violations stipulated in Articles 211, 212, and 213 of the CL are doubled (CL, Art.214). Recidivist is a person who commits the same offence or violation within three years. Offences under Articles 211 and 212 of the CL are investigated by the Public Prosecution (PP). Fines for violations provided under Article 213 of the CL can be imposed directly by the Ministry of Commerce and Investment or Capital Market Authority, and the fined person can appeal to the competent judicial authority (CL, Art.216). Imposition of any fine does not preclude the right of any person to claim compensation (CL, Art.218).

Some basic and legal ownership information on commercial entities is maintained by the Commercial Register. Any violation to provide or update information to the Commercial Register can be punished with a fine from SAR 5 000 to SAR 50 000 (LCR, Art.15). The Ministry of Commerce and Investment is responsible for assigning the penalty. In assigning the penalty, consideration will be made to the seriousness of the violation, its recurrence, the merchant's capital, and the damage caused to others.

Beneficial ownership information on legal entities must be maintained by the FI/DNFBP with which the legal entity has a client relationship or conduct a transaction with a FI/DNFBP. Sanctions apply to reporting entities for violation of the AML/CFT legislation (see R.35).

With regards to Associations and Organisation, violations of the Implementing Regulations and bylaws are dealt with by Ministry of Labour and Social Development. The Ministry will warn the entity providing a timeline for remedy and then may suspend any of the members, remove the board of directors, dissolve the entity or merge it with another one (Implementing Regulations of the NPO Law, Art.87).

Criterion 24.14 -

Saudi Arabia can provide international co-operation in relation to basic and beneficial ownership information. Access to information held in the commercial registry is

available to the public upon submission of a request to the Commercial Register. The Commercial Register contains information on the owners of some types of commercial entities. A website provides information on the registration and establishment process for each type of entity, and the general features of each legal entity however this is only available from Saudi Arabia. At the website www.aamal.sa, some basic information on companies is available online. Foreign authorities can access directly the Commercial Register to search for detailed information from abroad. This does not include updated information on the shareholding. When information on the owners needs to be accessed directly from the entities, the Ministry of Commerce and Investment can access it for the purpose of the implementation of the provisions of the CL. The investigative authorities, as well as the FIU, can obtain basic and beneficial ownership information, also for the purpose of exchanging it with foreign counterparts, with the limitations described in R.31, R.37, and R.40.

Criterion 24.15 –

Saudi Arabia did not provide detailed information on how it monitors the quality of assistance received on beneficial ownership information. This may be in part due to the little outbound international co-operation requests in relation to basic and beneficial ownership information (see Immediate Outcome 2). The authorities indicated that SAFIU and SAGIA have not identified concerns in relation to the information received from foreign counterparts. The authorities also noted that they will monitor the quality of incoming information when the need will arise.

Weighing and Conclusions

Saudi Arabia has a developed system to ensure transparency and availability of legal and beneficial ownership information of legal persons. The main deficiencies relate to not having sufficiently assessed the ML/TF risks associated with all types of legal persons and not monitoring the quality of assistance received from other countries in relation to basic and beneficial ownership of legal persons.

Saudi Arabia is rated largely compliant for R.24.

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

In the 2010 MER, Saudi Arabia was rated LC for the requirements on legal arrangement. There was uncertainty as to whether information on beneficial owners of waqfs was available. The FATF Recommendations have since been revised such that some elements of R.25 apply to all countries.

Saudi legislation allows for the formation of Waqfs, which are trust-like legal arrangement allowing the separation of control and ownership of an asset. Waqfs also presents some characteristics of legal persons in that they can own shares and hold bank accounts in their own names. The activities of a waqf are regulated through several rules and regulations, in particular the Law of Procedures before the Sharia Law (LPSL). Other relevant legislation includes Circular No. 12/ 178/T dated 22/9/1398 AH (17 June 2017), and Regulation of Administrative Works in Sharia

Departments, Public Endowment Authority Law by Royal Decree No. (M/11) dated 26/2/1437 AH (5 December 2015).

The Waqf is an asset established by a person (an endower) who no longer owns the asset, and the proceeds of which will be used for good. Saudi Arabia indicated that the purpose of the waqf is the development of the community and contribution to the various development areas (health, education, unemployment and others). Waqfs can take the form of public and private waqfs. Public waqfs are assigned to specific charity aspects, and are managed directly by the General Authority for Waqfs. Private waqfs identify family members as the beneficiaries of the endowed property and the trustee (beholder) is appointed by the endower (settlor) with approval by the competent judge.

In general, waqfs must be registered with a judge or with the Ministry of Islamic Affairs, even though waqfs may be established without registering title deeds in accordance with applicable rules and procedures (LPSL, Art.221). General courts are responsible for issuing title deeds for waqfs (LPSL, Art.31). Family courts are responsible for registration of waqfs in family matters, for recording the designation of trustees, guardians and administrators and for deciding over issues related to the waqfs (LPSL, Art.33). Waqfs can be established by Saudi citizens as well as by foreigners under certain conditions (LPSL, Art.222) but the endowed property must be in Saudi Arabia. As of December 2015, both private and public waqfs are supervised by the General Authority for Waqfs.

In addition to waqfs, nothing in Saudi legislation prevents a person in Saudi Arabia from acting as a trustee of a trust created under foreign law, or from property in Saudi Arabia being managed under the terms of a foreign trust.

Criterion 25.1 –

a) The identity of the settlor of a waqf is disclosed to the judge at the time of registration of the waqf, as a judge cannot register the establishment of a waqf unless ownership of said waqf by the endower is established and upon verification that his record is free from any encumbrances to such registration (LPSL, Art. 219). Family courts are also responsible for recording the designation of trustees, guardians and administrators, and can appoint or remove the trustee under certain conditions. The deed of the waqf needs to be provided to the judge, and contains information on the settlor, trustees, the protector, and beneficiaries. The law does not require the trustee to determine whether any other natural person exercises ultimate effective control over the waqf.

b) There is no obligation for the trustee (or for the competent judge) of a waqf to hold information on any other regulated agents of, and service providers to, the waqf, including investment advisors or managers, accountants and tax advisors.

c) Persons performing the services of trust service providers professionally are not covered by the AML/CFT legislation (see c.22.1). The availability of the information required under c.25.1.a and c.25.1.b for waqf is limited to the requirements of the specific legislation. In relation to foreign trust, the information available to the trustee will be required to be maintained under the laws of the creation of the trust. Where lawyers provide trustee services, they will be required by the AML/CFT legislation to maintain information on the trust (see c.10.10).

Criterion 25.2 -

On principle, ownership of the assets of a waqf cannot be transferred to another person. The competent judge may nonetheless approve the selling, replacing, transferring of a waqf (LPSL, Art.223). Information on the trustees and on the beneficiaries, as well as on the other persons relevant to the waqf, has to be updated both in the deed and in the records of the court after the Appeals Committee authenticates the new deed (Circular No. 12/ 178/T, 1-C). The gaps in relation to the obligations on the trustee to hold beneficial ownership information on the waqfs persist under this criterion.

In relation to foreign trust, as indicated under c.25.1.c, there is no obligation for professional trustees to hold information on a trust available.

Criterion 25.3 -

There are measures to encourage a trustee to disclose its status to FIs and DNFBPs when establishing a relationship with them. For a customer that is a legal arrangement, the financial institution or DNFBP shall obtain and verify the name, legal form and proof of existence, the powers that regulate and bind the legal arrangement, as well as identify and take reasonable measures to verify the identity of the endower, beholder, the beneficiaries or classes of beneficiaries, and any other natural person exercising ultimate effective control over the legal arrangement (Implementing Regulation to the AML Law, art.7/2). This ensures that the trustee would disclose itself if the FI/DNFBP is aware that the client is a legal arrangement. It is unclear whether there is any specific obligation on the trustee to disclose its status of the legal arrangement to an FI/DNFBP. The Saudi authorities indicated that a trustee who does not disclose the existence of the legal arrangement would be subject to sanctions based on behaviour that would constitute misconduct

Waqf can open bank accounts in their names, and banks must identify the trustee. When opening a bank account, the bank shall obtain a photocopy of the legal deed whereby the property is endowed, and a photocopy of the legal deed of trusteeship stipulating disposal of the endowment as per the conditions of the person who offered the property (Rules Governing the Opening of Bank Accounts, Art. 300.1.5.7). The bank must obtain photocopy of the ID of the trustee(s) and check it against the original, conformity with the original should be certified by the bank and the trustee (*ib.*). The identity of the trustee must also be disclosed to institutions opening investment accounts (Investment Accounts Instructions, Art.7.f.1).

Criterion 25.4 -

Waqfs are generally subject to registration with the competent judge, who also receives the deed. The information provided in the deed is then available to public authorities as Saudi Arabia indicated that there is no law or enforceable means that prevents the competent judge or the court from sharing it with other domestic or foreign authorities.

Criterion 25.5 -

LEAs have powers to timely obtain information on waqfs from the competent judges, as well as from the trustees of the waqf (see R.31). The information on the waqf is held by the Court where the waqf is registered. LEAs and the FIU can also obtain the information on the waqfs and foreign trust the FIs and DNFBPs might have.

Supervisors and other public authorities can obtain information held by the competent judge with no impediment. However, the information available with the competent judge, the trustee, does not necessarily include information on the beneficial owner of the legal arrangement.

Criterion 25.6 -

There are no impediments for authorities to obtain information on the waqfs from the competent judges for the purpose of sharing it with foreign authorities. Information from trustees and reporting entities can be obtained for the purpose of a mutual legal assistance request. The FIU can obtain information from reporting entities and exchange it.

Criterion 25.7 -

There are measures to ensure that the trustees of waqfs are legally liable for failure to perform the duties relevant to meeting their obligations. Family courts can dismiss the trustees, guardians and administrators if necessary (LPSL, Art.33). Saudi Arabia indicated that the decision of the Permanent Authority of the Supreme Judiciary Court No.84/5 dated 5/5/1415 H clarified that the judge has a general authority over the trustee in cases of both public or private Waqfs, a judge may remove a beholder and hold him accountable for circumvention or if he is charged for his misconduct, even if this will result in his imprisonment.

With regard to information held by a trustee of a foreign trust in Saudi Arabia, the obligations on the trustee depend on the laws of creation of the trust. There are sanctions on FIs/DNFBPs for not obtaining and maintaining information on the client legal arrangements.

Criterion 25.8 -

Information on waqfs is available with the competent judges, who should exchange it with other public authorities with no restriction. Sanctions on reporting entities can be applied if they do not provide information to requesting authorities (AMLL, Art.10). The competent judges may remove the trustee, although it is unclear if there are other sanctions available to the judges to compel the provision of the information by the trustee. In most cases, nevertheless, the information on the waqf would already be available to the judge.

Weighing and Conclusions

Saudi Arabia has legislation in place to ensure transparency of legal arrangements in Saudi Arabia. With the new AML Law passed in November 2017, the information on the beneficial owner of waqfs and foreign trusts should be available with the financial institution and/or DNFBP with which the legal arrangement has a business relationship. Nonetheless, the provisions on the trustee do not cover all ownership information as required by R.25, particularly beneficial ownership information.

Saudi Arabia is rated largely compliant with R.25.

Recommendation 26 – Regulation and supervision of FIs

In its 3rd round MER, Saudi Arabia was rated LC for Recommendation 23. The main technical deficiencies were found to be that fit and proper persons procedures were not tested against other sources for existing FIs and non-Saudi Nationals, there was a lack of human resource allocated to the activities of insurance and authorised persons, there was insufficient training for CMA's AML staff, and there were a low number of AML/CFT related examinations on authorised persons.

Criterion 26.1 - SAMA is the designated authority with responsibility for regulating and supervising entities undertaking banking, financial activities, money and currency changing businesses, and insurance and re-insurance activities for AML/CFT. The CMA is responsible for regulating capital markets activities for AML/CFT.

The AMLLIR (Art. 1/4) refers to SAMA and CMA as supervisory authorities, among others.

Supervisory Authorities are authorised to issue instructions, rules, guidelines, circulars, orders, decisions, etc., to implement the provisions of the AMLL, and ensure compliance of regulated entities with their AML obligations (*AMLL, Art. 24*). The supervisory authorities are provided with similar powers with respect to TF (*CFTL, Arts. 82).*

Supervisory Authorities are defined as authorities with the power to oversee or monitor FIs (*AMLL, Art. 24*). Despite the power of supervisors to licence FIs, this is not specifically provided for in the revised AMLL (*though Article 1 part 12 of old AMLL had provided for this)*, other laws such as BCL, SRB, etc., provide for the same. Thus, SAMA has powers to grant licences and inspect institutions' conduct with respect to banking activities (*BCL, Arts. 3 & 18*), financial activities including financial leasing, credit card finance and consumer finance (*FCCL, Articles 5 & 10*) and insurance and re-insurance activities (*LSCIC, Art. 2*). SAMA also has the authority to license and supervise money changing businesses buying and selling foreign currency, travellers' cheques and engaging in the purchase of bank drafts (*RGMCB, Arts. 3, 15*).

The CMA has powers to suspend capital market activities, approve the listing of stock traded, and inspect institutions' conduct with relating to capital markets activities (*CML, Art 5c and 6*). The CMA also has the responsibility for authorising persons undertaking securities business (*Securities Business Regulations, Art.5*), that includes persons dealing in securities, arranging securities business, managing a security belonging to another person and taking custody of a security on another person's behalf (*SRB, Art. 2*).

Criterion 26.2 - Banking businesses (*BCL, Art. 2*), financial activities (*FCCL, Art. 4*), Authorised Persons Regulations (*Arts. 1, 6 and 10*), capital markets activities constrained to brokerages (*CML, Art. 60*), money changing businesses (*RGMCB, Art. 3*), a person undertaking securities business (*Securities Business Regulations, Art. 5*), insurance and re-insurance companies (*LCSCIC, Art. 2*) are all required to be licensed or authorised. As all institutions undertaking the activities are covered by each law, Core Principles FIs undertaking the activities specified above are captured. Entities headquartered outside Saudi Arabia need to obtain a license to operate in Saudi Arabia and as part of the licensing approval they need to comply with local laws.

In August 2017, SAMA issued the requirement to open a foreign bank branch within Saudi Arabia. While there is no specific provision prohibiting the approval or operation of Shell Banks in Saudi Arabia, the process of granting licences ensures that the shell banks do not exist in Saudi Arabia

Criterion 26.3 **–** Founders and members of the board of directors of banking businesses are required to be assessed as persons of good reputation in order for the institution to possess a licence (*BCL, Art. 3/3*). Article 16 of the FCCL contains the fit and proper requirements of Board of Directors. Similarly, in terms of Article 10 of IR of FCCL, founding directors and persons intending to acquire shares in a finance company have to meet the fit and proper requirements. In terms of Article 27 of IR of Law of Cooperative Insurance Companies, fit and proper standards issued by SAMA shall be applied to the Company's and Insurance and Reinsurance Services Provider's Chairman, Board Members, Directors, and Senior Managers. Designated forms issued for this purpose shall be completed and approved by SAMA. Article 3 of Ministerial decision 1375 dated 01/05/1432H stipulates the fit and proper requirements for Money Exchange Business, including MVTS. Fit and proper tests are not applied to persons acquiring significant shareholdings.

In terms of Article (6)(e)(4) of the Authorised Persons Regulations, for getting a licence, an applicant should show CMA that its directors, officers, employees and agents who will be involved in the applicant's securities business have the necessary qualifications, skills, experience and integrity to carry on the kind of securities business that it proposes to carry on. Further, CMA has issued circular number (ص/1/6/3480/17) dated 15/6/2017, which includes additional clarifications for fit & proper and rejecting the registration request for board members if the proposed registered individual committed crimes.

Criterion 26.4 **–**

(a) for core principles institutions:

(i) Articles 18 and 22 of BCL briefly explain the role/powers of banking supervisor (SAMA). Similarly, Section 2.2 of Rules Governing Anti-Money Laundering & Combating Terrorist **Financing for all banks and money exchangers and foreign banks' branches operating in** the Kingdom of Saudi Arabia, issued by SAMA also explains that SAMA would monitor banks and money exchangers to see that they are applying sound CDD procedures and are sustaining ethical and professional standards on a continuous basis. Banks are subject to consolidated group supervision for AML/CFT purposes where appropriate.

(ii) The Saudi Arabia Monetary Agency, SAMA, has issued detailed inspection procedure document (manual) for AML/CFT supervision of FIs coming under its jurisdiction.

(iii) The Capital Market Law (*Art. 5*) provides the general framework for supervision by CMA which has issued a document in Excel format, detailing the ML/FT inspection procedure being followed by it.

(iv) The law on Supervision of Cooperative Insurance Companies (*Art. 8*) provides for the legal framework which could allow supervisory process.

(b) for other FIs:

(v) Chapter 5 (Arts. 21 and 28) of Finance Companies Control Law provides for the supervision of Finance Companies by SAMA and the supervisory powers which SAMA have, including the powers to suspend licence of FCs. In Rules governing AML/CFT of Finance Companies issued by SAMA, it is mentioned that based on the Ministerial Decision No 1566/1 dated 21/7/1420 AH, entrusting (SAMA) with the power to supervise and regulate the activity of financial leasing and financing companies under its supervision.

(vi) As regards Money Exchange Companies, some of which also undertake MVTS functions, a detailed Manual of Regulation of Money Changers Business Procedures has been issued by SAMA. This Manual has specified the procedures to be followed by MECs and SAMA looks into the implementation of the same during supervisory process.

Criterion 26.5 -. SAMA and CMA use risk matrix tools to determine the frequency and intensity of supervision. SAMA uses the tool for analysing the inherent and net risks of each entity, its impact on the financial sector, and measuring the extent to which the financial institution has taken the necessary measures to mitigate these risks. SAMA assesses each institution for its AML/CFT risks as *Very High, High, Upper Medium, Lower Medium* and *Low*. This assessment is determined based on residual risk derived from the risk matrix after internal controls are weighted against the inherent risks as well as the extent to which the financial institution affects the Saudi financial market. The assessment of residual risk of a financial institution will result in: (1) Planning inspection visits according to the highest risk, (2) Determining inspection ranges and focus, and (3) Determining the inspection mechanism.

The frequency and intensity of supervision of FIs and APs depend on their riskiness with respect to ML/FT threats. The inspection program includes all FIs with high and very high risk, and includes a number of medium and low risk FIs. In addition to the AML/CFT risks based on the risk matrix method, examinations are also prioritized based on other factors such as the interval from the last inspection, changes in the FIs business plans, liquidity levels, or incidents. The risk matrix can also give cause to sectoral inspections.

Criterion 26.6 - SAMA and CMA hold risk profiles of every financial institution under their supervision, based on the risk matrix tools described above. SAMA provided a detailed document on AML/CFT on-site examination procedure which also explains the procedures to be followed for off-site collection of data/returns, etc. The document explains that a risk-based approach is followed by SAMA which also verifies that FIs have adopted a risk-based approach as far as AML/CFT risks are concerned.

The Capital Market Authority has explained the detailed inspection (supervision) procedures followed by it for supervising APs with respect to AML/CFT risks. CMA has also provided a document (excel sheet) explaining the procedure for onsite supervision.

Weighting and Conclusion

Saudi Arabia is compliant with R.26.

Recommendation 27 – Powers of supervisors

In its 3rd round MER, Saudi Arabia was rated LC for Recommendation 29. The main technical deficiencies were found to be that there were an insufficient number of staff with insufficient expertise employed within the Insurance Control Unit in SAMA or in the CMA, and there were a low number of examination tasks carried out by SAMA and the CMA.

Criterion 27.1 -

(i) SAMA and CMA are the supervisors for FIs including banks, insurance companies, finance companies and authorised persons, etc.

(ii) In terms of Article 24 of AMLL, supervisors are vested with powers to supervise/monitor and ensure compliance by FIs with AML requirements. Similarly, Article 82 of new Law on CTF provides powers to supervisors to supervise/monitor and ensure compliance by FIs with CFT requirements

(iii) In terms of Rule 2.2 of the Rules governing Anti-Money Laundering & Combating Terrorist Financing, issued by SAMA, it is responsible for exercising regulatory and supervisory control over banks and money exchangers, issuing general rules and overseeing that all banks and money exchangers comply with and effectively implement the Anti-Money Laundering Law. Similarly, in terms of Section 1 of Anti Money Laundering & Combating & Terrorism Financing Rules issued by Insurance Division of SAMA, insurance companies are required to comply with the regulatory and supervisory instructions of SAMA. Article 8 of Law on Supervision of Cooperative Insurance Companies provides for supervision of insurance companies by SAMA. Chapter 5 of Finance Companies Control Law refers to the powers of SAMA to supervise finance companies. Further in the introductory paragraph of the Rules Governing AML/CFT for Finance Companies, it is mentioned that Based on the Ministerial Decision No.1566/1 dated 21/7/1420 AH, SAMA is entrusted with the power to supervise financing companies. Article 5 of CML refers to the powers of CMA for supervising Authorised Persons.

Criterion 27.2 - Supervisory authorities have been empowered in terms of Article 24(a) of the AMLL to collect information and other data from FIs (as also from DNFBPs and NPOs) as well as applying appropriate supervisory measures, including on-site inspections and offsite measures. Under Article 82.1 of CFTL, supervisors have been given similar powers for CFT. Further, Article 24(c) of the AMLL allows supervisory authorities to carry out an anti-money laundering risk assessment for the sectors for which the authority has a supervisory mandate.

Apart from the above, in terms of Article 18 of BCL, SAMA has the authority to inspect the records and accounts of banks onsite; in terms of Article 75 of IR of FCCL, SAMA is empowered to conduct onsite inspections of records and accounts of finance companies and Article 8 of LSCIC empowers SAMA to conduct inspection of insurance companies. The CMA is empowered to carry out inspections of any broker or broker's agent in terms Article 5c of CML to ensure compliance with CMA regulations.

Criterion 27.3 - The AMLL (*Art. 24/b*) stipulates that supervisory authorities shall have the powers to compel FIs (as also DNFBPs and NPOs) to provide any information that the supervisory authority considers relevant to carry out its function under this Law and its Implementing Regulation, and take copies of documents and files,

however and wherever stored. The CFTL (*Art. 82.2*) also provides similar powers to supervisors.

The AMLLIR (Art. 24/6/a) provides that financial institution or designated non-financial business and profession shall comply with any instructions, rules, guidelines or any other instruments issued by a supervisory authority, including an order under Article 24 (b) of the AMLL to provide any information as specified by the supervisory authority.

Further, as laws also empower supervisors to call for information in this regard. Thus, in terms of Article 17 of BCL and Article 11 of LSCIC, SAMA has powers to call for any information it deems necessary for banks and insurance companies to provide it with for AML/CFT requirements. SAMA can also request finance companies to provide it with any information requested (*FCCL, Article 28*). The CMA is provided with the power to inspect records or any other documents (*CML, Article 5c*).

Criterion 27.4 - The AMLL (*Art. 25*) provides that supervisory authorities have powers to impose a range of sanctions as under:

(1) Issue a written warning; (2) Issue an order to comply with a specific instruction; (3) Issue an order to provide regular reports on the measures taken to address the identified violation; (4) Impose a monetary fine of up to 5.000.000 riyals per violation; (5) Ban individuals from employment within the sectors for which the supervisory authority has competences for a period to be determined by the supervisory authority; (6) Restrict the powers of directors, board members, executive or supervisory management members, and controlling owners, including appointing one or more temporary controllers; (7) Dismiss or replace the directors, members of the Board of Directors or of executive or supervisory management; (8) Suspend, restrict or prohibit the continuation of the activity, business or profession or of certain business activities or products; (9) Suspend, restrict or revoke the license. Similar powers are given to supervisors under Article 83 of the CFTL.

Apart from the above, Article 22 of BCL, allows SAMA to impose different penalties on the banks and their functionaries, under Article 29 of FCCL, SAMA has powers to impose various penalties including suspension of licence of finance companies and Article 19 of LSCIC provides powers to SAMA to impose penalties on insurance companies including power to demand winding up of companies. Similarly, Articles 59 and 62 of CML, allow CMA to file a lawsuit with the Committee for Settlement of Securities Disputes to impose penalties including for revoking licence. Article 62 of CML also empowers CMA to take penal action without approaching the Committee for Settlement of Securities Deposits.

Weighting and Conclusion:

Saudi Arabia is compliant with R.27.

Recommendation 28 – Regulation and supervision of DNFBPs

Criterion 28.1 - Casinos are prohibited in Saudi Arabia.

Criterion 28.2 and 28.3 -

The Ministry of Commerce and Investment (MOCI) and the Ministry of Justice (MOJ), among others, are listed as supervisory authorities under Article 4/1 of the AMLLIR which lists the supervisory authorities concerned with Article 12 of the AMLL issued in 2017.

The Ministry of Justice has issued a Manual on AML/CFT requirements to be followed by Lawyers which also shows the risks to which Lawyers are exposed to. Further, in terms of Article 3 of Code of Practice of Law, a person who practices law has to have his name in the list of practising lawyers with the Ministry of Justice, prepared at the time of registration.

In January 2017, the MOCI issued a Manual on Combating Money Laundering and Financing of Terrorism, which are to be complied with by dealers of precious metals and stones (DPMS), real estate agents (REAs) and certified public accountants (APs). Further, Article 2 of Precious Metals and Gems Law issued by Royal Decree M/42 dated 22/4/1983 requires all precious metals and stones dealers to obtain licences from the MOCI.

In terms of Article 1 of Regulations for Real Estate Offices, Real Estate Agents have to register with Commercial Register (under MOCI) in accordance with the provisions of the Commercial Register Law and its executive regulations. In terms of Article 1 of Law of Commercial Register, the MOCI creates Commercial Register.

In terms of Article 19.6 of Law of Certified Public Accountants, Saudi Organization for Certified Public Accountants (SOCPA), operating under the supervision of the Ministry of Commerce is entrusted with the responsibility of setting up an appropriate field inspection system to ensure that certified public accountants apply accounting and auditing standards and comply with the provisions and regulations of this Law.

Criterion 28.4 -

(a) In terms of Article 24.a. of the AMLL, Supervisory Authorities are empowered to collect information and other data from DNFBPs as well as applying appropriate supervisory measures, including on-site inspections and offsite measures.

(b) In terms of Article 24.g. of the AMLL, Supervisory Authorities are to establish and apply effective fit and proper screening procedures for any person aiming to participate in the management or supervision of DNFBPs, or for any person aiming to own or control, directly or indirectly, or becoming a beneficial owner of significant shares.

(c) In terms of Article 25 of the AMLL, if the supervisory authority find that DNFBPs or any of their directors, board members, executive or supervisory management members failed to comply with any provision of the AML Law, its Implementing Regulation or relevant decisions or circulars, or any violation referred from other competent authority, the supervisory authority is empowered to impose one or more of the following measures: 1. Issue a written warning; 2. Issue an order to comply with a specific instruction; Issue an order to provide regular reports on the measures taken to address the identified violation; 4. Impose a monetary fine of up to 5.000.000 riyals per violation; 5. Ban individuals from employment within the sectors for which the supervisory authority has competences for a period to be determined by the supervisory authority; 6. Restrict the powers of directors, board members, executive

or supervisory management members, and controlling owners, including appointing one or more temporary controllers; 7. Dismiss or replace the directors, members of the Board of Directors or of executive or supervisory management; 8. Suspend, restrict or prohibit the continuation of the activity, business or profession or of certain business activities or products; and 9. Suspend, restrict or revoke the license. In addition, it is worth mentioning that different types of punishments are prescribed for lawyers who violate the Code (Code of Law Practice, Part Three). Finally, SOCPA is vested with powers to impose sanctions for violations by CPAs (Law of Certified Accountants, Art.28). The Precious Metals and Gems Law grants MOCI the power to carry out onsite inspections and sanctions any instance of non-compliance.

Criterion 28.5 - MOCI and MOJ, through their respective AML/CFT Departments, assess the ML/TF risks of DNFBPs through off-site tools and on-site visits. Based on the risk classifications of DNFBPs, their supervisory engagements including the priorities of field examinations are determined. MOCI and MOJ risk profiles of every DNFBP is maintained and evaluation results are updated semi-annually.

Weighting and Conclusion:

Saudi Arabia is compliant with R.28.

Recommendation 29 – Financial intelligence unit

In its 3rd round MER, Saudi Arabia was rated LC for Recommendation 26. The main deficiency related to the effectiveness of Saudi Arabia's FIU in terms of the processing of STRs, which is assessed as part of the effectiveness part of the evaluation. Since the 2010 evaluation, Saudi Arabia issued new laws that provide the FIU with a legal basis to enable it to function. The most recent laws were issued in November 2017 during the onsite visit (new AML law [AMLL] and a new CFT law [CFTL]), moving oversight of the FIU from the Ministry of Interior to the State Security Department.

Criterion 29.1 - The SAFIU has the responsibility for acting as a national centre for receipt and analysis of suspicious transaction reports and other information relevant to money laundering, associated predicate offences and terrorist financing; and for the dissemination of the results of that analysis (AMLL, Article 17; CFT Law, Article 76).

Criterion 29.2 -

a. The SAFIU serves as the central agency for the receipt of STRs filed by FIs, DNFBPs (and NPOs) ['reporting entities']. In line with R.20 and R.23, when a reporting entity suspects or has reasonable grounds to suspect that funds are the proceeds of criminal activity, or are related to terrorist financing, they are required to report the suspicion promptly to the SAFIU (AMLL, Article 15; CFT Law, Article 70; AMLLIR Article 15). FIs and DNFBPs are defined in line with the FATF Recommendations.

b. The SAFIU receives STRs submitted by NPOs and customs information collected as part of cross-border cash disclosures (AMLL Article 23/4, AMLL IR Article 23/12).

Criterion 29.3 -

a. The SAFIU is able to obtain any additional information that it deems necessary to carry out its analysis (AMLL, Article 18; CFT Law, Article 77). The SAFIU is authorised

to obtain information directly from reporting entities relating to information in an STR filed. In cases where further information is required from an FI, and it does not relate to a transaction or a person cited in the STR, the SAFIU must request the information via the relevant regulator – SAMA or the CMA (AMLL, Article 18 – AMLLIR, Article 18/1-2; CFT Law, Article 77). The SAFIU may obtain information directly from a DNFBP, whether it or not it relates to the information submitted in an STR (AMLL IR Article 18/1-2). It takes 5-7 days on average for the SAFIU to receive further information from FIs when requests are submitted via the regulators; however urgent requests are dealt with on an expedited basis. Therefore, the delays caused by needing to go through SAMA for additional information in the above circumstances are not assessed to have a material impact on the SAFIU's ability to perform its analysis. See Immediate Outcome 6.

b. The SAFIU has authorisation to obtain any information that it deems necessary to carry out its analysis, as above. The SAFIU has access to a wide range of administrative and law enforcement databases, including the Automated Civil Affairs Register, the Saudi Citizenship Register, the Border and Pilgrimage Register, the Automated Expat Affairs Register and the Sponsorship Register (that contains information on foreign employees and the Saudi National that must register them) the Drug Register, the Criminal Records Register, the Wanted Individuals Register, the Driving License Register, the Lands and Deeds Register and the Commercial Register of Companies. The SAFIU may also request access or has indirect access to a number of other databases, including a database of non-declarations provided by the Customs Authority, Zakat Authority and databases held by the Minister of Interior.

Criterion 29.4 -

a. The SAFIU has responsibility for conducting operational analysis, which uses available and obtainable information to identify specific targets to trace particular activities or transactions, and determine the links between those suspects and possible proceeds of crime, money laundering or predicate offences (AMLL IR Article 17/2). Terrorist financing is included as a type of predicate offence and therefore is included similar to other predicate offences and money laundering activity. While the SAFIU is conducting operating analysis, it is not always clear that the analysis is making links between targets and possible proceeds of crime, money laundering, predicate offences and terrorist financing. See Immediate Outcome 6.

b. The SAFIU has responsibility for conducting strategic analysis, using available and obtainable information, including data that may be provided by other competent authorities, to identify money laundering related trends or patterns (AMLL IR, Article 17/2). The FIU has conducted a number of strategic reports, including making use of data provided by other competent authorities, and disseminated them to competent authorities. The strategic analysis disseminated has included outputs relating to TF.

Criterion 29.5 -

The SAFIU is able to disseminating the results of its analysis to competent authorities either spontaneously or on request (AMLL, Article 17; CFT Law, Article 76). When disseminating information or the results of its analysis to competent authorities, the SAFIU should use dedicated, secure and protected channels (AMLL IR, 19/1). The adequacy of the channels is assessed in the effectiveness part of the evaluation.

Criterion 29.6 -

a. The SAFIU is required to have rules in place governing the security and confidentiality of information, including procedures for handling, storage, dissemination, protection of and access to information (AMLL IR, Article 17/3 a). The specific rules themselves are set out in the Information Security Policy Manual and include parameters for the justification of conducting searches, requirements around access to the information systems, and guideless for staff on the protection of information whether inside or outside of the administration. The MoUs signed between the SAFIU and other competent authorities contain confidentiality clauses, and the cases disseminated by the SAFIU are submitted to the relevant competent authority in a closed envelope that must be opened by a designated person at the relevant competent authority. The rules governing the confidentiality of information disseminated have not been provided so have not been verified. See also Immediate Outcome 6 for analysis of the protection of confidentiality.

b. There is a broad provision in law for the need for the SAFIU to take appropriate measures to ensure that employees understand their responsibility in dealing with sensitive information and its dissemination (AMLL IR, Article 20/2) and to have their employees cleared (AMLL IR, Article 20/1). Every individual with duties for or within the SAFIU is required to keep confidential all information obtained within the scope of their duties, including after they may have left their post (AMLL Article 20). The specific rules that safeguard the confidentiality of information are defined by the civil service system, as well as the officers and individuals' service system that determine the penalties for those who violate the rules on confidentiality. When selecting employees for the FIU, information is gathered on them confidentially, and successful candidates are required to sign confidentiality agreements. Where there are doubts those individuals are excluded from the process. New employees are required to take training courses in order for them to understand their responsibilities in handling and disseminating sensitive and confidential information.

c. There are legal requirements for the SAFIU to protect the information it receives or maintains by ensuring that there is limited access to the SAFIU's facilities, information and information systems (AMLL IR 17/3). To implement them, the SAFIU has a set of regulations and guidelines for determining security policies in both information security and building security. There are internal rules governing the entry and exit procedures and exit cancelation or modification when the employee moves. In terms of the security of the FIU headquarters, special guards and surveillance cameras are in place. According to the regulations and guidelines, only those authorized can access the facilities and information including IT systems.

Criterion 29.7 -

a. It is stipulated in law that the SAFIU has the authority to carry out its function freely, including the autonomous decision to conduct analysis, request, disseminate or forward specific information (AMLL Article 19 and AML IR Article 17/4; CFT law, Article 79).

b. The SAFIU is provided with the authority to seek or share information with a counterpart relating to the SAFIU's functions, and the SAFIU may enter into an agreement or arrangement to facilitate the exchange of information with a foreign authority (AMLL Article 22). The SAFIU may exchange or enter into agreements that allow the exchange of information between competent authorities in Saudi Arabia (AMLL, Article 21; CFT Law, Article 80; AMLL IR Article 17/4).

c. The SAFIU is affiliated to the State Security Presidency, and falls under the oversight of the President of State Security, with the President of State Security determining the organisational structure of the SAFIU (AMLL Article 17). The SAFIU is given a distinct function to distinguish it from other directorates that fall under the responsibility of the State Security Department (AMLL IR 17/4). The Saudi Arabian authorities have explained that various measures are in place to ensure that it has a distinct structure from the SSP, including the lines of responsibility, but it is not clear how these mechanisms are provided for or protected.

d. It is stated in law that the SAFIU should be able to obtain and deploy the resources needed to carry out its functions, on an individual or routine basis, free from undue political, government or industry influence or interference that may compromise its independence (AMLL IR Article 17/4). As the SAFIU moved from being affiliated to the Ministry or Interior to the Presidency of State Security while the onsite was conducted, it was not possible to fully examine the operational independence under 29.7d.

Criterion 29.8 - The SAFIU has been a member of the Egmont Group since 2009, participates in the working groups, and exchanges information through the ESW (Egmont Secure Web). The SAFIU's membership of Egmont is stipulated in the Implementing Regulations of the AMLL (AMLL IR Article 17/1).

Conclusion and weighting

There are several minor shortcomings; some of the rules regarding the dissemination of confidential information have not been verified; all aspects of operational analysis are not always conducted in line with criterion 29.4(a), and the mechanisms that enable the SAFIU to remain operationally independent and autonomous now that it is under the Presidency of State Security were not fully examined and therefore are not all clear. However, the majority of the requirements under R.29 have been met, and it has been assessed that none of these shortcomings materially impact the SAFIU's ability to perform its core functions under R.29.

Saudi Arabia is largely complaint with R.29

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

In its 3rd round MER, Saudi Arabia was rated LC for Recommendation 27. The main technical deficiency identified was whether or not all investigation authorities, other than the Prosecution Authority, had sufficient awareness and knowledge to properly investigate ML/TF.

The AMLL law that came into force on 24 October 2017 [See R.3], the CFT law that was issued on 1 November 2017 [See R.5], and the Law on Criminal Procedures, a decree issued in November 2013, provides the general framework within which law enforcement and investigative authorities are given the mandate to act with respect to the investigation of ML and TF.

Criterion 30.1 **-** The Public Prosecution is required to investigate and prosecute money laundering offences and associated predicate offences, issuing guidelines and instructions to the competent authorities under its supervision via the Law of

Criminal Procedures (AMLL, Article 48). The Public Prosecution is also responsible for investigating terrorist financing offences (CFT law, Article 18). The Presidency of State Security will oversee the investigation of crimes stipulated in the CFT law for a period of two years until the Public Prosecution is ready to take on the responsibility.

The Law of Criminal Procedures (issued November 2013) sets out the general processes and procedures for the investigation of criminal acts in Saudi Arabia, including the investigation of ML and TF. The various LEAs and Other Control Authorities (OCAs: see introduction to Chapter 3) conduct preliminary investigations into suspected ML or TF, before requesting that the PP initiates an official investigation in co-ordination with the relevant LEA or OCA, while the LEA or OCA continues to collect information and evidence to support the investigation. Preliminary criminal investigations are conducted by 'preliminary criminal investigation officers', defined as agencies, committees and persons assigned to conduct investigations pursuant to [other] relevant laws (LCP, Article 26). The AMLL (a 'relevant law') defines competent authorities as any administrative authority, law-enforcement authority, or supervisory authority, with each the main ministries, supervisors and the SAFIU cited. However, the instruments that provide the LEAs and OCAs with their powers to act under each ministry have not been provided.

Criterion 30.2 - Criminal Investigating Officers have the responsibility for criminal and administrative investigation into both predicate offences as well as associated money laundering in the their respective fields (AMLL, Article 49). Criminal Investigating Officers have responsibility for collecting information and evidence in relation necessary for the investigation and indictment of a ML act (LCP, Article 24). The State Security Presidency is responsible for the investigation of funds related to terrorist financing (CFT Law, Article 4). The authorities are provided with powers to investigate ML/TF offences that are not required to be linked to the investigation of predicate offences. Therefore they may conduct a financial investigation alongside or in the context of an investigation into ML, TF and/or predicate offence(s). The general provisions that provide the Public Prosecution with the authority to conduct ML investigations also does not preclude conducting parallel investigations. The only shortcoming is that Saudi Arabia has not demonstrated how all of the LEAs and OCAs, each with their own criminal investigating officers, are also subject to the same requirements [see Criterion 30.1].

Criterion 30.3 - Criminal Investigating Officers have responsibility for identifying, tracing or securing the proceeds or instrumentalities of crime [AMLL Article 49]. The PP, either on undertaking or upon the request of the SAFIU or a criminal investigating office, based on the suspicion of ML or a predicate offence, may provisionally seize funds that are or may be subject to confiscation for a period not exceeding 60 days.]. The State Security Presidency is responsible for identifying, tracing and initiating the seizure and withholding of funds suspected of being the proceeds associated with the financing of terrorism (CFT Law, Article 4).

Criterion 30.4 - The relevant provisions of R.30 as defined in the AMLL apply to competent authorities. Competent authorities are defined as any administrative authority, law-enforcement authority or supervisory authority (AMLL Article 1) [see also 30.2].

Criterion 30.5 - Saudi Arabia established a National Anti-corruption Commission (NACC) in 2011 (Royal Decree A/65 and Council of Ministers Resolution no 165).

Council Resolution 165 gives the NACC powers to investigate financial and administrative corruption in public works contracts, operation and maintenance contracts and other contracts relating to matters of public concern and interests of citizens in entities under the Commission's jurisdiction. 'Violations' and 'irregularities' relating to financial or administrative corruption are to be referred to auditing or investigation agencies on detection. However, the National Anti-corruption authority does not have investigative powers to investigate ML/TF offences arising from or relating to corruption offences. Mabaheth (administrative division) is responsible for the preliminary investigation of bribery (including ML relating to bribery), and the General Directorate of Security is responsible for the preliminary investigation of other corruption related offences (including the preliminary investigation of ML derived from other offences relating to corruption).

Weighting and Conclusions:

Saudi Arabia meets most of the requirements for R.30. The only shortcoming is that the instruments that provide the law enforcement authorities with the responsibility for the preliminary investigation of ML, predicate offences, and TF have not been made clear.

Saudi Arabia is largely compliant with R.30.

Recommendation 31—Powers of law enforcement and investigative authorities

In its 3rd round MER, Saudi Arabia was rated LC for Recommendation 28. The main technical deficiencies were found to be a lack of specificity regarding investigative powers related to ML and TF offences, statistics and case studies that didn't address investigative powers or distinguish between ML and TF, and a lack of operational law enforcement co-operation. The new Recommendation 31 contains more detailed requirements in the area of law enforcement and investigative powers. See the preamble to R30 for information on the relevant laws passed since Saudi Arabia's last MER.

Criterion 31.1 -

a. The Public Prosecution, either upon its own initiative or upon request by the criminal investigating officer (see R.30), may order any person or FIs -through the supervisory authority- or DNFBPs (or NPO) to provide records, documents or information (AML Article 43; CFT law Article 6). Both natural and legal persons are covered (AMLL IR, Article 1/1). The same mechanisms apply for the State Security Presidency when investigating TF (CFT Law, Article 6).

b. The Public Prosecution may, on its own initiative or upon the request of the criminal investigating officer [see 30.1], issue a warrant permitting the criminal investigating officer or the investigator to enter houses, offices or the headquarters of the reporting entity to search for, detect and arrest persons, or to search for and seize funds, properties, documents, evidence or information relating to a predicate crime or a ML crime at any time during the period specified in the Search Warrant (AMLL Article 45). Similar provisions are provided for in relation to TF offences (CFT Law Article 7).

The Law of Criminal Procedures provides a criminal investigation officer with the power to search an individual where it is lawful to arrest them (LCP Article 43).

c. A criminal investigating officer shall hear the testimony of witnesses, unless he deems it unnecessary. They may also hear the testimony of any other witnesses whose testimony may lead to proving the crime, its circumstances, and its attribution to the accused or innocence (LCP, Article 95). These are general provisions that apply to the criminal investigating officer investigating any money laundering, associated predicate offence or terrorist financing related activity.

d. A criminal investigating officer may search a dwelling or person(s) inside a dwelling and seize any item that may have been used in the commissioning of a crime or anything that may lead to solving a crime. There must be evidence to suggest that a person has been involved in a crime prior to the search (LCP, Article 80). Evidence is defined in the implementing regulation to the LCP as 'strong factual circumstances'. These are general provisions that apply to the criminal investigating officer investigating any money laundering, associated predicate offence or terrorist financing related activity. Complimentary provisions are provided in the AML and CFT law.

Criterion 31.2 -

a. The Public Prosecution may issue an order permitting an investigating officer to conduct an undercover operation for the purpose of gathering evidence of money laundering or a predicate offence. An undercover operation is an operation for intelligence conducted by the investigation officer to gain evidence or information related to the criminal behaviour (AMLL IR Article 49/1). This power extends to the investigation of terrorism financing offences on the basis that TF is a predicate offence for ML. The CFT Law also provides the competent authority (the State Security Presidency) with the responsibility for operations of a secret nature (CFT Law, Article 4).

b - c. The Public Prosecution may, at its own motion or upon the request of the criminal investigating officer, may issue a reasoned order permitting the criminal investigating officer or the investigator to monitor, control, record, intercept, seize and have access to all forms of evidence, records and messages including letters, publications, parcels, all forms of communications, telephonic conversations, information and data saved in computers, as specified in the Order, whether for a predicate crime or a ML crime (AMLL Article 46). For terrorist financing related crimes, the Attorney General of the Public Prosecution may issue a reasoned order to monitor and have access to evidence, records and messages, including letters, publications, parcels and all communication instrument and information and documents saved in electronic systems relating to any of the crimes stated in this Law, and to intercept, seize and records all these materials (CFT Law Article 8).

d. Investigating authorities may conduct or participate in a controlled delivery under the supervision of the Ministry of interior (AMLL IR Article 49/2). Controlled delivery is defined as a method whereby the competent authority, under its observation, is permitted to allow the illicit or suspicious fund or proceeds of crime to enter the Kingdom, pass it, or go outside the Kingdom for the purpose of identifying and detecting a crime and its perpetrators (AMLL IR Article 1). Controlled delivery in relation to TF is covered as TF is a predicate offence for ML.

Criterion 31.3 -

a. The Public Prosecution, either upon its own motion or upon request by the criminal investigating officer, may order that any person or FIs -through the supervisory authority- or DNFBPs (or NPOs) directly provides records, document or information. The requested entity shall execute the order as specified in the order, accurately, and without delay (AMLL Article 43). Person is defined as any natural or legal person (AMLL IR Article 1/1). Similar provisions apply for investigations of suspected TF activity (CFT Law Article 6). A special unit located at the supervisory authority (SAMA) has been established to identify whether natural or legal persons hold or control accounts.

b. According to the implementing regulation of the AMLL, when requesting records or documents from the financial institution, the supervisory authority should not provide prior notice to the party concerned (AMLL IR, Article 43). Saudi Arabia has informed the assessment team that the banks are instructed not to notify the owner. However, mechanisms have not been provided that cover assets held elsewhere, and no processes to identify assets without prior notification to the owner are set out in the ML Cases Procedures Manual for LEAs.

Criterion 31.4 - Information disclosed to the SAFIU may be exchange with other competent authorities conducting investigations into money laundering, associated predicate offences, and terrorist financing (AMLL Article 21; CFT Law Article 80). Saudi Arabia has confirmed that the exchange is both ways, and competent authorities conducting investigations of money laundering, associated predicate offences or terrorist financing are able to ask for all relevant information, with no requirement for reciprocity. The information can be obtained by the LEA or OCA with relevant powers and responsibilities to act as a competent authority (see R30 and other parts of R31).

Weighting and Conclusions

The only deficiency relates to the mechanisms that Saudi Arabia has in place to ensure that competent authorities have a process to identify assets that are not held with banks without prior notification to the owner. As the competent authorities may retrieve information about assets without prior notification via databases accessed by the SAFIU in practice, this is considered a minor shortcoming.

Saudi Arabia is largely compliant with R.31.

Recommendation 32—Cash Couriers

In its 2010 3rd round MER, Saudi Arabia was rated PC on SR IX. The main technical deficiencies identified were that there were no effective, proportionate and dissuasive sanctions regime in place; there was a lack of statistics to include a comprehensive overview of cases under investigation/law enforcement and sanctions; and the shortcomings associated with Recommendation 3 (Confiscation and Provisional Measures) and Special Recommendation III (Targeted Financial Sanctions) that had a negative impact on the rating of SR IX. Saudi Arabia was also criticized for not including bearer negotiable instruments (BNIs) in their declaration form.

The legal framework for the reporting of cross-border currency and BNI is derived from the AMLL. As TF is a predicate offence for ML, where there are references to predicate offences in the AMLL, this includes TF.

Criterion 32.1 – Any person who enters or leaves the Kingdom of Saudi Arabia in possession of currency, bearer negotiable instruments (as well as previous metals or stones or jewelry) exceeding the value threshold must make a declaration to the General Directorate of Customs. This includes any person who arranges the transportation of the above into or out of Saudi Arabia whether by cargo, courier, postal service, or through any other means (AMLL Article 23). The declaration form provided to the assessment team did not include BNIs. Saudi Arabia has confirmed that a new declaration system, in accordance with the new AMLL law, was implemented on the day that the 2017 AML law came into force and forms were distributed in advance. However, it is unclear whether or not this form included BNI and therefore that the declaration system for BNIs had been implemented at the time of the onsite.

Criterion 32.2 - All persons making a physical cross-border transportation of currency or BNIs (or precious metals or stones or jewellery) must make a declaration when the value of the asset in possession when entering or leaving Saudi Arabia is excess of 60,000SAR (approximately 13,100 Euro). The penalties applied for false declaration (AMLL Articles 23) implies a truthful declaration is required to be submitted.

Criterion 32.3 - Saudi Arabia has a declaration system.

Criterion 32.4 - Upon discovery of a false declaration of currency of BNIs (or previous stones or jewellery), or a failure to declare them, the Customs Authority, the designated competent authority, has the right to request additional information on their source and intended use (AMLL Article 23).

Criterion 32.5 - If a person fails to make a declaration, or makes a false declaration, and the Customs Authority is convinced that the reason(s) are innocent and there is no link to ML or a predicated offence, a fine shall be imposed. The fine shall be 25% of the seized items if it is the first violation, and 50% for any repeated cases (AMLL IR, Article 23/6). A person includes any natural or legal person (AMLL IR, Article 1).

Criterion 32.6 - The SAFIU shall obtain all information that the General Directorate of Customs holds, as specified by the AMLL (AMLL Article 23). The Customs Authority submits data on incoming and outgoing cash/BNI declarations to the SAFIU, and data received from the Customs Authority is updated on the SAFIU database on a daily basis.

Criterion 32.7 - The General Customs Department attends the Anti-Money Laundering Permanent Committee (AMLPC), the designated authority that is responsible for co-ordinating measures to implement International Standards on AML. The immigration authority is a member of the AMLPC through representation by the Ministry of Interior. In terms of TF, the customs authority is a non-permanent member of the PCCT, the body with the responsibility for co-ordinating policies to combat terrorism and its financing, and the immigration authority is a member of the PCCT through the representation by the Ministry of Interior. [See also R.2]

Criterion 32.8 - The General Directorate of Customs may stop or seize, any currency, bearer negotiable instrument, (and gold bars, precious metals or stones or jewellery) for a period up to 72 hours in the following scenarios (AMLL IRs Article 23/3):

a. If there is a suspicion that such currency, bearer negotiable instrument, (or gold bar or precious metal or stone or jewellery) is the proceeds or instrumentalities of crime or instrumentalities, or is related to a money laundering or a predicate offense, including in cases where the value of the items is under the threshold.

b. Where there is a false declaration.

Criterion 32.9 - The AMLL specifies that the SAFIU obtains all information that the General Directorate of Customs holds (AMLL Article 23) [See criterion 32.6]. Saudi Arabia has confirmed that the Customs Authority's database includes cases of declarations that amount to or exceed the prescribed threshold (60,000 SAR or approximately 13,000 Euros at February 2018), cases of non-declaration and false declaration, and cases suspected of being linked to ML or TF. Information is categorised in order to help facilitate its subsequent retrieval. The customs authority, whether acting on its own initiative or upon request, is able to co-operate and exchange information with foreign counterparts, or conduct inquiries on their behalf in relation to ML or predicate offences (AMLL IR, Article 23/16).

Criterion 32.10 - The Customs Authority has a dedicated database for collecting customs related information. Only authorised persons are allowed to enter information into the database at entry and exit ports, including sea ports, and are required to keep the information confidential. Access to the information is also limited. Based on the information provided, the safeguards do not appear to place restrictions on trade payments for goods and services or the freedom of capital movements.

Criterion 32.11 - In the case of a failure to declare or in the case of a false declaration for currency and BNI, or if there is a suspicion that the cash or BNI relate to a predicate offence or ML, the currency or BNI may be seized for 72 hours, with a possible extension to 60 days granted by the Public Prosecution (AMLL IR Article 23/3, 23/5 CFT Law Article 17). When there is suspicion that the currency or BNI seized may relate to predicate offences or ML, the case is referred to the Public Prosecution for further investigation and a notification is sent to the SAFIU (AMLL IR, Article 23/7). Measures consistent with R.4 enable the confiscation of currency or BNI, and sanctions consistent with R.3 and R5 apply if a conviction is subsequently secured for ML or TF.

Weighting and conclusion

The only shortcoming is that it was not clear when the declaration system for BNI had been implemented; before, during or after the onsite visit took place.

Saudi Arabia is largely compliant with R.32

Recommendation 33 - Statistics

Saudi Arabia was rated PC with this Recommendation in the previous MER, due to a lack of complete or reliable statistics in several areas, including: overall penalties on convictions; the difference between ML and TF; seizure provisions; AML/CFT staff and budgets of LEAs; customs; STR reporting by lawyers; and results of supervisory inspections.

Criterion 33.1 - Each Saudi authority maintains statistics on its own activities relating to AML/CFT. There is no central point which compiles or co-ordinates AML/CFT statistics and the coverage and quality of information is variable. Authorities do not use common definitions and methods, so data from different authorities (e.g. on the confiscation of proceeds and instrumentalities) is not comparable.

(a) Saudi Arabia's FIU maintains comprehensive statistics on STRs received and disseminated, including breakdowns according to sector, type of criminal activity, and the authorities concerned.

(b) Saudi authorities do not maintain comprehensive statistics on ML investigations, prosecutions, and convictions. Those statistics which are maintained are not comparable between the different agencies responsible. Authorities do maintain statistics on TF investigations, prosecutions, and convictions.

(c) Saudi authorities do not maintain comprehensive statistics on property frozen, seized, and confiscated in relation to ML or predicate offences, and those statistics available are not comparable. Comprehensive statistics are kept for seizures and confiscations at the border, relating to false or failed disclosures.

(d) Saudi authorities maintain statistics on MLA and other international requests for co-operation made and received, but not in relation to direct co-operation with foreign law enforcement and security authorities.

Weighting and conclusion

While some authorities do maintain comprehensive statistics, there are weaknesses, particularly in the statistics maintained by law enforcement authorities, which are not comprehensive, and are not comparable between agencies.

Saudi Arabia is partially compliant with R.33.

Recommendation 34 - Guidance and Feedback

In its previous evaluation, Saudi Arabia was rated PC with this recommendation. The main deficiencies were: that feedback was inconsistently applied and not adequately used as a tool to further the effectiveness of AML/CFT provisions; that insufficient guidance was given regarding ML and TF methods and typologies; that the guidance issued by supervisory authorities was not comprehensive and not industry-specific; that no specific guidelines had been issued to DNFBPs; and that no feedback was provided by SAFIU.

Criterion 34.1 - The AMLL authorises supervisors to issue guidance, decisions, instructions, rules, or other instruments to the entities subject to their supervision.

The FIU is mandated to issue and update guidance on identifying and reporting suspicious transactions, and to provide feedback on STRs received (*AMLL, Art. 24, AMLLIR 17/1*).

Supervisory authorities have issued rules or guidance for each regulated sector, which include basic information on money laundering and terrorist financing techniques and typologies, as well as red-flag indicators. SAMA and CMA rules for FIs and APs set out in more detail the obligations on the sectors and how they should be implemented. Most of these were issued in 2012 and do not appear to be updated regularly. Since 2012 SAMA has issued 3 circulars based on FATF statements, while MOCI has issued a manual on AML/CFT to newly-supervised sectors. SAMA also issued a circular (5403/MAT/12263, Feb 2011) to FIs on ML and TF risk indicators. The results of NRAs have been disseminated to the private sector through workshops and briefings, as well as bilateral meetings with some entities.

The SAMA has established five Committees, including the *Anti-Financial Crimes and ML Committee* (AFCMLC) and a *Self-Supervisory Committee* (SSC) as forums to facilitate feedback between institutions and SAMA on money-laundering and terrorist financing issues respectively. Similar committees have been created for the insurance and finance company sectors. These private sector-comprised groups meet regularly to share experiences regarding compliance issues, and specifically discuss emerging risks and methodologies and risk mitigation, among other issues.

Supervisors for other sectors have also established feedback mechanisms, including a permanent committee for lawyers, and regional workshops for the real estate sector and dealers in precious metals and stones. These committees are the main channel for communicating with regulated entities about AML/CFT risks and obligations.

The FIU provides feedback directly to reporting entities on specific STRs; holds workshops for compliance officers; and takes part in the sectoral outreach workshops organised by supervisors.

Weighting and conclusion

Saudi Arabia has good mechanisms for communicating with regulated entities, and has issued up to date guidance on the implementation of new provisions and the results of the NRAs.

Saudi Arabia is compliant with R.34

Recommendation 35 – Sanctions

Saudi Arabia was rated LC with Recommendation 17 in its last Mutual Evaluation. The main deficiency was the low level of corrective measures applied by SAMA and CMA.

Criterion 35.1 - The sanctions which can be applied to deal with persons that fail to comply with AML/CFT requirements are set out in various laws and regulations, depending on the nature of the violation, and the sector concerned. There are some gaps in the range of sanctions available, as set out below.

The AMLL provides for a range of sanctions, from fines up to SAR 50 million to imprisonment and/or imprisonment up to 15 years for natural persons for violating the AMLL. In respect of FIs/DNFBPs/NPOs, sanctions could be up to the withdrawal

of licence for non-compliance with AMLL. These apply to all sectors with obligations under the AMLL (AMLL Articles 25 to 32)

The CFTL includes similar provisions. Violations of provisions of this law could invite a variety of sanctions including death sentence and imprisonment up to 30 years, depending on the nature of violations. (CFTL Arts. 30 to 57 and 83).

For the banking sector, the Banking Control Law (BCL, Art. 22) sets out a range of actions which SAMA can take in cases where a bank has failed to comply with the provisions of the BCL or of any regulations issued under it. These actions include appointing advisers; suspending or removing a director or officer of the bank; limiting or suspending the granting of credits or acceptance of deposits; and requiring other steps which SAMA deems necessary, with the approval of the Minister of Finance and National Economy. In cases where the bank persistently contravenes the law and fails to make adequate proposals to rectify the problem, SAMA may recommend that the Minister, with the approval of the Council of Ministers, revoke the bank's license35.

Further penalties are set out in the Rules for Enforcing the Banking Control Law (Ministerial decision 3/2149 of 14/10/1406H (1985) [Doc 46]. These provide SAMA with powers to apply a range of additional measures, including to require a bank to rectify a contravention; require a bank board to discuss remediation measures; appointment of advisers; appointment of an observer to the Bank's board; and any other measures deemed necessary (subject to approval by the Minister). Administrative penalties are applicable under the BCR itself for breaches of specific requirements, including two relevant to AML/CFT supervision: carrying on banking business without a license; and failing to produce documents for inspection (SAR 5 000 per day). There is also a general penalty of SAR 5 000 (EUR 1 130) for contravening any other provision of the BCL or the regulations or decisions issued in execution thereof (Art 23.1, 23.5).

For the Insurance sector, the Law on Supervision of Cooperative Insurance Companies authorises SAMA to adopt a range of measures in case of violations, including to appoint a consultant, suspend or dismiss an employee or board member, prohibit the company from taking-on new customers, and obliging the company to take other necessary actions. (Art.19). The Law also provides for a fine of up to SAR 1million (EUR 220 000) or up to four years in prison, for persons violating the Law or associated regulations.

For Financing companies, the Financing Companies Control Law sets out a range of supervisory measures available to SAMA, including the same measures available for Banking and Insurance sectors (Art. 29), as well as fines of up to SAR 250 000 (EUR 56 000) or SAR 10 000 (EUR 2 200) per day for ongoing violations.

For money exchange businesses, SAMA has wide powers to issue any instructions it deems necessary to implement requirements of supervision and control on money changing business (Rules Governing Money Changing Business). In addition, the sanctions provisions of the BCL apply to such activity.

35 As noted in the 2010 Evaluation, 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.

For the Securities sector, the Capital Market Law gives the Capital Markets Authority powers to sanction breaches of the requirements. These include interventions ranging from warning the person concerned, compelling measures to rectify the violation, forfeiting gains from any violation, and barring the person or entity from acting as a trader/broker etc. The Authority can also apply a fine of between SAR10 000 and 100 000 (EUR 2 200 - 22000) for each violation. CML, Arts 59, 60).

Breaches of targeted financial sanctions are subject to separate sanctions provisions. The AML/CFT rules for banks require name checking for sanctions screening, and failure to screen names can therefore be sanctioned using the provisions of the BCL.

Criterion 35.2 - The AMLL (Art. 25) provides that if the supervisory authority find that FIs and DNFBPs or any of their directors, board members, executive or supervisory management members failed to comply with any provision of this Law, its Implementing Regulation or relevant decisions or circulars, or any violation referred from other competent authority, the supervisory authority may impose one or more of a range of sanctions mentioned therein. Similar provision under Article 83 of CFTL is also available.

Weighting and Conclusion

Saudi Arabia is compliant with R.35

Recommendation 36 – International instruments

Saudi Arabia was rated PC with recommendation 34 (Palermo Convention not fully implemented and TF Convention not implemented) and rated NC with SR 1 related to the implementation of UN instruments (TF convention was not implemented and failings related to UNSCRs 1267, 1373 and successor resolutions have a negative impact on this Special Recommendation).

Criterion 36.1 - Saudi Arabia ratified the Vienna Convention on 9 January 1992 (Royal Decree No. M/19); the Palermo Convention on 18 January 2005 (Royal Decree No. M/20); the Merida Convention on 29 April 2013 (Council of Ministers Decision 62 Date 2/3/1434H); and the Terrorist Financing Convention on 23 August 2007 (Royal Decree No. M/62).

Criterion 36.2 **-** The criterion requires countries to fully implement the Palermo, Vienna, Merida and Terrorist Financing Convention and that implementation should include certain articles as follows: the Vienna Convention (Articles 3-11, 15, 17 and 19), the Palermo Convention (Articles 5-7, 10-16, 18-20, 24-27, 29-31, & 34), the Merida Convention (Articles 14-17, 23-24, 26-31, 38, 40, 43-44, 46, 48, 50-55, 57-58), and the Terrorist Financing Convention (Articles 2-18).

Although some of the elements referred to in the mentioned conventions such as the criminalization of ML, TF, and corruption were covered by some laws there are still elements that need to be covered under the Saudi legislation in order to fully implement the provisions of the articles of the conventions. These include some weaknesses regarding Merida convention Arts. 15, 16, 17 (to more explicitly criminalise bribery and embezzlement), Art. 48 (as reviewed under R.40); and Arts. 54, 55, 57 (as assessed under R.38); and the corresponding articles of the Vienna and Palermo conventions. In addition, it is not clear that Saudi Arabia fully implements

Article 17 of the TF Convention, which requires that "*...a person who is taken into custody or regarding whom other measures are taken or proceedings are carried out pursuant to this Convention shall be guaranteed fair treatment, including enjoyment of all rights and guarantees in conformity with the law of the State in the territory of which that person is present and applicable provisions of international law, including international human rights law.*". As set out in the effectiveness analysis of IO.9, the investigation, prosecution and trial of terrorism offences in Saudi Arabia follows a different procedure to conventional criminal cases, affecting the period of detention and access to a lawyer. These differences expose extraditions to Saudi Arabia to legal challenges in other countries.

Weighting and Conclusion:

Saudi Arabia is partially compliant with R.36

Recommendation 37 – Mutual legal assistance

Saudi Arabia was rated largely compliant with the previous recommendation 36. The deficiencies were that the PCMLA should improve its co-ordination role in order to ensure the effective follow up of the implementation of foreign MLA requests. There was no legal framework or effective mechanism for dealing with conflicts of jurisdiction which caused uncertainty about the willingness to retain jurisdiction over every investigation in these conflicts of jurisdiction cases. Effectiveness could not be confirmed and the deficiencies in the TF criminalization may impact on the ability to provide MLA.

Criterion 37.1 - Saudi Arabia can provide mutual legal assistance in ML, predicate offences and TF crimes on the basis of the AMLL and the LTCF (AMLL, Art.25 and Implementing Regulations; LTCF, Art.30). Saudi Arabia can also provide mutual legal assistance in addition to other relevant international and regional conventions, multilateral and bilateral agreements as well as the principal of reciprocity. The MLA scope includes wide range of mode/forms as set out in the mentioned Articles and in the *Mutual Legal Assistance and Asset Recovery Procedures Manual* (MLAPM) (MLAPM, Art.3). The procedures allow foreign requests to be treated rapidly (MLAPM, Art.15).

Criterion 37.2 - The Permanent Committee for MLA (PCMLA) serves as the central authority to receive and handle foreign MLA requests (MLAPM, Art.2). Although there is a working mechanism of the Permanent Committee for MLA requests (Establishment and Internal Regulation of the PCMLA). This is supplemented by an internal circular sent to the Permanent Committee for MLA requests by the ministry of Interior on 6 November 2017 (2 days before the on-site), which sets out Criteria for prioritising MLA requests: requests relating to dangerous crimes such as murder, violence crime, organized crime, terrorism, money laundering, corruption, embezzlement and other crimes requiring detention are given high priority. It is not clear that this was in operation at the time of the onsite. Saudi authorities have not shown that adequate case management systems are in place.

Criterion 37.3 - There are no unreasonable or unduly restrictive conditions under the MLA framework. There are ordinary requirements that are in line with the requirements of the international or regional conventions (MLAPM, Art.4).

Criterion 37.4 - Saudi Arabia cannot reject legal assistance requests solely on the basis of bank secrecy or because the offence involves fiscal matters (MLAPM, Art.14(4)). Information disclosed by persons who are subject to the AML Law can be disclosed to foreign counterparts (AMLL, Art.25). Information obtained by the competent authorities responsible for fighting TF can be exchanged internationally (LTCF, Art.30).

Criterion 37.5 - The Permanent Committee for MLA (PCMLA) must maintain the confidentiality of the of the MLA requests (MLAPM, Art.5). The Saudi authorities indicated that in practice only persons with special clearance would have access to the relevant database and information.

Criterion 37.6 - Dual criminality is not required for the provision of MLA where requests involve non-coercive measures. (Article 39/5 of the IR to the AMLL).

Criterion 37.7 - Dual criminality is required for assistance involving coercive measures (Article 39/5 of the IR to the AMLL). The existence of dual criminality is determined based on the criminalisation of the underlying conduct, and not on the existence of the same category or terminology. (MLAPM, Art.14(1)(c)).

Criterion 37.8 - Competent authorities may use all powers available for the investigation of crimes domestically, (Article 39/2 and 39/3 of the IR to the AMLL).

Weighting and Conclusion:

Saudi Arabia is largely compliant with R.37

Recommendation 38 – Mutual legal assistance: freezing and confiscation

Saudi Arabia was previously rated partially compliant with the former R.38 and SR.V, as there was no specific provision regarding the confiscation or seizure of property of corresponding value and international co-operation and effectiveness could not be assessed as a result of lack of implementation. Also there was no legal framework for dealing with non-ML MLA confiscation cases.

Criterion 38.1 - Article (39) of the AML Law gives the authorities the powers to implement the MLA requests relating to the detection, tracking, seizure and confiscation of funds, proceeds or instrumentalities associated with ML crimes (but not the instrumentalities intended to be used in ML). The scope of types of Funds subject to confiscation is set out in the AML and CFTL.

Article (74) of the CFT Law states that the Committee for Mutual Legal Assistance shall receive and process requests for mutual legal assistance concerning crimes set out in the CFT Law. Any property subject to confiscation in a domestic context is also subject to confiscation in an international context.

Articles (10 &11) of the MLAPM provide for expeditious action. Seizing orders should not exceed 30 days but can be extended if necessary.

Criterion 38.2 - Requests related to non-conviction based confiscation orders can be executed under the Saudi Arabian framework (MLAAPM, Art.3(10)). In cases where the offender cannot be prosecuted due to death, flight or absence, or where the offender is unknown, the PCMLA would refer such a request to the PP to undertake

the necessary action. The request would be accompanied with a statement to explain why and how the requesting country considers the funds to be associated with criminal conduct. This is sufficient to enable the executing Saudi authority to seek relevant orders under Saudi Law.

Criterion 38.3 - Article (39) of the AML Law gives the authorities the powers to implement MLA requests relating to the detection, tracking, seizure and confiscation of funds, proceeds or instrumentalities associated with ML crimes as well as whatever subject to confiscation in a domestic context. The above legislation contains arrangements regarding the seizure of ML related funds or the seizure and confiscation of funds related to predicate offences including TF. In addition the Saudi authorities indicated that the arrangement for seizure and confiscation is governed by bilateral and multilateral agreements. There are no general arrangements to co-ordinate seizure or confiscation actions with other countries, other than those contained in bilateral and multilateral agreements.

The *Public commission for the guardianship of trust fund minors and their counterparts* is responsible for managing the confiscated funds and assets in ML crimes and relevant predicate offences including TF. As per criteria 4.4, under the Article 44 of the AMLL, there is a mechanism for managing or disposing of property frozen, seized or confiscated; such a mechanism is however not clear in CFT Law. Under the AML Law, when the Public Prosecution (in the case of ML or a predicate offense) decides to seize funds that are or may become subject to confiscation, they must determine, on a case by case basis and taking into account the facts of the case, the risk of dissipation of the funds, and the nature of the property, whether the funds shall remain under the administration of the person that held an interest in it at the time of issuance of the order, or a third party, which essentially results in the property being frozen; or whether the funds shall be transferred by order from the Public Prosecution or State Security to the Public Commission for the Guardianship of Trust Funds Minors for management of the funds. In the latter case, the funds are then to be managed pursuant to the procedures applicable by the Commission.

Criterion 38.4 - The PCMLA has the power to share the confiscated funds proceeds or instrumentalities related to ML with other countries that are a signatory to a valid agreement or treaty with Saudi Arabia under the conditions of the law, although these powers have never been used in practice (AMML, Arts. 12 and 17). The provisions above deal with sharing the funds related to predicate offences including TF.

Weighting and Conclusion

It is not clear what mechanisms are in place for managing, and when necessary, disposing of property frozen, seized or confiscated.

Saudi Arabia is Largely compliant with R.38.

Recommendation 39 – Extradition

In its 1st MER, Saudi Arabia was rated largely compliant with the previous R. 39. The main deficiencies were not clear how Saudi Arabia authorities submit the case to its competent authorities for prosecution pf the offences where extradition has been

refused, extradition on the basis of reciprocity not effective and the effectiveness of the system could not fully confirmed.

Criterion 39.1 -

(a) ML and TF are extraditable offences. The terms of extradition are set out in laws, multilateral and bilateral agreements concluded by Saudi Arabia, and 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". Extradition requests are granted pursuant to a multilateral or bilateral agreement or on the basis of reciprocity.

Extradition can be obtained through: (1) an extradition treaty between Saudi Arabia and the requesting country; (2) a multilateral agreement to which both Saudi Arabia and the requesting party are signatories, and which contains provisions on extradition; or (3) a specific agreement entered into between Saudi Arabia and the requesting country with respect to a person or persons in a particular case. Alternatively, Saudi Arabia may provide extradition in ML/TF cases on the basis of reciprocity. Saudi Arabia has concluded many agreements that include extradition for example criminal extradition between Egypt, Jordan, the Arab Riyadh Agreement on Judicial Cooperation, the Arab Agreement on Terrorism Combating, and the GCC Security Agreement. In addition, Saudi Arabia has concluded a bilateral agreement with many countries, such as Kuwait, Oman, Pakistan, Qatar, UAE, and Yemen, Algeria, India, Spain, Germany, and Italy. Extradition is also made based on other international conventions, such as the Palermo Convention, the Merida Convention, and the TF Conventions. (Article (41) of the AML Law and Article (73) of the CFT Law).

(b) An internal circular sent to the Permanent Committee for MLA requests by the ministry of Interior on 6 November 2017 sets out Criteria for prioritising MLA requests. The Public Prosecution has internal structures and procedures to execute extradition requests, including dedicated MLA departments in central and regional offices. However, Saudi authorities have not shown that adequate case management systems are in place to monitor progress and ensure timely execution of requests.

(c) With respect to unreasonable or unduly restrictive conditions, generally, the preconditions for Saudi Arabia to grant the extradition is that the requesting country is signatory to a valid treaty or agreement that Saudi Arabia also has signed.

Criteria 39.2 - Saudi Arabia does not extradite Saudi nationals normally. Saudi Arabia has concluded several bilateral agreements with neighbouring countries from GCC, which do allow for such extradition of Saudi nationals (although these may still be refused for reasons of nationality). When an extradition request is denied for nationality reasons, the case can be tried before competent courts in Saudi Arabia on the basis of evidence provided by the requesting country (AMLL, Art 41).

Criterion 39.3 - Saudi Arabia requires dual criminality for extradition under the Saudi Arabian legal framework; Article (41/3) AMLL IR and Article (73) of the CTF Law indicates that extradition shall be subject to dual criminality and the dual criminality principal is available when the requesting country and the Kingdom criminalized the act subject to the extradition, regardless the classification of the act as per the criminal laws.

Criterion 39.4 - Saudi Arabia can follow simplified procedures in cases where a person does not contest extradition and waives formal extradition proceedings.

Weighting and Conclusion

Saudi Arabia's legal framework for extradition includes all the required elements; however, it has not shown that case management systems and processes are in place.

Saudi Arabia is largely compliant with R.39.

Recommendation 40 – Other forms of international co-operation

Recommendation 40 was rated partially compliant in the MER published in 2010. The reason for the rating was due to the insufficiency of international co-operation by supervisors (SAMA and CMA) FIU (SAFIU) and Customs. Also, there was an unclear legal basis for some forms of international co-operation by some law enforcement bodies. Finally, statistics to confirm effectiveness for most forms of international co-operation, especially by supervisory bodies and the FIU were lacking.

Criterion 40.1 - The AMLL and its implementing regulations give broad powers to the authorities to provide a wide range of assistance to a foreign country, including any form of assistance available in relation to a domestic investigation in relation to ML, associated predicate offences and TF. The law neither requires nor prevents rapid or spontaneous co-operation (AMLLIR, Art.39/2, 39/3, and Article 72 of the CTF Law).

Criterion 40.2 – (a, b, c) Competent authorities have a lawful basis for providing co-operation, provided in the AMLL (Art.39). These are supplemented by bilateral and multilateral arrangements applicable to the FIU (including the Egmont group), supervisors, and law enforcement authorities (including Interpol). There are no specific restrictions on the means used to co-operate or on the channels used.

(d and e) Saudi Arabia authorities have not shown that clear case management systems or processes exist for the timely execution of requests. Prioritisation criteria were introduced in November 2017 as noted in the analysis of c39.1(b) above. Except for the FIU, there are no specific arrangements for safeguarding information received from international partners, although all relevant agencies apply the same safeguards which they apply to domestic information (AMLLIR, Art.17/3). Article 87 of the LTCF stipulates that any person concerned with the implementation of the provisions of this law shall maintain the confidentiality of information he becomes privy to, and such information may not be disclosed except for the use of the competent authorities.

Criterion 40.3 - The SAFIU can enter into MOUs by virtue of AMLL, and to date has concluded 28 MOUs. Competent authorities are required to co-ordinate with the FIU when exchanging financial or non-financial information pertinent to persons or entities identified in accordance with the provisions of the AMLL.

Criterion 40.4 - SAFIU and supervisory authorities provide feedback to foreign authorities when requested. The relevant laws do not prevent the competent authorities from providing feedback on any request or exchange of information, but Saudi Arabia has not demonstrated that other authorities provide feedback.

Criterion 40.5 - Exchange of information and assistance between competent authorities and their counterparts does not face any unreasonable or unnecessary restriction:
(a) Bilateral agreements signed with counterparts provide that the request of assistance shall not be refused on the ground of the request involved fiscal matters.
(b) Financial institution secrecy laws and data protection requirements do not affect co-operation between authorities.
(c) requests may be postponed if the implication of such request would impede the ongoing investigation, proceedings or judicial procedures, but not simply because an investigation exists.
(d) Authorities are permitted to co-operate with counterparts regardless of their nature and status. (AMLLIR Arts 24, 39)

Criterion 40.6 - Information is required to be used only for the purpose for which it was requested, and should be disclosed to a third party unless otherwise approved by the relevant local authority. Additionally, bilateral agreements and the MLAPM contain provisions to ensure that information exchanged to be used only for the purpose for which it was requested or submitted. (AMLLIR, Art 22.1)

Criterion 40.7 - Article 87 of the CFTL provides for maintaining the confidentiality of information any person becomes privy to concerned with the implementation of the provisions of this Law except for the use of the competent authorities. Also, no disclosure may be made to any person of any of the reporting, inquiry, investigation or trial procedures, or of data related thereto, in respect of any of the crimes of terrorism or its financing.

Criterion 40.8 - Competent authorities can conduct inquiries and exchange any information that would be available in relation to a domestic inquiry. (AMLL Art 38, CFTL Art 72, and bilateral agreements)

Financial Intelligence Unit

Criterion 40.9 - The FIU may seek from or share with a foreign counterpart any information it has received in the course of its functions, and may enter into an agreement or arrangement as per the legal procedures to facilitate the exchange of information with a foreign concerned authority.(AMLL Art???, CFTL Art 81)

Criterion 40.10 - SAFIU is authorised to, and does, provide feedback to foreign counterparts on the use of information and the outcomes achieved. (AMLIR Art22)

Criterion 40.11 - SAFIU can share with counterparts all information that it can obtain domestically (AMLL Art.22).

Financial Supervisors

Criterion 40.12 - Supervisory authorities are authorised to exchange any information with counterparts, on the basis of agreements or reciprocity. (AMLLIR Art 24/1, LTCF Art 72)

Criterion 40.13 and 40.14 - There are no restrictions on the types of information which supervisory authorities may exchange with foreign counterparts for anti-money laundering or terrorist financing purposes: all domestically available information can be shared, including regulatory, prudential, and AML/CFT information. (AMLL art 24, 38, AMLLIR Art 24/1; LTCF Arts 72, 82).

Criterion 40.15 - Supervisory authorities are entitled to make queries on behalf of foreign counterparts and facilitate the ability of a foreign counterpart to carry out group supervision. (AMLLIR Arts 24/3)

Criterion 40.16 - Supervisory authorities are obliged to obtain prior authorisation from foreign counterparts before disseminating information, or to inform them if obliged to disclose information. (AMLLIR Art 24/2)

Law Enforcement Authorities

Criterion 40.17 - Law enforcement authorities may exchange any domestically available or accessible information with foreign counterparts for intelligence or investigative purposes relating to money laundering and associated predicate offenses, including for purpose of identifying, tracing or securing proceeds or instrumentalities of crime. (AMLL Art 38; AMLLIR Art 38/2; CFTL Art 72)

Criterion 40.18 - All powers available in a domestic case may be used to conduct inquiries and obtain information on behalf of a foreign counterpart. (AMLLIR Arts. 39/2 and 39/3)

Criterion 40.19 - Criminal investigating officers may form joint intelligence teams to conduct co-operative intelligence or establish bilateral or multilateral arrangements to enable such joint intelligence - e.g. under the bilateral agreement with Spain, or the multilateral *Gulf Security Convention* (AMLLIR Art.38/2).

Criterion 40.20 - There is no restriction preventing diagonal co-operation with non-counterparts (other than limitations on further dissemination without authorisation, as set out above).

Weighting and conclusion:

Saudi Arabia's very recently updated legal framework for international co-operation is comprehensive, and includes all the required elements, though minor gaps remain with respect to building systems and processes for managing cases, and to provide feedback to foreign counterparts.

Saudi Arabia is largely compliant with R.40.

Summary of Technical Compliance – Key Deficiencies

Compliance with FATF Recommendations		
Recommendations	**Rating**	**Factor(s) underlying the rating**
1. Assessing risks & applying a risk-based approach	LC	• The CFT law, regulations, and rules do not define the nature of simplified measures or the scenarios in which they could be applied, and do not permit DNFBPs to apply simplified measures.
2. National co-operation and co-ordination	LC	• The Action Plan does not yet fully reflect the risks identified in the NRAs, • The FIU is not a direct member of PCCT or the Ch.VII Committee
3. Money laundering offense	C	The Recommendation is fully met
4. Confiscation and provisional measures	LC	• It is not clear what mechanisms are in place for managing, and when necessary, disposing of property frozen, seized or confiscated.
5. Terrorist financing offense	C	The Recommendation is fully met
6. Targeted financial sanctions related to terrorism & TF	PC	• It is unclear whether the measures in place ensure that the sanctions will be without delay in all cases. • Not all natural and legal persons in Saudi Arabia are required to freeze the funds and assets of designated persons. • Saudi TFS mechanisms do not specifically prohibit nationals and persons within the jurisdiction from making any funds and other assets available to designated individuals and entities, although the criminal legislation in part mitigates this issue. • The procedures for de-listing and unfreezing the funds are not clear.
7. Targeted financial sanctions related to proliferation	PC	• The Ch.VII Committee does not include some relevant agencies • It is unclear how the relevant FIs/DNFBP supervisors missing in the Committee would implement the relevant obligations • No supervisory authority has yet published procedures to implement the provisions of UN Resolutions; • In the absence of procedures for implementation, it is unclear whether this obligation would cover the reporting of attempted transactions. • The authorisation to release certain funds may be granted when the Chapter VII Committee has determined that the funds shall be used for a payment by a person or body designated by the Sanctions Committee or United Nations Security Council in accordance with a relevant UN Resolution. This is not fully in line with the standard in that the payment should not be made to a designated person.
8. Non-profit organisations	LC	• Saudi Arabia has not conducted a comprehensive risk assessment that allows them to identify the nature of threats posed by terrorist entities and specifically identify how terrorist actors abuse NPOs • Saudi Arabia's risk-based approach is based primarily on a financial integrity health check and lacks specifics regarding other terrorist financing indicators
9. Financial institution secrecy laws	C	The Recommendation is fully met
10. Customer due diligence	C	The Recommendation is fully met
11. Record keeping	C	The Recommendation is fully met
12. Politically exposed persons	C	The Recommendation is fully met
13. Correspondent banking	C	The Recommendation is fully met
14. Money or value transfer services	C	The Recommendation is fully met

15. New technologies	LC	• There is no national-level risk identification and assessment of new technology
16. Wire transfers	LC	• There is no explicit requirement on institutions to file STRs in any countries affected and make relevant information available to the FIU.
17. Reliance on third parties	C	The Recommendation is fully met
18. Internal controls and foreign branches and subsidiaries	C	The Recommendation is fully met
19. Higher-risk countries	C	The Recommendation is fully met
20. Reporting of suspicious transaction	C	The Recommendation is fully met
21. Tipping-off and confidentiality	C	The Recommendation is fully met
22. DNFBPs: Customer due diligence	LC	• There is no national-level risk identification and assessment of new technology (as in R.15).
23. DNFBPs: Other measures	C	The Recommendation is fully met
24. Transparency and beneficial ownership of legal persons	LC	• Saudi Arabia has not sufficiently assessed the ML/TF risks associated with all types of legal persons • Authorities do not monitor the quality of assistance received from other countries in relation to basic and beneficial ownership of legal persons
25. Transparency and beneficial ownership of legal arrangements	LC	• For a waqf, the law does not require the trustee to determine whether any other natural person exercises ultimate effective control over the waqf; or to hold information on other regulated agents of, and service providers to, the waqf, • In relation to foreign trust, as indicated under c.25.1.c, there is no obligation for professional trustees to keep information on a trust available; • The information available with the competent judge, the trustee, does not necessarily include information on the beneficial owner of the legal arrangement
26. Regulation and supervision of FIs	C	The Recommendation is fully met
27. Powers of supervisors	C	The Recommendation is fully met
28. Regulation and supervision of DNFBPs	C	The Recommendation is fully met
29. Financial intelligence units	LC	• Some of the rules regarding the dissemination of confidential information have not been verified; • Operational analysis is not always conducted in line with criterion 29.4(a), • The mechanisms that enable the SAFIU to remain operationally independent and autonomous now that it is under the Presidency of State Security are not all clear.
30. Responsibilities of law enforcement and investigative authorities	LC	• The instruments that provide the law enforcement authorities with the responsibility for the preliminary investigation of ML, predicate offences, and TF have not been made clear
31. Powers of law enforcement and investigative authorities	LC	• Saudi Arabia lacks mechanisms to identify assets that are not held with banks, without prior notification to the owner.
32. Cash couriers	LC	• It is not clear if the declaration system for BNI had been implemented at the time of the assessment
33. Statistics	PC	• Saudi authorities do not maintain comprehensive statistics on ML investigations, prosecutions, and convictions; or on property frozen, seized, and confiscated in relation to ML or predicate offences; or on direct co-operation with foreign law enforcement and security authorities. • There is no central point which compiles or co-ordinates AML/CFT statistics and the coverage and quality of information is variable.

		• Authorities do not use common definitions and methods, so data from different authorities is not comparable.
34. Guidance and feedback	C	The Recommendation is fully met
35. Sanctions	C	The Recommendation is fully met
36. International instruments	PC	• Saudi Arabia does not fully implement Merida convention Arts. 15, 16, 17 (to explicitly criminalise bribery and embezzlement); Arts 48, 54, 55, 57, and the corresponding articles of the Vienna and Palermo conventions. • It is not clear that Saudi Arabia fully implements Article 17 of the TF Convention
37. Mutual legal assistance	LC	• Saudi authorities have not shown that adequate case management systems are in place, or that prioritisation of requests was taking place at the time of the assessment.
38. Mutual legal assistance: freezing and confiscation	LC	• It is not clear what mechanisms are in place for managing, and when necessary, disposing of property frozen, seized or confiscated.
39. Extradition	LC	• Saudi authorities have not shown that adequate case management systems are in place.
40. Other forms of international co-operation	LC	• Saudi Arabia authorities have not shown that clear case management systems or processes exist for the timely execution of requests • Saudi Arabia has not demonstrated that other authorities provide feedback.to foreign counterparts

Glossary of Acronyms

Abbreviation	Full name in English
ADD	The Anti-Drugs Directorate
AMLL	Anti-money laundering law
AMLL IR	Anti-money laundering law implementing regulation
AMLPC	Anti Money Laundering Permanent Committee
BNI	Bearer negotiable instruments
CFTL	Counter-terrorist financing law
CFTL IR	Counter-terrorist financing law implementing regulation
CMA	Capital Market Authority
CR	Commercial register
ECD / ECU	Economic Crimes Division / Unit within the PP
Edaa	Securities Depository Center Company
FTF	Foreign terrorist fighter
GAZT	The General Authority of Zakat
GDNC	General Directorate of Narcotics Control
GID	The General Intelligence Directorate or Mabaheth
GSD	Directorate of General Security
Hajiri calender	Islamic lunar calender used in Saudi Arabia
Hajj	Pilgrimage to Mecca at specific times of the year; the fifth pillar of Islam.
LEA	Law enforcement authority
MLA	Mutual legal assistance
MLSD	The Ministry of Labour and Social Development
MOCI	The Ministry of Commerce and Investment
MOF	Ministry of Finance
MOI	Ministry of Interior
MOJ	The Ministry of Justice
NRA	National risk assessment
OCA	Other Control Authorities
PCCT	Permanent Committee for Counter Terrorism
PCLAR	The Permanent Committee for Legal Assistance Requests
PP	Public Prosecution (formerly BIPP: Bureau of Investigation & Public Prosecution
PSD	The Directorate of Public Security (PSD)
QFI	Qualified Foreign Investor
SAFIU	Saudi Arabia Financial Intelligence Unit, also referred to as the General Directorate of Financial Intelligence
SAGIA	Saudi Arabia General Investment Authority
SAMA	Saudi Arabian Monetary Authority
SAR	Saudi Riyal
SCC	The Specialised Criminal Court
SME	Small and medium sized businesses
SOCPA	Saudi Organisation of Certified Public Accounts
Sukuk	Shari'ah compliant bonds; securities representing ownership of assets
Tadawul	Saudi Stock Exchange
Umrah	Pilgrimage to Mecca that may be performed at any time of the year.
Waqf	Islamic endowment of property to be held in trust

ANNEX A. Databases that the SAFIU has access to

Note. The SAFIU may access other information from reporting entities and from other LEAs and OCAs. See R.29 and Chapter 3 (Immediate Outcome 6) above.

Database	Direct or indirect access	Number of fields
Automated Civil Affairs Register	Direct	60
Saudi Citizenship Register	Direct	90
Border and Pilgrimage Register	Direct	41
Automated Expat Affairs Register	Direct	77
Sponsorship Register	Direct	18
Drug Register	Direct	41
Criminal Records Register	Direct	44
Wanted Individuals Investigation Register	Direct	43
Wanted Individuals Register	Direct	22
Driving License Register	Direct	44
Shamus Register (Tourist Information)	Direct	Dependent on nature of enquiry
Ministry of Justice Register (Land and Deeds)	Direct	Dependent on nature of enquiry
Ministry of Commerce and Investment Register (Commercial Register)	Direct	Dependent on nature of enquiry
Public Database Search	Direct	Dependent on nature of enquiry
SAGIA (data on investors)	Direct	Dependent on nature of enquiry
Customs Authority (declaration and non-declaration)	Direct (uploaded regularly)	Dependent on nature of enquiry
Customs Authority (Import and Export Data)	Indirect	Dependent on nature of enquiry
World Check	Direct	Dependent on nature of enquiry
General Organisation for Social Insurance	Indirect (agreement in place to enable direct access)	Dependent on nature of enquiry

www.fatf-gafi.org | www.menafatf.org

September 2018

Anti-money laundering and counter-terrorist financing measures - Kingdom of Saudi Arabia

Fourth Round Mutual Evaluation Report

In this report: a summary of the anti-money laundering (AML) / counter-terrorist financing (CTF) measures in place in Saudi Arabia as at the time of the on-site visit on 8-23 November 2017.

The report analyses the level of effectiveness of Saudi Arabia's AML/CTF system, the level of compliance with the FATF 40 Recommendations and provides recommendations on how their AML/CFT system could be strengthened.