FATF

MENAFATF
مينافاتف
GAFIMOAN

# Anti-money laundering and counter-terrorist financing measures

# Kingdom of Bahrain

## 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 - Bahrain,*
Fourth Round Mutual Evaluation Report, FATF, Paris
http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-bahrain-2018.html



Photo Credit - Cover: © Central Bank of Bahrain

# Table of contents

# Executive Summary

1. This report summarises the AML/CFT measures in place in the Kingdom of Bahrain as at the date of the on-site visit (7-22 November 2017). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Bahrain's AML/CFT system, and provides recommendations on how the system could be strengthened.

## *Key Findings*

- Overall, Bahrain has a moderate level of understanding of its money laundering and terrorist financing (ML/TF) risks, with the national risk assessment (NRA) process on going at the time of the onsite. The understanding of ML/TF risks is still evolving and will be further developed as the NRA process is concluded.
- Domestic coordination, cooperation and information exchange at the operational level is strong and proactive. There have been a number of initiatives, policies and actions by authorities to address ML/TF risks. However, more generally, the objectives and activities of authorities will need to be strengthened and aligned with the identified ML/TF risks.
- Financial intelligence and other information are accessed and used in investigations for ML/TF and associated offences. During 2012-2017, Bahrain initiated 43 investigations for ML, resulting in nine convictions, and a number of ongoing cases. However, the investigation and prosecution of ML, generally, do not appear to be fully in line with its ML risks.
- Bahrain's terrorism offence (which is cross referenced in the TF offence) includes an exemption that is inconsistent with the TF Convention. This exemption significantly impacts Bahrain's compliance at the technical level, but has not yet had a discernible impact on effectiveness. TF activities are identified and investigated by LEAs, though TF is mostly identified as a result of terrorism investigations. Given the strong domestic coordination in Bahrain, information and intelligence is rapidly exchanged in TF cases.
- Financial institutions in Bahrain immediately implement TFS (both PF and TF) without delay. However, the majority of the DNFBP sector does not implement TFS without delay, and the remaining DNFBPs (as well as all natural and legal persons in Bahrain) do not have legal obligations in relation to TFS.
- Bahrain identified a subset of high risk NPOs for potential terrorism abuse. Yet, restrictive obligations are placed on all NPOs operating in Bahrain, regardless of their identified risk profile. While these measures may be effective at mitigating TF

abuse of the NPO sector, they are not applied on a risk-basis and may unduly or inadvertently restrict NPO's ability to access resources, including financial resources, to carry out their legitimate activities.

- In the financial sector, the application of proportionate mitigating measures by large financial institutions is robust. Progress still needs to be made regarding the understanding and implementation of beneficial ownership obligations. Implementation of preventive measures, including suspicious transaction reporting by the DNFBP sector needs improvements.
- Bahrain has strong controls to prevent criminals from beneficially owning a significant or controlling interest or holding a management function in a financial institution. The CBB has strong elements of a risk based approach to supervision and requires remediation from institutions it supervises. It has imposed a range of sanctions and made referrals for prosecution, though there is scope to increase the use of sanctions as the level of onsite supervision increases.
- International cooperation between Bahraini authorities and foreign counterparts is collaborative and provided upon request and spontaneously, with priority given to terrorism and TF. Mutual Legal Assistance (MLA) requests are mainly used as complementary tools, in addition to more informal cooperation channels.

## *Risks and General Situation*

2. Bahrain is a regional financial and trading hub with a liberal business environment. Bahrain's economy has shown steady growth during in recent years despite the financial meltdown in 2008-2009. Bahrain's real GDP was USD 31.8 billion in 2016, and grew by around 3.3% from that in 2015. Oil comprises 75.6% of the country's budget revenues and 20% of its GDP. Bahrain enjoys a strong, diverse, and competitive economy which promotes business growth. The financial services sector accounted for 16.5% of the real GDP in 2016, and is the largest non-oil contributor to the GDP.

3. Bahrain is exposed to domestic ML/TF risks, and the ML/TF risks associated with cross-border customers and activity. Bahrain is currently undertaking its first formal and comprehensive National Money Laundering and Terrorist Financing Risk Assessment (NRA). The NRA process is organised and led by the National Policy Committee (NPC) and carried out by working groups representing relevant AML/CFT stakeholders in the country, including private sector.

4. As per the draft NRA as at the time of onsite, the most important ML threats are investment fraud, cash courier/cross-border violations including smuggling and immorality and prostitution. The banking sector is considered to be the most targeted sector for ML, with money changers, custodians and real estate being medium risk targets.

5. Bahrain is also exposed to geopolitical risks, most notably in relation to TF. According to the authorities, the risk of terrorism and TF is high. Though the understanding of risk is still being finalised, Bahrain identifies the most prevalent and high risk TF areas as: cash smuggling via land and sea (i.e. foreign funding); NPOs; and fundraising.

## Overall Level of Compliance and Effectiveness

### *Assessment of risk, co-ordination and policy setting (Chapter 2; IO.1, R.1, 2, 33 & 34)*

6. Bahrain is currently undertaking a ML/TF NRA, with most of the relevant authorities contributing to the process. It is moving forward methodically and the NRA process will continue to build on existing sectoral assessments carried out by the Central Bank of Bahrain (CBB) and the Ministry of Industry Commerce and Tourism (MOICT), which has a dual role: registrar of legal persons and DNFBP supervisor for dealers in precious metals and stones, accountants and auditors and real estate agents which are structured as companies (until September 2017 at which point, real estate sector was transferred to a separate authority). Understanding of ML/TF risks is still evolving and will be further developed as the NRA process is concluded. At the time of the onsite a draft NRA report had been prepared.

7. The assessment of risks both in general, and in a range of particular areas, needs to be deepened so as to allow substantiated conclusions on risks, and their relative importance from a national perspective. There should also be more in depth analysis in certain areas, including the threats from, and vulnerabilities to, cross-border flows; legal persons and legal arrangements; and, organised crime. This would enable Bahrain to reach robust conclusions.

8. The Bahrain has a longstanding co-ordination framework, which covers AML/CFT and combatting of PF. Domestic co-operation and information exchange at the operational level is strong and visible and a number of informal exchanges also occur, for example in the context of national security. There is strong domestic coordination by the authorities within the Ministry of Interior (MOI) and the National Security Agency (NSA) in relation to investigations of terrorism and TF offences and to progress investigations once started. This enables intelligence to be shared rapidly in all cases between various units of the MOI involved in these cases and the NSA.

9. The NPC with its subcommittee, the Legislation/Policy Committee, sets and coordinates AML/CFT policy. There is also a separate committee, the National Committee on the Implementation of UNSCRs, which follows up on the implementation of UNSCRs. The NPC develops 3-5 year strategies, which can be updated as needed. However, the existing strategy and action plans do not constitute a comprehensive national policy to address key risks. The absence of agreed and fully articulated ML/TF risks at national level means that the authorities have not been well placed to direct their objectives and policies towards the highest national risks.

### *Financial intelligence, ML investigations, prosecutions and confiscation (Chapter 3; IO.6, 7, 8; R.1, 3, 4, 29–32)*

10. Bahraini Financial Intelligence Directorate (FID) is a law enforcement FIU and is well integrated through electronic systems and direct communication channels with other agencies. Financial intelligence and other information are accessed and used in investigations for ML, TF and associated predicate offences,

including for the development of evidence for associated predicate offences. The FID has access to several databases which enhance its ability to produce financial intelligence of quality using a variety of sources.

11. There is strong and effective co-operation and co-ordination between FID and other law enforcement authorities including national security agencies and supervisors. The FID is supporting the operational needs of law enforcement agencies to a considerable extent; however, more in depth strategic analysis on emerging trends and typologies is needed to better support the work of all the competent authorities.

12. Bahrain has a sound legal framework for the investigation of ML. The initial investigation of ML cases is carried out by the FID and referred to the Public Prosecution Office (PPO) for judicial investigation. The PPO and FID work collaboratively with other relevant competent authorities in the course of ML investigations and prosecutions. In recent years, Bahrain has pursued more complex ML investigations and among the ML cases provided, both small and large-scale ML cases exist, including various types of ML offences. However overall, the assessment team has concerns that Bahrain does not consistently and systematically investigate and prosecute ML in line with its ML risks.

13. A wide range of sanctions are imposed for ML offences for natural and legal persons. In practice, of the 34 individuals convicted of ML during 2012-17, the average sanction applied was four years, with the highest sentence applied being seven years' imprisonment and included fines up to BHD 200 000 (EUR 431 077).

14. Bahrain's legal framework for seizing, freezing and confiscating assets is adequate and has been used to some extent. The disclosure system for incoming and outgoing cross border currency movements and BNIs was significantly strengthened at the time of the onsite. There is, however, no specific policy or guidelines requiring law enforcement agencies to pursue confiscation as a policy objective, though, authorities seem to pursue it as part of a larger proceeds-of-crime approach to combat crime. More generally, confiscation results can be considered modest, taking into account Bahrain's risk profile.

### *Terrorist and proliferation financing (Chapter 4; IO.9, 10, 11; R. 1, 4, 5–8, 30, 31 & 39.)*

15. Bahrain's terrorism offence includes an exemption which is cross-referenced in its TF offence, and is inconsistent with the TF Convention. This exemption significantly impacts Bahrain's compliance at the technical level, though it does not have a discernible impact on effectiveness, as it has not been used as a defence in court or by authorities to limit their identification or investigation of TF.

16. The authorities have an evolving understanding of TF threats in Bahrain. TF activities are identified and investigated by LEAs, though TF is mostly identified as a result of terrorism investigations. As a result, the assessment team has concerns that Bahrain is not proactively pursing TF investigations and prosecutions as a preventive measure to identify and financially disrupt terrorists. Sanctions imposed in TF cases are effective, proportionate and dissuasive.

17. Financial institutions in Bahrain immediately implement the relevant UNSCRs related to TFS, as they are legally obliged to comply with UN Chapter VII

designations without the need for additional orders from Bahraini authorities. DNFBPs supervised by the MOICT [real estate agents which are structured as companies (until September 2017 at which point, real estate sector was transferred to a separate authority, RERA under SLRB), DPMS, accountants and auditors] also have a legal obligation to implement TFS upon notification by the MOICT. However, changes to the relevant lists were not communicated without delay by the MOICT prior to the end of the onsite visit, though the MOICT changed its procedures subsequently.

18. The CBB and MOICT verify their respective reporting entities' compliance with UNSCR obligations during onsite and offsite inspections. Understanding and implementation is varied and limited, particularly outside the financial sector. The assessment team also had serious concerns about a case where a financial institution permitted access to an account by a UN 1267 listed individual.

19. In regard to PF, Bahrain has no trading relations with Iran or the DPRK; however given the geographical proximity to Iran, PF exposure risks do exist. Bahrain's customs officials have an advanced understanding of the risks of proliferation and PF, including diversion and sanctions evasion. Case studies exist that demonstrate that the competent authorities are monitoring and ensuring compliance with PF related TFS, including the application of the CBB's most severe administrative penalties, as well as the pursuit of criminal charges. Detailed guidance and outreach on PF by the relevant supervisors will further help mitigate the PF risk.

### *Preventive measures (Chapter 5; IO.4; R.9–23)*

20. Bahrain has a diverse financial industry with banks as the key players. The Financial Crime Module (FC Module) issued by the CBB is recognised as a solid base for understanding and complying with AML/CFT obligations across financial sector. Understanding of ML/TF risks and commensurate mitigating measures across FIs and DNFBPs vary depending on the nature of the sector. Banks, MVTS, insurance and securities have a good understanding of ML risks and in some instances, less understanding of TF risks. The level of understanding of ML/TF risks among DNFBP sector in general needs improvements. Implementation of CDD measures is relatively less robust in the DNFBP sector. Some elements of the CDD process, such as identifying and verifying the identity of beneficial ownership need to be improved across the financial and DNFBP sectors.

21. Banks, money changers and MVTS providers are the largest contributor to STRs with five banks filing nearly 52% of the total STRs filed by the banking sector. This is in line with the overall risk and context of Bahrain. Both the level and quality of reporting done by DNFBPs needs major improvements. Authorities indicated that the quality has improved over last few years and the level of defensive reporting from the sector has reduced, though the assessment team has concerns about very low level of reporting by the DPMS and absence of any reporting by the real estate sector, in particular during the last five years.

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

22. The CBB supervises the financial sector, including trust service providers, and has strong controls to prevent criminals from beneficially owning a significant

or controlling interest or holding a management function in a FI. The Ministry of Justice (MOJ) has reasonable controls in relation to the fitness and properness at initial licensing of lawyers and thereafter. The MOICT also has reasonable controls at initial registration and thereafter to prevent criminal ownership and control of its supervised entities.

23. The CBB has strong elements of a risk-based approach to supervision and it reviews significant offsite information (including STRs), which informs onsite inspections and the use of other supervisory tools to address risk. The CBB has imposed a range of sanctions and made referrals for prosecution. There is scope to increase the use of sanctions as the level of onsite supervision increases.

24. The MOICT has put in place a framework for, and a largely risk based approach to supervision (it too reviews STRs and, in addition, auditors' reports on the quality of AML/CFT controls). The MOICT has also risk graded each DNFBP it supervises and uses both onsite and offsite monitoring tools, though further enhancements are needed to ensure a more comprehensive risk based approach.

### *Transparency and beneficial ownership (Chapter 7; IO.5; R.24, 25)*

25. Bahrain is yet to conduct a comprehensive assessment of the ML/TF risks posed by legal persons created in the country.

26. Bahrain has a centralised registry for companies, partnerships and individual establishments (Sijilat system). Basic and legal ownership information is accurately and adequately kept. The registry is frequently updated, searchable on different parameters and user friendly.

27. The registry includes information on authorised signatories, board of directors and shareholders. The registry also separately captures names of all shareholders who own 5% and above in a company's shares as well as names of ultimate natural person who is the beneficial owner of the shares (however it lacks reference to those who may control a legal person through means other than ownership). The beneficial ownership is relatively easily traced through the Sijilat system where no foreign ownership or control is involved.

28. The MOICT has a dual role in Bahrain's AML/CFT regime: as DNFBP supervisor and as registrar of legal persons and needs further resources to fulfil its mandate effectively.

29. Information related to Waqfs is available through a court order in the Sharia Courts and Waqfs councils, which supervise and manage Waqfs to preserve their state. With regard to trusts, authorities have access, upon request, to all information relating to trust service providers, available with the CBB. No specific instances of abuse of trusts or Waqfs had come to the notice of authorities thus far.

### *International co-operation (Chapter 8; IO.2; R.36–40)*

30. International cooperation is an important element for Bahrain, given its role as a financial and business centre. Bahrain sends and responds to MLA requests for both ML and predicate offences and uses informal cooperation mechanisms for a variety of purposes, including TF. Formal bilateral agreements are signed at the request of counterparts, although no agreements or MOUs are required under

Bahraini law to provide MLA or exchange information. Bahrain takes a collaborative approach towards requests and it has not refused an international cooperation request because of a lack of reciprocity.

31. The number of outgoing MLA requests is not fully in line with the ML/TF risk profile of Bahrain. However, the FID exchanges information related to ML/TF through other channels. The FID is active on outgoing exchange of information requests particularly for ML cases. The CBB has the authority to, and has exchanged supervisory information with its international counterparts when relevant to AML/CFT.

32. Extradition requests are fulfilled by Bahrain in a timely manner, given that: i) no complaints with regard to extradition were noted by counterparts; and ii) the fact that by law, the average time to process extraditions cannot exceed 30 days (which could be extended to a maximum of 60 days), unless a reason is given by the requesting state. The number of both incoming and outgoing extradition requests is significant considering Bahrain's size and context.

### *Priority Actions*

- Bahrain should finalise its NRA, including by utilising information from outside Bahrain; utilising more statistics and ensuring that the statistics used are robust; further analysing external risks and the risks of organised crime; and reviewing the DNFBP sectors in more detail. Assessment of TF risk should improve in depth and coverage.
- Bahrain should develop and implement national AML/CFT policies based on the findings of the ML/TF risk assessment and provide a clear strategy as well as action plans to address the risks identified.
- Bahrain should prioritise the investigation and prosecution of all types of ML in accordance with the country's risks, in particular cross-border risks.
- Bahrain should develop policy guidelines and strategies on seizures and confiscation in order to ensure a consistent approach across LEAs. Bahrain should also take measures to adequately track trends and results obtained in this regard.
- Bahrain should urgently amend its terrorism offence (which is cross-referenced in its TF offence) to remove the exemption as it is inconsistent with the TF Convention.
- Bahrain should seek to routinely identify and investigate TF as a distinct criminal activity instead of investigating TF primarily as part of terrorism cases.
- Bahrain should implement mitigation measures that are commensurate to the risks identified through its review of the NPO sector and understanding of the TF risks in the sector. A targeted risk based approach, outreach and guidance on how to identify, prevent and report TF, with a focus on those NPOs assessed as higher risk for potential TF abuse would help avoid restricting and disrupting legitimate NPO activities.

- Bahrain should further develop the understanding of the ML/TF risks being faced by the financial sector and DNFBPs, in particular by communicating the findings of NRA once finalised and through proactive engagement.

## *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 |
|---|---|---|---|---|---|
| Moderate | Substantial | Substantial | Moderate | Moderate | Substantial |
| **IO.7 - ML investigation & prosecution** | **IO.8 - Confiscation** | **IO.9 - TF investigation & prosecution** | **IO.10 - TF preventive measures & financial sanctions** | **IO.11 - PF financial sanctions** | |
| Moderate | Moderate | Moderate | Moderate | Moderate | |

### *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 |
| PC | LC | LC | C | PC | 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 | LC | C | LC |
| **R.13** – Correspondent banking | **R.14** – Money or value transfer services | **R.15** –New technologies | **R.16** –Wire transfers | **R.17** – Reliance on third parties | **R.18** – Internal controls and foreign branches and subsidiaries |
| LC | LC | C | LC | C | LC |
| **R.19** – Higher-risk countries | **R.20** – Reporting of suspicious transactions | **R.21** – Tipping-off and confidentiality | **R.22** - DNFBPs: Customer due diligence | **R.23** – DNFBPs: Other measures | **R.24** – Transparency & BO of legal persons |
| LC | LC | LC | PC | PC | 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 | LC | LC | LC | C | C |
| **R.31** – Powers of law enforcement and investigative authorities | **R.32** – Cash couriers | **R.33** – Statistics | **R.34** – Guidance and feedback | **R.35** – Sanctions | **R.36** – International instruments |
| C | LC | LC | LC | LC | LC |
| **R.37** – Mutual legal assistance | **R.38** – Mutual legal assistance: freezing and confiscation | **R.39** – Extradition | **R.40** – Other forms of international cooperation | | |
| LC | LC | LC | LC | | |

# Mutual Evaluation Report

## *Preface*

This report summarises the AML/CFT measures in place in the Kingdom of Bahrain (hereinafter referred to as Bahrain) as at the date of the onsite 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 assessment team during its onsite visit to the country from 7 to 22 November 2017.

The evaluation was conducted by an assessment team consisting of:

- Abdelsattar ELNAJAR, Deputy Head of International Co-operation Department, Egyptian Money Laundering and Terrorist Financing Combating Unit, Central Bank of Egypt, financial expert;
- Marc De BACKER, Team leader, Belgian Federal Police, legal and law enforcement expert;
- Mehmet Onur YURDAKUL, Expert, Financial Crimes Investigation Board, Turkey, legal expert;
- Peter PIATETSKY, Policy Advisor, Terrorist Financing and Financial Crimes, Department of The Treasury, USA, TF expert; Jamie KRAUT, Senior Policy Advisor, Terrorist Financing and Financial Crimes, U.S. Department of the Treasury, and
- Richard WALKER, Director of Financial Crime and Regulatory Policy, Guernsey, risk and financial expert.

The team was supported by the FATF Secretariat, represented by Ashish KUMAR, Diana FIRTH and Kristen ALMA, and the MENAFATF Secretariat represented by Alwaleed ALSHEIKH. The report was reviewed by Khaled ALGHAZALI (Kuwait), Pieter SMIT (South Africa) and the IMF.

Bahrain previously underwent a MENAFATF Mutual Evaluation in 2006, conducted according to the 2004 FATF Methodology. The 2006 evaluation report and the 2012 follow-up report have been published, and are available at www.menafatf.org. That evaluation concluded that the country was compliant with seven Recommendations; largely compliant with 16; partially compliant with 22, and non-compliant with three Recommendations. One Recommendation was assessed as not applicable to Bahrain. Bahrain was rated compliant or largely compliant with six of the 16 Core and Key Recommendations. Bahrain was placed under the regular follow-up process immediately after the adoption of its 3rd round Mutual Evaluation Report, and moved to biennial updates in November 2012.

# CHAPTER 1. ML/TF RISKS AND CONTEXT

33. Bahrain is an archipelago in the Arabian Gulf. It is made up of 36 islands with a total surface area of 760 sq. km. The main island, which comprises approximately 91.3% of the total surface area, is connected to Saudi Arabia through a 25 km causeway. The population of the country is 1.37 million, and is considered to be the lowest in comparison to regional gulf countries. Bahrain is a member of the Co-operation Council for the Arab States of the Gulf (or the Gulf Co-operation Council, GCC). Bahrain's strategic location provides a natural gateway to the growing Gulf economies, and positions the country as a perfect hub for operations in the GCC, Middle East, and North Africa.

34. Bahrain's economy has shown rapid growth during 2000-2012 despite the financial meltdown in 2008-2009. Bahrain's real GDP was USD 31.8 billion in 2016 and grew by around 3.3% in real terms as compared to 2015. Oil comprises 75.6% of the country's budget revenues and 20% of its GDP.

35. Bahrain enjoys a strong, diverse, and competitive economy which promotes business growth. The financial services sector accounted for 16.5% of the real GDP in 2016, and is the largest non-oil contributor to the GDP. As part of its economic diversification plans, Bahrain has shifted focus on enhancing its manufacturing and industrial sectors. The manufacturing industry in Bahrain has seen an increase in output of 85.6% during the last 10 years, and is the third largest contributor to Bahrain's economy, and accounted for 14.9% of real GDP in 2016.

36. Bahrain is a constitutional monarchy with a democratic system of government. The government is segregated into legislative, executive, and judicial authorities. The country adopted its Constitution in February 2002. The Constitution provides for a National Assembly comprising two chambers, the Consultative Council ("Shura Council") and the Chamber of Deputies.

## ML/TF Risks and Scoping of Higher Risk Issues

### Overview of ML/TF Risks

37. Bahrain is a regional financial and trading hub with a liberal business environment. The country's strong growth since 2000 is continuing; it is rapidly diversifying its economy to decrease its dependence on oil. The financial services sector is benefitting from these policies, and is well developed and the largest non-oil contributor to GDP. Government initiatives are being undertaken to further develop and diversify both this sector and other sectors, such as real estate. Bahrain is therefore exposed to domestic ML/TF risks, and the ML/TF risks associated with cross-border customers and activity. The country is also exposed to geopolitical risks, most notably in relation to TF.

1

38. The main predicate offences for ML are investment fraud, immorality, drug trafficking, human trafficking and smuggling. Smuggling of cash is also an important threat element. The banking sector, money exchangers, and real estate sectors are considered vulnerable for laundering the proceeds of crimes.

39. Bahrain is also vulnerable to TF. The understanding of this risk is evolving, and includes illegal fund raising, abuse of NPOs, smuggling of cash, and Foreign Terrorist Fighters (FTFs).

### *Country's Risk Assessment*

40. Bahrain is currently undertaking its first formal and comprehensive National Money Laundering and Terrorist Financing Risk Assessment (NRA). The NRA process is organised and led by the National Policy Committee (NPC), and carried out by working groups representing relevant AML/CFT stakeholders in the country, including members of the private sector.

41. While the NRA was not completed at the time of the onsite, a majority of relevant authorities are contributing to the process. The NRA process will build on certain existing sectoral assessments carried out by the Central Bank of Bahrain (CBB) and the Ministry of Industry Commerce and Tourism (MOICT) and other competent authorities.

42. As per the draft NRA as at the time of onsite, the key threats are investment fraud (highest threat, with other types of fraud and related acts not being considered as relevant or low risk), cash courier/cross-border violations (including smuggling) (high), immorality and prostitution (high), drug trafficking (medium), human trafficking (medium), corruption (medium), illegal trade in work permits (medium) and illegal fund raising (low). The banking sector is considered to be the most targeted sector for ML, with money changers, custodians and real estate being medium risk targets.

43. According to the authorities, the risk of terrorism and TF is high. Though the understanding of risk is still being finalised, Bahrain identifies the most prevalent and high risk TF areas as: cash smuggling via land and sea (i.e. foreign funding); NPOs; fundraising; and, FTFs. As per the draft NRA, Bahraini authorities have noted that the primary TF risks emanate from a country with which it does not have relations. Geopolitical factors are the main contributor to the TF risk for Bahrain.

### *Scoping of Higher Risk Issues*

44. In deciding what issues to prioritise, the assessment team reviewed material provided by Bahrain on national ML/TF risks, and information from reliable third-party sources (e.g. reports by international organisations). The issues listed present areas of higher ML/TF risks (including threats and vulnerabilities), as well as issues that were of significant concern to the assessment team:

- ***Understanding of risk and implementation of risk-based measures:*** As the NRA was yet to be finalised at the time of on-site, the assessment team focused on Bahrain's understanding of its ML/TF risks, and the application of risk-based measures in accordance with existing strategies and action plans. The assessment team also focused on how well cross-border ML/TF risks are understood and managed by the financial institutions, and on how

effectively relevant law enforcement authorities and supervisors are responding to these risks.

- ***Cross-border movements of cash:*** Due to geographical location of Bahrain, illegal smuggling of cash in and out of Bahrain (both for ML/TF) is a concern. There have also been instances where Bahrain has been used as a transit route for such illicit activities. The assessment team focused on the extent to which the existing legal framework related to bulk cash smuggling and cash couriers meets the requirements, and is being effectively implemented, including resources and capacity of authorities.
- ***Fraud and criminal breach of trust:*** As per authorities, domestic fraud, criminal breach of trust and related offences are the most significant predicate offences for ML. The assessment team focused on the investigation and prosecution of ML cases arising out of such cases, as well as resources and capacity of relevant authorities.
- ***Corruption:*** Corruption related offences have caught the attention of authorities in recent years. For example, in December 2013, the Crown Prince established an Investigation Committee to oversee the cases highlighted within the National Audit Bureau's annual report. In February 2014, the Minister of State for Follow-up Affairs announced that seven cases had been transferred for public prosecution, of which one had been transferred to court. The assessment team focused on the authorities' understanding of risks related to corruption, as well as the efficacy of enforcement and preventive measures.
- ***Terrorist Financing:*** Terrorism is a significant threat to Bahrain, particularly from militant groups targeting Bahraini security forces. Terrorist financing related to the recent terrorist attacks in Bahrain have been linked by the authorities to Iran and Hezbollah. ISIL related activities have also occurred in Bahrain. According to Bahrain, the most significant TF threats relate to the abuse of charities/NGOs, the smuggling of cash and supply of equipment and training across borders. The assessment team focused on the effectiveness of measures to combat TF in all its forms including the financing of FTFs, implementation of targeted financial sanctions, and the integration of CFT in the broader counter-terrorism strategy.
- ***NPOs:*** Bahrain identified 55 non-profit organisations as being at risk of TF (out of 417) and public fundraising as a TF risk, in its draft NRA. The assessment team focused on the extent to which Bahrain has established clear policies to promote accountability, integrity, and public confidence in the administration and management of NPOs. Implementation of targeted risk-based supervision or monitoring of NPOs, and whether proportionate and effective actions are being taken in this regard, were also considered.
- ***Real estate:*** Since Bahrain has designated certain areas where non-Bahrainis are permitted to own property; there has been a significant influx of new buyers, from expatriates within Bahrain, as well as from non-residents. Authorities estimated that the size of the real estate sector is fairly large in comparison to the overall DNFBP sector, and the overall risk profile of the sector might be high due its potential risky customers. The assessment team

1

focused on how well the sector understands its risks and obligations, and takes effective and commensurate measures to manage and mitigate such risks.

- ***Dealers of Precious Metals and Stones (DPMS):*** The jewellery and gold market is considered to be one of the most prominent markets of Bahrain. There is a sizeable jewellery and gold retail industry in Bahrain. The coverage and implementation of preventive measures by, and supervisory processes for the DPMS sector was identified as a focus area for the assessment team.

45. Through the scoping exercise, the assessment team identified the following areas for lesser focus:

- ***ML related to domestic tax fraud:*** Bahrain has no tax on corporate income, personal income, wealth, capital gains, withholding or death/inheritance.
- ***Casino sector:*** Casinos are not permitted in Bahrain. The assessment team also focused on the extent of illegal gambling, if any, occurring in the country.

### *Materiality*

46. The geopolitical situation of Bahrain provides a natural gateway to the growing gulf economies and positions the country as a hub for operations in GCC, Middle East and North Africa. In addition, as a regional logistical trading hub, the country is exposed to the inflow and outflow of goods. Bahrain shares maritime borders with Iran, Qatar, and Saudi Arabia, and is in proximity to Dubai, a major international financial hub, and areas of regional conflict and unrest, which may expose Bahrain to ML/TF risks.

47. Bahrain is considered to be a regional middle-eastern financial centre. It has a well-developed financial sector, which includes 29 retail banks (including seven Islamic retail banks) and 76 wholesale banks (including 19 Islamic wholesale banks). 14 retail banks are locally incorporated while 15 are branches of foreign banks. Bahrain, with 26 Islamic banks (both retail and wholesale), has the largest concentration of Islamic bank operations among the countries that operate dual banking systems.

48. Bahraini authorities believe (a view shared by the assessment team) that the greatest risk of ML is related to foreign proceeds that might transit through Bahrain. This exposes Bahraini financial sector to ML risks originating outside Bahrain, and makes Bahrain's supervision of its financial institutions' compliance with AML/CFT obligations important to the region as a whole.

49. Casinos are banned in Bahrain; however, there are other constituents of the DNFBP sector in Bahrain with varying level of importance. For example, dealers in precious metals and stones (DPMS) sector is well developed with a number of players, real estate agents and notaries play a significant role in real estate transactions (notaries' role in real estate transactions is to confirm that the person signing the sale contract has the capacity to do so and confirming their identity), and lawyers are often involved in complex transactions as well as in formation of companies. The role of accountants and auditors is relatively less significant, as the

existing legal framework in Bahrain limits the scope of their work to maintaining accounts, audit and related consultancy work.

### *Structural Elements*

50. The key structural elements for an effective AML/CFT system are present in Bahrain, such as political and institutional stability, accountability, transparency, rule of law, a professional bar association as well as a capable, efficient and independent judiciary. Bahrain has strong political commitment to ensure it has a robust AML/CFT framework.

### *Background and Other Contextual Factors*

51. Financial exclusion is not a serious issue in Bahrain. As of 2014, almost 82% of the Bahraini population over the age of 15 reported to have accounts at financial institutions (up from 64.5% in 2011): *Global Findex 2014 (World Bank).* As per the *Migration and Remittances Factbook 2016 (World Bank),* internet users per 100 people in Bahrain in 2014 were 91. Bahrain is the sixth largest immigration country, relative to its population (54%). With outward remittance flows of USD billion 2.36 in 2014, Bahrain also figures in top ten remittance sending countries in terms of percentage to GDP (7%).

#### *AML/CFT strategy*

52. The NRA was not finalised at the time of on-site, though authorities indicated that the outcomes derived from the NRA would be used to develop a risk-based National AML/CFT Action Plan. Notwithstanding this, the National Policy Committee, the Legislation/Policy Committee, and the National Committee on the Implementation of UNSCRs set and coordinate AML/CFT policy, including TFS implementation. The National Policy Committee develops 3-5 year strategies, which are updated as needed. The current AML/CFT strategy was developed in 2012. However, the strategy, action plans and evidence are currently being updated to incorporate the results of the draft NRA.

#### *Legal & institutional framework*

53. The following primary authorities are an integral part of the AML/CFT framework of Bahrain:

- **National Policy Committee (NPC)** is a committee formulated in accordance with Art. (4) of Decree Law No. (4) of 2001. The NPC includes the CBB (Chair); Ministry of Interior (MOI); Ministry of Foreign affairs; Public Prosecutions Office (PPO); MOICT; Survey and Land Registration Bureau (SLRB); Ministry of Finance; Ministry of Justice and Islamic Affairs (MOJ), Ministry of Labour and Social Development (MLSD); National Security Authority (NSA); Ministry of Youth and Sports Affairs, Legislation and Legal Opinion Commission and Custom affairs. Primarily, the responsibilities of the NPC include formulating AML policies and strategies and determining a mechanism to coordinate among relevant domestic authorities.

1

- **Central Bank of Bahrain (CBB)** follows a dual mandate as a central bank and the sole regulator of Bahrain's financial sector, covering the full range of banking, insurance, investment business and capital markets activities. CBB also licenses trustees, and information on all trusts is maintained in the trusts register maintained by the CBB.
- **Ministry of Interior (MOI)** is responsible for maintenance of security, general order and safety, and law enforcement in Bahrain. It comprises a number of directorates, which play a key role in the AML/CFT framework of Bahrain. These include, Financial Intelligence Directorate, General Directorate of Anti- Corruption and Economic and Electronic Security, General Directorate of Criminal Investigation, Public Security Directorates and the Nationality, Passport and Residence Affairs, among others.

**Financial Intelligence Directorate (FID)**, housed within the MOI is Bahrain's law enforcement FIU. It is the central authority to receive, analyse and disseminate STRs. It also receives intelligence and other reports from security agencies as well as cross-border currency reports from Customs. FID also carries out initial investigations in potential ML/TF cases before referring them to the PPO for judicial investigations.

- **Anti-Corruption Directorate** is part of the General Directorate of Anti-Corruption and Economic and Electronic Security, within the MOI. Its role is to investigate corruption cases. The department coordinates with FID and other competent authorities in performance of its duties.

  **Anti-Economic Crime Directorate** is the part of the General Directorate of Anti-Corruption and Economic and Electronic Security, which combats fraud, embezzlement and other related crimes. The department coordinates with FID and other competent authorities in performance of its duties.
- **Cyber Crime Directorate** is part of the General Directorate of Anti-Corruption and Economic and Electronic Security, which combats crimes committed using cyber media. The department coordinates with FID and other competent authorities in performance of its duties.
- **Customs** is responsible for the detection of illicit transportation of cash and bearer negotiable instruments (BNIs) across borders and reporting them to the FID. Customs also has a role in identifying potential trade based ML and under/over invoicing, based on the automated system for customs clearance being used in 12 ports in Bahrain. Bahrain Customs does not conduct ML/TF investigations on its own, but cooperates and coordinates with the FID and the PPO in such cases.
- **Bahrain Coast Guard Police** is one of the primary authorities responsible for the country's border security. The coast guard deploys various border control mechanisms to counter any smuggling attempts through sea borders.
- **Joint Counter Terrorism Centre (JCTC)** is responsible for gathering and analysing information regarding terrorist organisations and affiliated individuals in addition to liaising with local and international agencies on that regard.

- **Ministry of Industry Commerce and Tourism (MOICT)** is the main supervisor of the DNFBP sector. Primarily the sectors under the ministry's

supervision include: jewellers and precious metals dealers, auditors and accountants. The real estate sector was previously supervised by the MOICT; however, the sector's supervisory authority was transferred to the Real Estate Regulatory Authority (RERA), attached to the Survey and Land Registration Bureau (SLRB) in August 2017. MOICT is also responsible for the administering the commercial register: Sijilat system (www.sijilat.bh), which allows the search for any registered legal person using the Commercial Registration Number (CRN).

- **Ministry of Foreign Affairs (MoFA)** is responsible for transmitting UNSCR lists to domestic authorities in Bahrain. The Ministry also coordinates all engagement with the United Nations on sanctions related resolutions (TF/PF).
- **Ministry of Justice and Islamic Affairs (MOJ)** is the supervisory authority for lawyers and real estate agents (individuals) until the summer of 2017 when the licensing of real estate agents was moved to newly created entity. The Ministry is responsible for regulating and supervising lawyers and notaries with regards to AML/CFT and all laws in Bahrain. This Ministry also supervises the formation and activities of waqfs.
- **Public Prosecutions Office (PPO)** is an independent judicial authority entrusted with the power to initiate and handle criminal proceedings as well as case referrals and appeals before the Court of Cassation. It comprises a High Prosecution office, District and Specialised Prosecution offices, Technical Office of the Attorney General and the Judicial Inspection Administration. The PPO carries out judicial investigations in ML/TF cases. As part of the investigations, the PPO is authorised to order confiscation of property and/or assets linked to the ML/TF crime. The PPO coordinates with the relevant authorities; specifically the FID to further develop the ML/TF cases referred to it. This occurs through use of various investigative techniques by the FID and by obtaining information from financial institutions, commercial establishments, registries and notaries, or other entities, as needed.
- **National Security Agency (NSA)** is responsible for gathering intelligence on terrorism/TF. The agency coordinates with other Bahraini competent authorities (e.g. FID, CBB) on issues of national security and has both intelligence gathering and law enforcement powers.
- **Ministry of Labour and Social Development (MLSD)** is the policy making and supervisory authority of NPOs, including charities.
- **Survey and Land Registration Bureau (SLRB)** is responsible for the registration of real estate properties in Bahrain. Since 2017, the bureau is the supervisory authority of real estate agents.
- **National Committee on the Implementation of UNSCRs** is responsible for the implementation of UNSCRs.

### *Financial sector and DNFBPs*

54. Bahrain's financial sector is well-developed and diversified, consisting of a wide range of conventional and Islamic financial institutions and markets, including

retail and wholesale banks, specialised banks, insurance companies, finance companies, investment advisors, money changers, insurance brokers, securities brokers and mutual funds. Banks play a predominant role in the financial sector, representing 6.2 times of its GDP as at the end of the third quarter of 2016.

55. Following is a breakup of the financial sector and DNFBPs in Bahrain:

Table 1**. Size of the financial sector and DNFBPs**

| Sector | Constituents/Services | Number (Nov. 2016) | Size (Nov. 2016) in BHD billion* |
|---|---|---|---|
| **Banks** | Retail banks | 29 (incl. 7 Islamic retail banks) | 31.50 |
| | Wholesale banks | 76 (including 19 Islamic wholesale banks) | 39.95 |
| **Insurance firms** | Share of life insurance in gross premium is 19% compared to 81% for non-life | 11 | 0.52 (19% of gross premium) |
| **Insurance brokers** | | 31 | - |
| **Investment Business Firms** | Category 1 and 2 (asset management) | 34 | 2.90# |
| | Category 3 (advisory) | 18 | |
| **Custody, Administration and Registrar** | Five part of international groups, two part of regional group and two local companies | 9 | 3.50 |
| **Stock brokers/dealers** | Ten part of banking group and three small dealers | 13 | Daily average no. of trades: 43 in 2016 |
| **Money changers and remittance services** | 11 small scale with limited operations and eight large scale | 19 | 18.60 (currency exchange and remittance) |
| **Finance companies (including micro finance)** | Mainly offering credit facilities | 11 | Not allowed to accept deposit |
| **Ancillary service providers** | Providing card processing and/or payment services support to other FIs such as banks | 14 | Not available |
| **Trust service providers** | Part of international group | 3 | - |
| **Lawyers** | | 989 | - |
| **Notaries** | 16 | 16 | - |
| **Accountants and auditors** | Providing auditing, assurance, tax consultancy & accounting services | 25 Auditing firms 90 individuals working in this firms | 2.9 Million |
| **Dealers in precious metals and stones (DPMS)** | Sale and trade in gold, silver, and all kind of bullion and precious metals and stones | 378 | 110 Million |
| **Real estate agents** | Buying, selling and management of real estate and properties | 4518 | 1.03 Billion |

*Note*: Draft ML/TF NRA and CBB website.
*Source*: BHD 1 is equivalent to EUR 2.24 as on 29 November 2017. # Net Asset Value USD 7.67 billion as on June 2017.

### *Preventive measures*

56. Financial institutions and trust service providers are subject to Decree Law No. (4) of 2001 with respect to the Prevention and Prohibition of the Laundering of Money, and it subsequent amendments of 2006 and 2013 (AML Law). They are also subject to the Central Bank and Financial Institutions Law (CBB Law) and the Financial Crime Module (FC Module), which is part of various Rulebooks issued by the CBB for different sectors.

57. The FC Module is a comprehensive framework of rules and guidance issued by the CBB with the primary aim to combat ML/TF. The FC Module contains detailed requirements relating to customer due diligence, record-keeping, training, transaction monitoring and reporting, and the role and duties of the Money Laundering Reporting Officer (MLRO).

58. The following table illustrates the various FC modules and the respective financial institutions subject to them:

Table 2. **FC Modules and their Applicability**

| FC Module | Applicable to |
|---|---|
| **1** | Retail and whole sale conventional banks |
| **2** | Islamic banks |
| **3** | Insurance sector |
| **4** | Investment firm licensees |
| **5** | Specialised licensees (money changers; financing companies; representative offices; administrators; trust service providers, micro finance institutions and ancillary services providers) |
| **6** | Capital market service providers |

59. The DNFBP sector in Bahrain is subject to the AML law and preventive measures set out in various Ministerial Orders issued by the MOICT (for DPMS, accountants, and auditors), and the MOJ (for lawyers and notaries and individual real estate agents until September 2017). Real estate agents which were structured as companies were supervised by the MOICT until September 2017, at which point the real estate sector was transferred to a separate authority, Real Estate Regulatory Authority (RERA) under SLRB. The legislation framework for lawyers and notaries was strengthened while the assessment team was in Bahrain. Trust service providers are registered by the CBB and covered under FC Module 5.

### *Legal persons and arrangements*

60. Bahrain has an electronic system (www.sijilat.bh/) to register legal persons. The system is administered by the MOICT, which is the designated Ministry responsible for the creation, registration, and supervision of legal persons. The Sijilat system is publically accessible, and contains basic and beneficial ownership information (further details are provided in the analysis under IO.5 and Technical Compliance Annex).

1

61. All legal persons or other establishments operating in Bahrain (irrespective of their origin) are required to be registered in the Sijilat system, which is a live system facilitating real time analysis, updating of information and detection of any aberration in financials or other parameters.

62. The breakdown of legal persons and establishments registered in Bahrain is as follows:

Table 3. **Breakdown of legal persons and establishments (2017)**

| Type of legal person | Total |
|---|---|
| **Bahrain Shareholding Company (Closed)** | 690 |
| **Bahrain Shareholding Company (Public)** | 43 |
| **Branch of a Foreign company (foreign companies)** | 769 |
| **Partnerships** | 1 275 |
| **Simple Commandite (Limited Partnership Company)** | 66 |
| **Single Person Company** | 4 213 |
| **Specialised Partnerships** | 15 |
| **Limited Liability Company** | 11 179 |
| **Individual Establishments** | 25 730 |

63. There are 43 trusts registered with the CBB. Three trust and company service providers are registered with the CBB as specialised licensees. Bahrain also has waqfs, which are similar to trusts and allow individuals to endow property in favour of a charity or a member(s) of its family. There are 1681 waqfs registered in Bahrain (as of April 2018), out of which 78 were waqfs created during 2012-2017, which gives an indication that numbers are quite stable.

### *Non-Profit Organisations (NPOs)*

64. Bahrain has a number of organisations that meet the FATF definition of Non-Profit Organisations (NPOs). Bahrain has three types of NPOs: Associations, Private Institutions and Special Committees[1] to which the same provisions apply, albeit with

[1] An **Association** is defined as any group with a permanent structure formed of a number of natural or legal persons to achieve a special purpose; not aiming at financial gains; aims at conducting special social, educational, cultural or charitable activity. This definition applies to associations, cultural or social clubs no matter their names and no matter whether they practice physical sports as long as this sport is not the major purpose of the association or the club. **Private institutions** refer to a specific amount provided for a specific period, for a specific purpose, charitable, artistic or other, with no financial gain purpose inside or outside of Bahrain. A **specialised committee** refers to any group with permanent structure formed of a number of natural or legal persons to provide care to youth by providing national sports services and related social, spiritual, health and entertainment services and not aiming at financial gains for its members (i.e. Olympic Committee).

some small variations. All are regulated under the Law of Associations, Social and Cultural Clubs, Special Committees Working in the Field of Youth and Sports and Private Institutions, Decree Law No. (21) 1989, and its amendments. Bahrain also has charitable purpose waqfs as noted in paragraph 63 above and also meets the definition of NPO as regards disbursement of funds, which are supervised by the MOJ. Bahrain is in the process of following a more nuanced approach to dealing with NPOs, as at the time on the onsite, measures such as fundraising controls applied to nearly all types of NPOs. There are only three types of organisations that are not subject to these controls and do not fall under the definition of NPO: youth clubs, which are not significant in number (37 in total) and were not found as high risk by Bahrain (nor in the draft NRA or in their assessment of NPOs); and the Royal Charity, which is a state managed charity that undergoes specific strict separate controls, such as auditing by the national audit court as well as external auditors, and is supervised by the Royal Court. The Royal Charity also works with large international NPOs and cooperates with the MOI and MOFA to ensure that it does not engage in unfavourable business. Lastly, charitable purpose waqfs do not engage in fundraising activities but rather serve as a vehicle for disbursing funds from a single donor the waqif, hence no license is required.

65. Measures to regulate fundraising seem to have been implemented following a need to protect the public from fraud, as well as to prevent potential ML/TF abuse. Since 2013, Bahrain requires most NPOs to apply for a license and security clearance before they can collect funds from the public and prior to conducting overseas transfers, regardless of the amount. These requirements are enforced and there have been three ML convictions involving illegal fundraising.

66. Prior to the introduction of the aforementioned measures, banks were required to obtain an official letter from the MLSD authorising the receipt or remittance of funds before accepting or processing such funds on behalf of charity and NPO. During the period from January 2011 to June 2012, the Ministry also referred seven cases to the PPO against a number of charities and NPOs for violating the laws and procedures, two of which resulted in sentences.

### *Supervisory arrangements*

67. The CBB is the sole regulator (both for prudential and AML/CFT) of the financial sector, and trusts service providers. The CBB derives its authority from the AML Law, CBB Law and its Rulebooks. As per Art. 4 of the CBB Law, the CBB is granted the power and duty to regulate, develop and license the services stated in Art. 39, and exercise regulatory control over institutions that provide such services.

68. Casinos are illegal in Bahrain. The supervisory framework for DPMS, corporate real estate agents (until September 2017), auditors and accountants is set out by the MOICT. The real estate sector's supervisory authority was transferred to RERA in September 2017. RERA is currently drafting regulations to establish AML/CFT obligations for real estate agents.

69. MOJ registers and supervises lawyers, notaries and individual real estate agents (until September 2017), which are subject to AML/CFT obligations.

1

### *International co-operation*

70. International co-operation is an important element for Bahrain, given its role as a financial and business centre. Bahrain is a party to a number of international conventions, which are relevant in the context of combatting crime, including ML and TF. Bahrain receives and responds to MLA requests for both ML and predicate offences primarily through diplomatic channels and it utilises informal co-operation mechanisms. Formal bilateral agreements are signed at the request of counterparts, although no agreements or MOUs are required under Bahraini law to provide MLA or exchange information. Bahrain requires dual criminality for extradition, but requests are guided by the principle of reciprocity and there is no requirement for crime types to be identical to those in Bahrain; authorities would seek to use whichever offence is most appropriate from the set of offences available domestically.

71. Authorities have used MLA and Interpol channels in several ML cases. With regard to extradition, authorities use Interpol arrest warrants for facilitation. The FID is very active in exchanging information related to ML/TF via the Egmont Secure Web, including beneficial ownership information. The CBB has the authority to, and does exchange supervisory information with its international counterparts, including on AML/CFT related issues.

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

## Key Findings and Recommended Actions

### *Key Findings*

**Bahrain achieved a moderate level of effectiveness for IO.1.**

1. Bahrain has taken strong steps to complete an AML/CFT NRA; the process has engaged most of the relevant authorities and was ongoing at the time of the onsite.
2. Some authorities such as the FID, PPO, CBB and, although not to the same extent, the MOICT have a general understanding of ML/TF risks. The assessment of risks both in general, and in a range of particular areas, needs to be deepened so as to allow substantiated conclusions on risks, and their relative importance from a national perspective. Understanding of TF risks is relatively less developed than for ML.
3. There is a longstanding co-ordination framework, which covers AML/CFT and combatting of PF. The framework should be developed to cover risk-based approaches on AML/CFT matters.
4. Domestic and multilateral co-operation and information exchange at the operational level is strong.
5. There have been some significant policies and actions by the authorities to address risk (e.g. the CBB's strong controls to prevent criminal ownership or operation of FIs). However, more generally, the objectives and activities of authorities need to be strengthened and aligned with identified ML/TF risks.
6. Areas of simplified due diligence are relatively minor and appear to be consistent with Bahrain's risks although published risk material has not led to specific requirements on EDD.
7. The private sector is not yet aware of the draft NRA; the authorities plan to publish the NRA report on completion.

### *Recommended Actions*

1. The NRA should be finalised, with extended articulation of the assessment of ML/TF risks either in the NRA report or elsewhere, including:
    - all of the AML/CFT authorities;
    - utilising information from outside Bahrain;
    - utilising more statistics and ensuring that the statistics used are robust;
    - further analysing external risks and the risks of organised crime;
    - reviewing the DNFBP sectors in more detail;

- conducting a specific and comprehensive assessment of the risks posed by legal persons;
- assessment of TF risk separately to any wider assessment of facilitation of terrorism; including through coverage of ISIL, FTFs and Al Qaida in the risk assessment; and
- more detailed analysis of charities and other NPOs.

2. With regard to co-ordination, the framework should:
   - review issues in more depth from the perspective of risks as identified in the NRA and the risk-based approach in operational matters; and
   - coordinate the objectives and activities of all AML/CFT authorities so that they are aligned and addressing ML/TF risk effectively.
3. Business activities should be reviewed to ascertain whether any further risks relevant to Bahrain should be subject to EDD and any necessary changes made to the EDD framework;
4. The authorities should routinely communicate comprehensive information relevant to risk to private sector entities; this should include the NRA when it has been completed.

72. 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*

73. Bahrain is undertaking a ML/TF NRA, with most of the relevant authorities contributing to the process. It is moving forward methodically and the NRA process will continue to build on existing sectoral assessments carried out by the CBB and the MOICT. Understanding of ML/TF risks is still evolving and will be further developed as the NRA process is taken to its logical conclusion. This first NRA, when completed, will be a major step in enhancing Bahrain's understanding of risk. At the time of the onsite a draft NRA report had been prepared.

74. After the team left Bahrain, it was provided with a revised draft. The assessment team makes a distinction on the one hand between the assessment and understanding of risk demonstrated by the authorities at the time of the visit (whether or not the understanding and risk was articulated in writing) and, on the other, the developed written articulation of risk reflected in the revised NRA, which can be used to help ascertain whether or not measures undertaken by Bahrain are consistent with its risk profile. At the time of the visit the risks in the draft NRA report had been provided by individual authorities and had not been considered or agreed by the National Policy Committee or otherwise agreed at the national level. In completing the NRA, all authorities relevant to AML/CFT should be involved and further sources of information inside and outside Bahrain should be utilised. A more in depth analysis of the information available will help form conclusions on residual risks.

75. In some areas, individual authorities have a general understanding of ML/TF risks. The FID, PPO, CBB and (although not to the same extent), the MOICT have a relatively better understanding of ML risks. This general understanding comes from

information gathered in the course of the authorities' operational activities, together with risk assessment work with reporting entities undertaken by the CBB and MOICT.

76. The key threats of laundering of funds at the time of the visit were seen as arising from fraud and related acts, including breach of trust (medium threat) and, to some extent, illegal fund raising (medium threat), with immorality and prostitution and drug trafficking being seen as low to medium threat; other criminality, where it was considered relevant, was considered to be low threat. At that time, threat levels had been predicated on the number of convictions and, in addition, Bahrain's statistical framework did not allow for corruption offences to be unbundled from what had been categorised as fraud and related acts. The threat profile of ML has been revised in the next version of the draft NRA report. In this revised document (particularly pertinent to the other IOs in this report and in demonstrating the preliminary nature of the draft at the time of the visit), the revised threats are investment fraud (highest threat, with other types of fraud and related acts not being considered as relevant or low risk), cash courier/cross-border violations (including smuggling) (high), immorality and prostitution (high), drug trafficking (medium), human trafficking (medium), corruption (medium), illegal trade in work permits (medium) and illegal fund raising (low).

77. ML from investment fraud (and possibly other frauds) and cash courier/cross-border are identified as high threats for Bahrain. The threat arising from corruption, particularly foreign corruption, is uncertain, particularly considering Bahrain's status as a regional financial centre. In light of the high number of drug trafficking cases and some uncertainties of information and, therefore, assessment, greater attention is needed. It is also not clear that the threat of ML from immorality and prostitution should be considered as one of the highest threats or why the overall higher threat picture is inconsistent with what might be expected from a finance centre with significant cross-border business.

78. The banking sector is considered to be the most targeted sector for ML, with money changers, custodians, and real estate being medium risk targets.

79. The assessment team agrees with the overall conclusion of risk in relation to the banking sector. However, the sector's ratings are based in part on being targeted for all fraud, breach of trust and related acts and illegal fund raising. Generally, it is not wholly clear how the ratings (the CBB's conclusions) tie in with what are considered to be the highest threats or the seeming prevalence of the use of cash for some criminality, such as immorality and prostitution (the conclusions of other authorities). The CBB was articulate in discussion on the ML client and product risks presented by each part of the banking sector. It was also articulate on the higher product risks (private banking, correspondent banking relationships, current accounts and introduced business). This analysis would seem to require more focus as medium/high or high risk client and product risks of the sector cover large parts of it. For example, they cover all current accounts and all NPOs rather than those which are higher risk (See IO.3).

80. The CBB representatives who discussed the risks of money changers and insurers with the assessment team were also convincing about the assessment and understanding of sectoral risk, to the extent that the team was left with the impression that the insurance sector seemed to have less risk than suggested in the

NRA (See IO.3). It is not entirely clear why custodians have been rated as having the same risk as other sectors in the medium risk category. Any changes to assessment and understanding of ratings of FIs would appear to be one of degree rather than fundamental.

81. The MOICT has undertaken onsite inspections of all DNFBPs for which it has oversight responsibilities, and which inform its understanding of risk. It has put in place a framework for a risk-based approach to supervision. With reference to DNFBPs, only the MOICT had been involved in the NRA assessment and less information had been obtained from DNFBPs as opposed to FIs. The assessment team does not consider that there has been a sufficient assessment of risk to support the rating of lawyers as low risk.

82. The FID is the key agency involved in the NRA, and is responsible for gathering relevant information from other agencies (such as the PPO) for identification of the main ML risks. As a central hub of all financial intelligence, and in its role as law enforcement FIU carrying out initial ML/TF investigations, generally, the FID has a good operational understanding of the key ML/TF risks being faced by Bahrain. The PPO, as a judicial investigating authority, has also developed a generally good understanding based on its investigative and prosecutorial experience. This understanding will be further developed as the NRA process is completed, and further sources of information are considered going forward.

83. The draft NRA does not assess how legal persons established under Bahraini law have been used to launder the proceeds of crime and there is no specific assessment of the threats, vulnerabilities and risks presented by these structures (except to the extent that FIs and, in part, DNFBPs which are legal persons are themselves covered by the NRA). There is reference to legal persons in the MOICT's DNFBP risk assessment report but this is restrained to a tabular description of the number of STRs received by legal type and the part of Bahrain from which they have been made. This information informs the MOICT's risk score template which it uses to categorise the risk of each individual legal person. Further assessment is needed so as to have a comprehensive understanding of the risks presented by legal persons. The draft NRA covers legal arrangements and trustees. This, combined with discussions by the team indicated general understanding by the CBB of the risks of legal arrangements. There are a low number of trusts; a Bahraini trustee is required and the trusts are registered with the CBB, which is provided with a copy of the trust instrument, as a consequence, information on settlors.

84. There was some written assessment of cash courier and cross-border smuggling violations (See above), (although the Bahrain authorities advise that the disclosure reports made at the borders are analysed routinely; examples of this analysis have not been provided to the assessment team) and a breakdown of STRs received by the MOICT by nationality of the subject. The CBB indicated that it had carried out some analysis of wire transfers based on the responses to the NRA questionnaire for banks. However, the cross-border element of ML risks to Bahrain has not been separately considered within the overall risk analysis. While there might have been some understanding by the FID of other elements (in particular cross-border links and prostitution). Bearing in mind Bahrain's position as a regional hub, the impact of external threats warrants more in-depth consideration

by Bahrain; the authorities were already mindful of the need to consider cross-border transactions, including the volume of transactions, in more detail.

85. The authorities had a concern about the risks emanating from the use of cash within Bahrain. As indicated in chapter one, the use of cash is diminishing and the shadow economy is small, but the assessment team shares the views expressed by Bahrain that the risk of cash is sufficient to warrant attention.

86. There had been no specific assessment of the ML risks emanating from organised crime. Meetings during the onsite indicated that organised crime was active in relation to the large number of cases of cash smuggling into Bahrain. It was also indicated by one of the LEAs that organised crime was active in Bahrain more generally. There was no nationally agreed view on the risks and the absence of a specific assessment, combined with the number of smuggling cases and the suggestion that organised criminality is active at least to some extent in Bahrain indicates that this warrants attention from the authorities.

87. Statistical limitations also militate against understanding of risk; it is planned to address these limitations after the completion of the NRA.

88. In general, a more rounded approach should be taken to ML analysis, using sources of information from outside Bahrain, combined with further consideration of the AML/CFT process as a whole in place of reliance on convictions. There should also be more granularity of analysis in the various areas of the report, including the threats from, and vulnerabilities to, cross-border flows; legal persons and legal arrangements; and, organised crime. This would enable Bahrain to reach robust conclusions. The authorities were already mindful of the need to undertake elements of this work.

89. TF risk has not had the same depth of analysis as ML and the national level of understanding of TF is not as developed as for ML.

90. The assessment team concurs with Bahrain's assessment that its geography and the existence of terrorist groups in the region means that the TF threat is high. Terrorism is a significant threat, particularly from militants targeting Bahraini security forces (See IO.9), with Bahrain having been subject to terrorist attacks. There have been terrorism convictions in over 33 cases, as well as 22 TF convictions at the time of the onsite.

91. There is some assessment of TF risks in the draft NRA from both foreign and domestic perspectives. The assessment derives from co-ordination between the FID, LEAs and the PPO, and is based in large part on intelligence held by the FID. During its visit, the assessment team noted that, although there have been 33 terrorism cases and 22 cases with convictions for TF, information from other authorities had not yet been comprehensively integrated in the analysis of TF risk. The absence of diplomatic links and, as a consequence, contact for information gathering purposes with one country suspected of being involved with TF also militates against full understanding of risk.

92. TF is linked by Bahrain to local terrorist groups associated with the ideologies of Hezbollah, Asa ib Ahl al-Haq and the Iranian Revolutionary Guards Corps. Domestic terrorist attacks have often involved homemade explosive devices,

which are low cost and do not require significant funding. It is unclear to what extent funds might flow from or through Bahrain for use elsewhere.

93. High foreign risk in the draft NRA was considered to arise from the smuggling of cash across borders by religious tourist expeditions, seaborne smuggling and training camps. In contrast, high risk from a domestic context is assessed as arising from drop box deliveries and religious donations. Transfer and laundering of funds through the financial system, NPOs and fundraising are assessed as having medium risk.

94. The majority of TF risks identified by Bahrain relate to the physical transfer of cash. It appears that seaborne smuggling and training camps achieve such a high rating for TF because the draft NRA focusses to a large extent on facilitation of terrorism from a wider perspective than terrorist financing (with, for example, the seaborne smuggling analysis concentrating on the smuggling of weapons). This suggests that there should be more and distinct focus on TF for the purposes of CFT assessment and understanding. It is also not clear how the financial system achieved a medium risk rating beyond a consideration of the inherent vulnerabilities that exist due to the size of the financial sector (although in practice the rating had not settled at the time of the assessment team's visit to Bahrain).

95. A limited assessment of NPO risks has been carried out. Ties have been detected between a few NPO leaders and terrorist organisations although the threat aspect of the assessment has not been developed. The MLSD had not been fully involved in the NRA related assessment of charities or other NPOs, or of fundraising or donations, at the time of the assessment team's visit. It categorised NPOs for risk purposes by the level of funding and the level of funding/disbursements entering/leaving Bahrain. NPOs have been classified into three risk levels based mainly on these two indicators; they do not easily tie in with the additional categorisations specified in IO.10. However, the controls on NPOs mean that the FID has good levels of information on NPO (and charity) fund raising and disbursements outside Bahrain.

96. Charities, fund raising and religious donations were each assessed separately to NPOs. There has been very little assessment of charities in practice. In addition, religious donations (rated as high risk) and tax type contributions (rated as low risk) were assessed separately; in this regard the FID considered that, generally, higher risk individuals are associated with religious donations, thus supporting its elevated risk. The quantum of this risk is not specified. FTFs are not included in the NRA but it was apparent that the FID had some understanding of their risks as its intelligence activity had focussed on FTFs and disruption actions have been taken against FTFs (See IO.9).

97. Overall, a more in depth analysis of TF is needed, and this should also cover, for example, the threats posed by ISIL, FTFs, and Al Qaida.

### *National policies to address identified ML/TF risks*

98. The NPC (with its subcommittee, the Legislation/Policy Committee) sets and coordinates AML/CFT policy and counterterrorism efforts. There is also a separate committee, the National Committee on the Implementation of UNSCR Resolutions, which follows up on the implementation of UNSCRs. The NPC develops 3-5 year

strategies, which can be updated as needed. The assessment team was advised that the current AML/CFT strategy was developed in 2012. It was also advised that the strategy focusses actions on specified deficiencies (including deficiencies in the last mutual evaluation report) and that there are action plans which have been made under the strategy. However, the strategy has not been updated since 2012 (notwithstanding that in 2015 the individual strategic plans of the authorities were gathered together under the auspices of the NPC; and the strategy, action plans, and evidence of monitoring the implementation of the strategy and action plans have not been provided to the assessment team. The NPC intends to adopt a revised strategy and action plans, taking full account of the risks identified for Bahrain in the NRA. However, while the existing strategy and action plans are primarily aimed at addressing AML/CFT related deficiencies identified in the 3rd round mutual evaluation and there have been some initiatives coordinated or discussed within the auspices of the NPC (See below), this framework cannot be said to constitute a national policy to address the key risks.

99. In addition to the national policy activity on AML/CFT, there are also other positive national frameworks which address key areas of predicate criminality or other themes. In particular, a national anti-corruption strategy and an anti-corruption committee were introduced in 2015. In addition, while there is no written national policy, there is a consensus among the supervisory authorities as to the importance of improving corporate governance. The CBB has issued guidance for FIs. In 2010, the MOICT issued a corporate governance code and more recently, it has appointed a senior official to be responsible for improving governance among registered entities. There is now a particular focus by the MOICT on family owned businesses, and the intensity of the review of checks on the corporate governance of individual businesses (some of which are DNFBPs) has increased. The responses by the private sector to these initiatives, improve the quality of AML/CFT measures.

### *Exemptions, enhanced and simplified measures*

100. There are no specified exemptions for reporting entities in their application of AML/CFT measures.

101. FIs must undertake EDD for customers identified as having a higher risk profile and in relation to non-face-to-face business; the provision of significant electronic and internet banking services; PEPs; charities, clubs and other societies; pooled funds; and correspondent banking relationships (See R.1 and criterion 10.17). Elements of this list fall within the factors emerging as higher risk in the NRA process. There is no specific provision requiring entities automatically to take account of the NRA or other risk material produced by the authorities into account. Simplified measures are permitted only in defined circumstances (See criterion 10.18). The circumstances have not been subject to formal risk assessment supporting the application of due diligence but they do not appear to be inconsistent with the findings to date of the NRA process or the assessment team's findings.

102. DNFBPs supervised by the MOICT must carry out EDD when procedures identify a higher risk, when the client is not physically present, when entering a relationship with a PEP or in any other situation where a higher ML/TF risk might exist. There is no specific provision requiring entities automatically to take account of the NRA or other risk material produced by the authorities into account although

the MOICT has advised that it will issue an instrument under Art. 1 of Order (173) of 2017 to require entities it supervises to reflect the NRA in their procedures and apply the findings of the NRA in practice. The Order allows simplified due diligence to be undertaken in relation to clients who are well-known from their previous business history. The assessment team does not consider that simplified due diligence would necessarily be appropriate in all such circumstances. Where other types of DNFBP are subject to AML/CFT obligations, these obligations do not include a risk based approach (also see R.1 and criterion 22.1.)

### *Objectives and activities of competent authorities*

103. Some significant activity has been undertaken by the authorities to address risk (for example, the CBB's strong controls to prevent criminal ownership or operation of FIs, the additional requirements for reporting entities to identify source of funds on cash transactions above the threshold of BHD 6 000 (EUR 13 000), activity by the MOICT to reduce reliance on use of cash, and risk rating of STRs by the FID). However, the absence of agreed and fully articulated ML and TF risks at national level and the issues mentioned above means that the authorities have not been well placed to direct their objectives and policies towards the highest national risks. In a number of areas, the risk picture is still being formed (See above and IO.10) even if individual authorities have views on risk.

104. In regard to prevention (See IO.3), the CBB has strong controls to prevent criminals from beneficially owning a significant or controlling interest or holding a management function in a FI. The MOJ has reasonable controls in relation to the fitness and properness at initial licensing and thereafter. The MOICT has controls at initial registration and the Sijilat system automatically checks persons included within the system against UNSCR designations on an ongoing basis but its overall controls are relatively less robust.

105. Regarding supervision, the CBB has strong elements of a risk-based approach. For example, it has risk rated some FIs, and focuses more onsite supervisory resources at banks and money changers in line with identified risk, and devotes more attention to higher risk areas identified by the FI and the CBB. It considers significant offsite information. However, the overall approach is not a comprehensive AML/CFT risk-based approach and the assessment team has a concern about the level of supervision. The MOICT has a largely risk-based approach to supervision. There is strong momentum by the MOJ to introduce supervision of lawyers (emphasised by legislative changes made at the time of the assessment team's visit to Bahrain). There is also strong momentum to ensure that the new RERA, supported by the SLRB, will meet its responsibilities for supervision of all real estate agents and brokers.

106. The CBB requires remediation, has the appetite to apply sanctions and has imposed a range of sanctions and made referrals for prosecution, though there is scope to apply further sanctions as the number of onsite inspections increases. The MOICT has suspended or revoked CR registrations for compliance failures. The MOJ has revoked the licences of lawyers who do not meet statutory requirements of fitness.

107. All the existing operational supervisory authorities require additional staff resources to undertake comprehensive risk-based supervision.

108. Strong measures have been introduced with regard to NPOs. For example, all NPOs require permits to raise funds, receive or disburse funds, or send funds abroad. However, while the MLSD has developed risk ratings, its risk profiles have not yet meaningfully affected the type or frequency of measures applied to each NPO. The MLSD has taken the positive step of developing an outreach plan. It has an element of a risk-based approach in that, shortly before the assessment team visited Bahrain, the MLSD held a CFT workshop for those NPOs it considered had higher TF risk (See IO.10).

109. The MOICT has taken the very positive step of establishing the Sijilat system for the registration of basic and beneficial ownership of legal persons. The system itself seems to be robust and is helpful to reporting entities and the authorities, though some concerns exist on the accuracy of beneficial ownership information in all cases (See IO.5).

110. The FID has conducted some strategic analysis on emerging and domestic trends. More in depth analysis of trends and typologies to better support the operational needs of operational authorities is encouraged.

111. The FID adopts a risk-based approach to categorising STRs received so as to prioritise its review and development of financial intelligence. FID's high level of resources and its access to a vast number of databases means that there is no loss of effectiveness as it reviews all STRs and other intelligence to a minimum level and is able to respond swiftly to any additional intelligence.

112. The FID is the central hub for financial intelligence and has a close relationship with other LEAs. Both the FID and PPO use a wide variety of financial and other information and intelligence for ML and associated predicate offence investigations, though the number and type of ML cases investigated are not in line with Bahrain's risk profile, with lower than expected numbers of ML prosecutions in general and complex prosecutions in particular (See below).

113. Initial investigation of ML cases is carried out by the FID and referred to the PPO for judicial investigation; the majority of ML cases have been initiated by the FID. Different types of ML case are pursued, including self-laundering, stand-alone and third party ML. However, there is a disproportionate focus on the investigation of predicate offences, the assessment team has a concern that Bahrain pursues predicate offences at the expense of ML investigations (i.e. not all the major proceeds generating crimes are systematically pursued for ML prosecution) and the majority of ML convictions so far relate to self-laundering. In addition, while parallel financial investigations have been carried out in some cases with high amount of proceeds, they are not systematically pursued. In recognition of the importance of focussed prosecution of complex ML, the PPO has agreed to create a dedicated unit to prosecute ML (See IO.7).

114. A number of the ML cases prosecuted are associated with investigations into fraud (including breaches of trust) and illegal fund raising. The quality of the most recent ML investigations appears to be high but the number and types of investigations is lower than that warranted by ML risk profile of Bahrain as it appeared to the assessment team at the time of the onsite visit. Further, major proceeds generating offences such as corruption and prostitution are not

systematically pursued for possible ML prosecution and ML charges are not pursued vigorously when funds are transferred abroad.

115. TF investigations are referred to the FID by other authorities within the MOI and by the NSA. The FID has recognised the importance of focussing on and resourcing the work of combatting TF separately to ML by establishing a separate department. However, TF cases are mostly identified as a result of terrorism investigations (with only one independent TF case initiated during the assessment period). Any possible financial aspects are considered in each terrorism investigation. Investigated cases are the primary contributor to Bahrain's understanding of risk, thus it is not clear to what extent Bahrain's investigation and prosecution of TF addresses its risks (See IO.9).

116. Following ML convictions, the PPO and the FID were able to secure confiscation of cash, money in bank accounts, real estate, cars, and shares in companies and there is evidence that instrumentalities of crime, particularly for TF, are systematically confiscated. There has also been confiscation of non-declared cash at the borders. However, a confiscation policy has not been articulated. The 10 ML cases where there have been confiscations since 2012 have involved underlying predicate offences of prostitution, illegal fund raising, fraud, breach of trust and a cash courier. Figures have not been provided for confiscation in relation to predicate offences committed where there has been no ML conviction. Overall, confiscation activity appears limited (See IO.8).

117. Financial institutions generally implement TFS without delay, DNFBPs supervised by the MOICT [real estate agents which are structured as companies (until September 2017 at which point, real estate sector was transferred to a separate authority, RERA under SLRB), DPMS, accountants and auditors] also have legal obligations to implement TFS, without delay. Both the CBB and the MOICT issue notifications to their respective reporting entities on changes to the relevant UN lists. DNFBPs supervised by the MOJ and RERA do not receive any notifications about changes to these lists. The CBB supervises compliance with TFS but the assessment team has a concern about the priority in this area (See IO.10).

118. The importance of international co-operation to Bahrain has been recognised by the establishment of a dedicated office within the PPO to address international co-operation requests. A variety of types of assistance have been provided in response to MLA requests, involving a range of authorities. Co-operation, including extradition, has been constructive and timely to a large extent, although timing for extradition has been variable. The number of criminals extradited is significant in light of Bahrain's size and population. International co-operation on TF is generally dealt with by the security and intelligence agencies, including the FID, using informal mechanisms. Bahrain has to some extent sought assistance from other jurisdictions to pursue domestic ML (and associated predicate criminality) and TF.

### *National co-ordination and co-operation*

119. There is strong political commitment to ensuring that Bahrain has a robust AML/CFT framework. The country appears to have high level co-ordination and policy making mechanisms.

120. The NPC was formed in 2001[2] with a responsibility to establish general AML/CFT policies. In practice its role has extended to high level co-ordination and this is now reflected explicitly in legislation. Meetings are held quarterly and have included consideration of disclosure of suspicion, DNFBPs, NPOs, issues raised by individual authorities such as the FID, how to address deficiencies and other revisions to the framework such as how to ensure that banks implement TFS without delay. The committee's work has not yet evolved to cover risk based approaches to ML/TF. The NPC has established a sub-committee-, namely the Legislation/Policy Committee (2017). A separate committee, the National Committee on the Implementation of UNSC Resolutions, has also been established (initially, it was a subcommittee of the NPC). Its memberships consists of: MOFA (chair); MOI; the Bahrain Defence Force; the NSA; MLSD; CBB; MOJ; Islamic Affairs and Endowments; Customs Affairs; Civil Aviation Affairs; and the General Organisation of Sea Ports. The committee/subcommittee meets every four months and as needed.

121. Strategies are developed every three to five years; the current strategy dates to 2012. There are several action plans which have been made under the strategy.

122. Consideration of the enactment of AML/CFT legislation and preparation of the NRA has taken place at the national level through the NPC. There has also been discussion by the committee in relation to discrete matters such as the publication of MOI statistics, and the resolution of issues such as the development of the STR system used by FIs and the development of the MOICT's AML/CFT department.

123. The Legislation/Policy Committee considers every proposal for legislative change. The National Committee on the Implementation of UNSC Resolutions has addressed sanctions implementation since 2012. It includes both TF and PF in its remit. This Committee, which is chaired by the MOFA, meets four times per year (and when necessary) to discuss policy and operational issues related to UNSCRs, including the communication of UN sanction lists to reporting entities. The committee has been effective in recognising delays in the system for implementation of UNSCRs (and potentially in the freezing of assets). The committee is also responsible for identifying possible entities for designation to the UN and consideration of requests for the potential removal of persons from the relevant UN lists. For example, the committee was involved in the delisting of two Bahraini nationals from the UN 1267 list.

124. While there have been a range of national initiatives coordinated or discussed within the auspices of the NPC framework, the overall approach does not yet comprise a comprehensive approach to coordinating the establishment and monitoring of national policies and activities.

125. Domestic bilateral and multilateral co-operation at the operational level is strong in relation to both ML and TF. MoUs are not needed.

[2] Memberships consists of: CBB (Chair); MOI; MoFA; PPO; MOICT; SLRB; Ministry of Finance; MOJ, MLSD; NSA; Ministry of Youth and Sports Affairs, Legislation and Legal Opinion Commission and Customs.

126. At the preventive stage, there is strong co-operation between the FID and the CBB and the MOICT. Both the CBB and the FID receive STRs from FIs through a joint IT system. The two authorities routinely share information and views, including on STRs, and have formed joint investigation teams. This co-operation has assisted the development of criminal cases (See IO.3). The MOICT is linked electronically with other authorities in Bahrain through the Sijilat system, which is also used for sharing information. It receives STRs from DNFBPs it supervises and discloses each STR and a basic analysis of it from the MOICT's records promptly to the FID. The MOICT exchanges information with other supervisory authorities, particularly the CBB; for example, it alerts the CBB to relevant matters arising from its onsite inspections, checks registration information with the CBB and alerts the CBB to potential unlicensed financial activity. The MOICT spontaneously shares CR information with the FID. In addition, there is co-operation by all three authorities together; there have been onsite inspections which have included representatives from each of the CBB, the MOICT and the FID. There is two-way information exchange in connection with NPOs between the MLSD on the one hand and the CBB and the FID on the other; there is also discussion between the MLSD and the MOJ on fund raising.

127. The FID is the hub for financial intelligence and investigatory activity. The FID has direct access to the Sijilat system and to criminal records and ongoing cases through the Najem system[3], which enables it to cross-reference and enrich its operational analysis. The Najem system has different access levels to ensure that information that should be kept for instance, strictly for the use of the FID, is maintained that way. The FID and the PPO work collaboratively with other relevant competent authorities to initiate and develop ML investigations and prosecutions. Domestic co-operation between LEAs is strong and, during the initial and judicial investigations, the FID and the PPO work closely with other police units within the MOI and the CBB. Information held by the CBB on CDD is exchanged very quickly.

128. There is strong domestic co-ordination by the authorities within the MOI and the NSA in relation to initiate investigations of terrorism and TF offences and to progress investigations once started. This enables intelligence to be shared rapidly in all cases between the MOI (CID, FID and Customs) and the NSA. Task forces can include representatives of all of these bodies and the PPO. The FID also liaises

[3] The Najem system is the unified criminal database system that is used in almost all operational directorates in MOI (e.g. police stations, General Directorate of Anti-Corruption and Economic and Electronic Security and its associated directorates, narcotics, General Directorate of Anti-corruption and Economic and Electronic Security and its associated directorate, Prison Directorate, Control Rooms, Coast Guard, Passport, Traffic, Certificates and permits section, Lost and found, forensic lab, etc.). It is integrated with many external and internal systems; however the main integration is between the police, public prosecution and criminal court, in order to have a complete cases cycle. The Najem system includes several modules, for example: cases; detentions and criminal records. Among its objectives, the Najem system is said to provide a comprehensive, integrated suite of applications based on a common open architecture enabling government to government, government to business/non-profit and government to citizen communication and exchange of information. It is also understood as a platform that enhanced collaboration while protecting independence of each party, and the security and confidentiality of information shared.

closely with the CBB where bank statements and other related information are needed for an investigation.

129. Co-operation between the FID and Customs has been key to the successful results in the confiscation of falsely or undeclared cross-border currency transactions. Customs also shares other information with the FID and the CBB, such as on trade based issues.

130. Co-ordination of PF is carried out by the UN National Committee. The Committee benefits from strong input by Customs and works in close co-operation with the NPC, the NSA and MOFA. At the bilateral level there has been positive co-operation and information exchange between the CBB and the FID in relation to a breach of PF requirements (See IO.11).

### *Private sector's awareness of risks*

131. The authorities propose to issue the final version of the NRA report to the private sector.

132. IO.3 analysis describes what information has been provided to reporting entities by the CBB and the MOICT. Part of this information is directly pertinent to increasing awareness of ML/TF risks, internal controls, high risk customers, STR trends etc. The FID has provided feedback on individual STRs and also has exchanges with MLROs directly as well working through the CBB and MOICT.

133. There is generally a good level of understanding of ML/TF risks among FIs and a varied level of understanding among DNFBPs (See IO.4). The NRA process and the national understanding of risks has benefitted from input by FIs and, to a lesser extent, DNFBPs on their firm and sector perspectives.

### *Overall conclusions on IO.1*

134. **Bahrain is rated as having a moderate level of effectiveness for IO.1.**

# CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

## Key Findings and Recommended Actions

### *Key Findings*

#### *Use of financial intelligence (Immediate Outcome 6)*

**Bahrain achieved a substantial level of effectiveness for IO.6.**

1. Financial intelligence and other information are accessed and used in investigations for ML, TF and associated predicate offences, including for the development of evidence for associated predicate offences.
2. The FID is a law enforcement FIU, within the MOI and is well integrated through electronic systems and direct communication channels with other agencies, including the CBB, the SLRB, PPO, and Customs. The FID has access to several databases which enhance its ability to produce financial intelligence of quality using a variety of sources.
3. There is strong and effective co-operation and co-ordination between FID and other law enforcement authorities including national security agencies, CBB and MOICT.
4. The FID supports the operational needs of LEAs to a considerable extent. Strategic analysis needs to be further developed to identify new and emerging trends and patterns to be used as a basis for operational actions by relevant agencies.
5. STR levels need to be improved as noted under IO.4, given that reporting by DNFBPs is low and there are some concerns about quality.

#### *ML investigation and prosecution (Immediate Outcome 7)*

**Bahrain achieved a moderate level of effectiveness for IO.7.**

1. Bahrain has a sound legal framework for the investigation of ML. The initial investigation of ML cases is carried out by the FID and referred to the PPO for judicial investigation. The PPO and FID work collaboratively with other relevant competent authorities in the course of ML investigations and prosecutions. The majority of ML cases are initiated by the FID, while a number of cases are referred to the FID by specialised law enforcement units investigating predicate offences. In some cases, parallel financial investigations are conducted upon the identification of a financial component of a predicate offence.
2. During 2012-2017, Bahrain initiated 43 investigations for ML, resulting in 34 persons convicted of ML, and a number of ongoing cases. Half of the investigated cases are associated with investigations into fraud (including breach of trust and foreign corruption) and illegal fundraising; the latter of which does not correspond to the primary ML risks identified by Bahrain. Overall, Bahrain does not consistently investigate and prosecute ML in line with its ML risks.

3. Bahrain demonstrated that it is pursuing different types of ML cases for prosecution, including self-laundering, stand-alone, and third party ML to some extent; however, the majority of the ML convictions achieved relate to self-laundering.
4. A wide range of sanctions are available for ML for natural and legal persons. Sanctions of imprisonment up to seven years, a fine up to BHD 1 million (EUR 2 million), and confiscation are available. In practice, the sanctions applied range from one to seven years and include fines up to BHD 200 000 (EUR 431 077). The sanctions for ML are assessed as proportionate, dissuasive, and effective.
5. Alternative criminal justice measures are available and pursued to a limited extent.

### *Confiscation (Immediate Outcome 8)*

**Bahrain achieved a moderate level of effectiveness for IO.8.**

1. Bahrain's legal framework for seizing, freezing and confiscating assets is adequate and has been used to some extent. The disclosure system for incoming and outgoing cross border currency movements and BNIs was significantly strengthened at the time of the onsite.
2. There is no specific policy or guidelines requiring LEAs to pursue confiscation as a policy objective, however, authorities seem to pursue it as part of a proceeds-of-crime approach to combat crime. Bahrain prioritises settlements in order to return funds to victims, particularly in fraud cases.
3. Overall, confiscation results can be considered modest, taking into account Bahrain's risk profile and role as a regional financial centre.

### *Recommended Actions*

### *Immediate Outcome 6*

1. Bahrain should further pursue and develop strategic analysis to support the operational needs of law enforcement agencies. Such analysis should identify emerging trends, patterns, typologies and vulnerabilities, as well as an appropriate response, which considers Bahrain's context.
2. The FID should continue its engagement with reporting agencies through feedback, training and other communication tools.
3. Bahrain should continue to raise awareness about the importance of using financial intelligence by different law enforcement agencies while pursuing predicate offences and ML cases and as part of a larger proceeds of crime approach. The FID and other LEAs should follow a more integrated approach in order to fully exploit the vast amount of financial intelligence accessible by the FID.

### *Immediate Outcome 7*

1. Bahrain should ensure that all units within the MOI that investigate predicate offences are referring cases of possible ML to the FID. Similarly, Bahrain should ensure that parallel investigations are systematically pursued, and joint investigations are used where practicable.
2. The FID and PPO should prioritise the investigation and prosecution of all

types of ML in accordance with the country's risks. Specifically, Bahrain should investigate and prosecute ML in line with its highest risk predicate offences.

3. Bahrain should enhance the investigation into stand-alone ML, third party ML, ML involving legal persons, and the laundering of proceeds from foreign predicate offences.
4. Bahrain should ensure that adequate resources are allocated to the FID and PPO to enhance the investigation and prosecution of complex ML schemes and develop its technical and human resource capabilities in this area. The planned creation of a dedicated ML unit within the PPO will help to support this objective.

*Immediate Outcome 8*

Bahrain should:

1. Develop policy guidelines and strategies on when to pursue seizures and confiscation for a consistent approach across LEAs.
2. Take measures to adequately track trends and results in terms of seizure and confiscation, through consolidated statistics.
3. Consider further work in the matter of asset recovery, including appointment of a specialised prosecutor within the PPO, and further strengthening its procedures for asset management, within its plans for a separate ML unit within the PPO.
4. Provide training and awareness to law enforcement and prosecutors, on the need to pursue and prioritise confiscation and asset tracing and recovery investigations, for all predicate offence investigations. To this effect, Bahrain noted it has started work on training through the Judicial and Legal Studies Institute of the MOJ.

135. The relevant Immediate Outcomes considered and assessed in this chapter are IO.6-8. The Recommendations relevant for the assessment of effectiveness under this section are R.1, 3, R.4 and R.29-32.

## *Immediate Outcome 6 (Financial Intelligence ML/TF)*

### *Use of financial intelligence and other information*

136. The FID (Bahrain's FIU) and the PPO, are the authorities responsible for conducting ML investigations in Bahrain and as seen in the case studies presented under IO.7, they both use a wide variety of financial and other information and intelligence for ML and associated predicate offence investigations. The FID is the central hub for financial intelligence and has a close relationship with other LEAs.

137. The FID has access and uses a variety of Government databases: the Traffic Police Department, General Directorate of Nationality, Passports and Residence Affairs, and the Sijilat system, which captures basic and beneficial ownership information of legal persons (See IO.5). The FID also accesses criminal records and refer to ongoing cases (through the Najem system) being pursued by other agencies, which enables it to cross-reference and enrich its operational analysis and aids in its investigations. The FID has also access to intelligence reports from other LEAs and agencies. Similarly, the FID accesses bank statements and information on foreign transfer funds involving money or value transfer services to pursue investigations.

138. The FID has used its ability to search private and public premises or persons, as well as to take witnesses and seize evidence, through production orders, obtained from the PPO. Information from reporting institutions can be obtained and has been obtained, pursuant to Art. 5(d) of Decree Law No.4 of 2001 (which indicates that institutions should provide the FID with further information or assistance upon request). There are no restrictions as to the information that the FID can request, once there is probable cause, and reporting entities noted that the FID often goes back to them formally as well as informally for further information, when analysing an STR.

139. Further, upon obtaining a court order, any person must submit information, including documents, requested to the FID, as described in R.31. No challenges were noted in terms of timelines or procedures to obtain a court order.

140. In any case, to prevent asset flight while a court order is obtained, the FID has the ability to administratively freeze assets for three days. This ability was used 17 times in 2014, 23 and 35 in 2015 and 2016, respectively, and 29 times in 2017 (as of November 2017).

141. The FID provided examples where special investigative techniques, including wiretapping, had also been used to gather information and develop evidence. For instance, in the investigation of ML involving a remittance company (See Box. 3 in IO.7) where the FID noted that the tapping of initial suspects, led to further generation of intelligence, which facilitated the identification of other suspects involved in the crime (i.e. cash smugglers).

142. There is close co-ordination and co-operation between the PPO and the FID which includes an ongoing feedback loop whereby the PPO provides its input to the FID on an ongoing basis on how to improve and enhance intelligence, information and evidentiary standards to develop a case.

143. Bahrain conducted 43 ML investigations (including multiple predicate offences) since 2012 of which, 10 convictions (involving multiple offenders) were obtained with the support of financial intelligence. Financial intelligence has also been integral for Customs to detect cash smuggling in the border (See IO.8), although this may not result in a ML offence being pursued.

144. Financial intelligence seems to be used to a lesser extent, by other LEAs, including the Anti-Corruption Directorate, where only six ML investigations were conducted, out of 230 corruption cases pursued by that Department since 2012. The use of financial intelligence to pursue ML investigations in the case of human trafficking and prostitution offences needs to be improved to identify patterns, networks and organised groups involved. During the interviews, LEAs, including the Anti-Corruption Directorate, noted however, that they often rely on intelligence provided by the FID, for the development of evidence, in the investigation of the predicate offence even if not for ML.

145. LEAs require further awareness and training to encourage the referral of cases to the FID, upon identification of a ML/TF aspect, or as noted in IO.7, in order to systematically conduct parallel investigations. It is a positive development that authorities reported to have established an internal MOI committee where all LEAs in charge of pursuing ML, predicate offences and TF meet and share intelligence and

information, including on training needs. Parallel financial investigations would also be valuable for the purpose of recovering proceeds of crime.

146. Intelligence is used for TF investigations, particularly that received from the NSA, or from the CID, following a terrorist incident, as TF investigations are included, for the most part, within terrorist acts investigations. Intelligence has also been useful in detecting cash courier violations which in one case led to a TF investigation (See IO.9). The FID's ability to intercept communications and conduct surveillance has been useful in this regard, to further obtain evidence. There is also a Joint Counter Terrorism Centre which brings together the FID, Bahrain's Interpol liaison and NSA, among other security agencies. Agencies involved in this joint group meet regularly to exchange information on potential terrorists and related TF information. Exchanges in this joint group, contributed to the identification of 26 FTFs by Bahrain and to their monitoring, as authorities seek to freeze the accounts of these FTFs and stop welfare payments, besides taking other actions (See IO.9).

147. A review of ongoing TF investigation cases by the assessment team has revealed that financial intelligence and analysis has also helped in identifying disbursement of funds to several unrelated individuals, and unusual activities in companies being used as a front to purchase explosives and other material in connection with terrorist acts. Authorities analysed bank statements and travel records to gather evidence for a case currently pending in court and for other cases made available to the assessment team (See also IO.9).

148. Financial intelligence and other information are accessed and used in investigations for ML, TF and associated offences to a large extent. However, having the FID within the MOI with other LEAs could be further benefited from, by providing greater awareness to other LEAs, of what the FID does, and the importance of conducting parallel investigations as set out at the beginning of this section. There is also a need of strengthening its joint or task force approach, of the FID with specialised agencies conducting the investigation of predicate offences, to focus more and readily identify ML/TF links. This will help integrate the vast amount of intelligence accessible by the FID in pursuing financial investigation in cases involving corruption, human trafficking etc., where network and pattern identification may help authorities go after the main suspects.

149. Bahrain's Authorities indicated that there are plans for a specialised ML unit within PPO, which should also help in this regard.

### *STRs received and requested by competent authorities*

150. The FID receives STRs, cross-border currency reports (disclosures), and it both receives and requests intelligence from other LEAs and international counterparts. Bahrain conducted 43 ML investigations (including multiple predicate offences) in total since 2012 (See details in Table 10 in IO.7). According to information presented by the FID and the PPO, nine of these cases derived from a number of STRs. TF investigations have also been pursued by the FID, which have had connections to STRs although no prosecution has been initiated from a STR.

151. All STRs received are classified by the FID following a risk-based approach, and depending on the outcome, they are filed, disseminated or used to pursue legal action. Overall the number of STRs has been increasing, see Table 4 below.

152. Most financial information is received through STRs filed by banks and other FIs. Reporting by some FIs and generally by DNFBPs is low (as further explained under IO.4). This is a concern, given the vulnerability of the sector (i.e. real estate) to ML in Bahrain, as noted in Bahrain's draft NRA. However, as explained in greater detail in IO.3, efforts are being made to further increase compliance in the DNFBP sector, not only as regards to STRs but AML/CFT generally, with the strengthening of current supervisors (i.e. MOICT) and the appointment of new supervisors for some of the sub-sectors.

153. STRs by FIs are received electronically and are also accessed by the CBB for supervisory proposes. This does not interfere or overlap with the FID analysis as the CBB does not conduct any parallel ML/TF investigations based on such STRs. It does however assist the CBB in assessing the quality of the STRs and inform its supervisory processes such as onsite examinations. The online system has been and continues to be enhanced to allow for more complete information and attachments to be sent together with the STR. No concerns of incomplete information were raised.

154. STRs from DNFBPs are received electronically by a specific assigned email since 2012, and will soon be automatically sent to FID via a new system which is being finalised. This should improve DNFBP reporting which is currently limited. As with the CBB, STRs are also shared online with the supervisor (MOICT) for supervisory purposes.

155. The FID also receives reports from other LEAs such as the Economic and Cybercrime Directorate, the Anti-Narcotics Directorate and the Immorality & Human Trafficking Directorate, among others. See Table 5 below.

156. The FID can and has requested reports or information from the PPO, any of the above Directorates and the CBB, in relation to for instance, currency exchange related violations. It can also request and has requested information from the MOICT as regards to company registration.

Table 4. **STRs received and workflow as of November 2017**

| Action | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | Total |
|---|---|---|---|---|---|---|---|
| Filed* | 369 | 634 | 855 | 1,046 | 764 | 518 | 4186* |
| Ongoing Investigation (under further review by the FID) | 0 | 0 | 4 | 15 | 136 | 533 | 688 |
| Disseminated to Security agencies | 9 | 9 | 3 | 14 | 16 | 14 | 65 |
| Disseminated to CBB | 0 | 1 | 0 | 0 | 0 | 0 | 1 |
| Disseminated for internal Investigation | 4 | 0 | 2 | 0 | 8 | 4 | 18 |
| Sent to PPO | 0 | 4 | 4 | 0 | 0 | 0 | 8 |
| Total | 382 | 648 | 868 | 1,075 | 924 | 1069 | 4966 |

*Note*: * The term "filed" should not be interpreted as a simple filing or archiving of a report. As explained below, regardless of its minimal threat level, a basic review will be performed for every STR. Authorities noted that some concerns exist regarding the quality and volume of STRs, especially those received from DNFBP sector, though it has been improving over the time. The assessment team also has similar concerns considering a large proportion of STRs are filed.

Table 5. **Reports received from other LEAs ML/TF**

| Years | ML | TF |
|---|---|---|
| 2012 | 17 | 7 |
| 2013 | 31 | 21 |
| 2014 | 26 | 37 |
| 2015 | 24 | 53 |
| 2016 | 35 | 46 |
| 2017 | 94 | 81 |
| **Totals** | **227** | **245** |

*Note*: This table only includes formal reports. A number of informal exchanges also occur, for example in the context of discussions on National Security.

157. The FID has an AML/CFT awareness department (Research and Co-operation Section), which focuses on enhancing the quality of STRs and frequently engages with a wide range of supervisors (CBB, MOICT, MLSD and MOJ). The FID also visits FIs and DNFBPs at their request (for capacity building and guidance) or to follow-up on issues which require clarification. The FID provides feedback to reporting entities on the STRs that they submit on a one-on-one basis, and sends statistics regarding the categorisation and quality of STRs to competent authorities (i.e. CBB) regularly, for them to follow-up with the respective entities as needed. The FID also publishes its annual reports and statistics on STRs reported [www.bahrainfiu.gov.bh/about-financial-intelligence-unit].

158. The CBB also advises the FID of any activity which may have gone unreported, if found when supervising an entity. Bilateral meetings are conducted with Money Laundering Reporting Officers (MLRO's; Compliance officers), to update them with upcoming trends in ML/TF crimes. One of the areas of focus for the FID during upcoming months will be increasing reporting in DNFBPs, following the incorporation of private notaries and lawyers as reporting entities.

### *Operational needs supported by FIU analysis and dissemination*

159. The FID is supporting the operational needs of LEAs to a considerable extent. The FID is a strong well-resourced FIU of 27 persons, which includes the Director, a researcher and a team of financial analysts; five of them dedicated to TF related analysis. As noted, at the beginning of this IO, it is embedded in the MOI and interconnected with other LEAs and government databases, which represent an advantage to the intelligence it produces. The majority of STRs are received electronically. Custom reports are also received electronically. The FID uses analytical tools and other software to pursue linkages between STRs, previous STRs, family members, banks statements, etc.

160. When a STR is received, according to the FID procedures, it is awarded a threat level which implies it will be subject to different steps of analysis, depending on the severity of the threat. At a minimal, all STRs are analysed against criminal sheet or background; it is identified if suspect is in/out of Bahrain; further information is requested from reporting entities, and FID databases are reviewed for further information on the suspect (past information).

161. Enhanced review of STRs includes a thorough review of bank accounts, financial transactions and assets owned by the suspect and when needed, interviewing the suspect regarding the STR (without disclosing the existence or contents of STR itself). Procedures for the higher risk STRs, include requesting information from the NSA, Interpol, foreign FIUs, and the Search and Detection Directorate, which investigates high value theft and robbery and which the FID has formed joint teams with.

162. The FID noted that there were no backlogs in the review of STRs at the time of the onsite and that if information for the relevant STR is readily available and the STR does not require for instance, international co-operation, the preliminary analysis of STRs is normally completed within 24 hours. What additional information is needed or what further steps need to be taken with regard to a STR depends on risk as explained in paragraph 160 above. Besides, the FID has in place an escalation process for past-due STRs. A STR is determined to be past-due if it is not fully reviewed within three to five months (deadline is only set as a reference based on average time considered as past due STRs by the FID). Escalation is done to varying levels of seniority to ensure STRs are reviewed within appropriate times.

163. Once analysed, STRs are used for the FID's investigations or disseminated to other LEAs as shown in the tables below and with a number of agencies.

Table 6. **Financial intelligence disseminated to other LEAs for ML/TF**

| Years | ML | TF |
|---|---|---|
| 2012 | 6 | 16 |
| 2013 | 36 | 10 |
| 2014 | 28 | 9 |
| 2015 | 63 | 31 |
| 2016 | 48 | 32 |
| 2017 (as of November 2017) | 58 | 54 |
| Total | 239 | 152 |

Table 7**. Financial intelligence disseminated to other LEAs (Breakdown by LEA)**

| LEA | Total | LEA | Total |
|---|---|---|---|
| CID | 54 | Bahrain Defence Force | 6 |
| NSA | 84 | Legal Affairs Directorate | 3 |
| Anti-Economic Crimes Directorate | 50 | Antinarcotics Directorate | 10 |
| Anti-Corruption Crimes Directorate | 28 | JCTC | 4 |
| Cyber Crimes Directorate | 3 | Police Stations | 20 |
| Discipline & Crime Prevention Directorate | 15 | Passport, Nationality and Immigration Affairs Directorate | 2 |
| PPO | 12 | MOI | 3 |
| MOI Court | 9 | Office of Undersecretary of MOI | 4 |
| Office of Chief of Public Security | 18 | Saudi Interpol Communications Directorate | 1 |
| Detection & Patrolling Directorate | 8 | Internal Audit Directorate | 3 |
| Interpol | 28 | Terrorism Combating Directorate | 5 |
| Military Courts | 16 | Human Trafficking Affairs Directorate | 2 |

Table 8. **STRs contents disseminated to other LEAs**

| Years | Input (STR) | Output (STR) | | | | |
|---|---|---|---|---|---|---|
| | | Economic Security Directorate | Cyber Security Directorate | Anti-Narcotics Directorate | Immorality and Human Trafficking Directorate | Sent to PPO (for ML) |
| 2012 | 382 | 9 | 0 | 0 | 0 | 0 |
| 2013 | 648 | 8 | 2 | 12 | 0 | 7 |
| 2014 | 868 | 2 | 1 | 15 | 4 | 4 |
| 2015 | 1075 | 4 | 1 | 19 | 2 | 0 |
| 2016 | 924 | 9 | 0 | 24 | 0 | 2 |
| 2017 | 1069 | 2 | 0 | 0 | 1 | 1 |
| Totals | 4966 | 34 | 4 | 70 | 7 | 14 |

Table 9. **TF STRs* vs. cases sent for prosecution**

| Year | TF STRs received | Other TF related information received from LEAs (including police stations and JCTC) | Sent to the PPO | Sent to other LEAs (for example, Criminal Investigation Directorate and JCTC) |
|---|---|---|---|---|
| 2012 | 3 | 5 | 0 | 9 |
| 2013 | 5 | 18 | 1 | 24 |
| 2014 | 8 | 33 | 2 | 39 |
| 2015 | 7 | 48 | 1 | 40 |
| 2016 | 4 | 39 | 0 | 53 |
| 2017 | 2 | 16 | 0 | 52 |
| Total | 29 | 159 | 4 | 217 |

*Note:* *All received from FIs, majority of banks.

164. As can be seen from the tables above, financial intelligence as a whole is used to a large extent, particularly by Directorates investigating predicate offences and also for ML/TF investigations, even when STRs have not directly resulted in a TF prosecution. The assessment team believes it is positive that intelligence is being shared across the breadth of law enforcement community, including the Immorality and Human Trafficking Directorate, considering prostitution as one important threat to Bahrain. Information has also been shared with the Anti-Corruption Directorate. More could be done to use financial intelligence to pursue financial crime in line with the country risk profile and this had an effect in the not so positive results at the ML/TF conviction level, noted in IO.7 and IO.9.

165. Bahrain should further work in the area of strategic analysis, which needs to be more developed. The FID needs to focus on conducting more in depth strategic analysis to identify trends and patterns. Currently two staff members within the FID are dedicated to conducting strategic analysis. The FID needs to build capacity to conduct analysis of risks, trends and methods of ML/TF behaviour that would allow it to develop typologies, profiles and further tools to aid its operational analysis. This

could for example, include priority issues such as human trafficking, illegal fund raising, TF and sophisticated ML networks where the FID can add value. The FID has initiated some preliminary work in these areas (e.g. on crypto-assets and illegal transfer of funds), however strategic analysis is not carried out systematically with a view to identify new and emerging trends and provide detailed lead information to other law enforcement and for its own investigations. A more practical approach would help address the needs of agencies involved, including other LEAs and PPO.

166. Notwithstanding these areas that need further work, case examples presented by Bahrain, related to ML and illegal fundraising, lead the assessment team to believe that the FID, has to a large extent, supported the purposes of authorities, both of LEAs and other competent authorities such as the CBB, though more focused attention in the area of strategic analysis is needed in line with Bahrain's risk and context.

### *Co-operation and exchange of information/financial intelligence*

167. There is continued and effective co-operation between the FID and all other supervisory, security entities and departments which includes periodic bilateral meetings to ensure effective implementation of the AML/CFT framework. As all relevant authorities are part of the National Policy Committee, this facilitates side discussions and informal exchange occurs where needed. In particular, the PPO provides feedback to the FID in regard to improving the quality of evidence brought forward to the PPO.

168. The FID cooperates closely with the CBB in the provision of guidance and training for FIs and DNFBPs as well as NPOs, and to ensure that relevant information is shared which has in more than one occasion helped to discover irregularities and cases of non-compliance with regulatory provisions, such as those related to targeted financial sanctions (See Box 8 in IO.11). Within the MOICT, the main supervisor for DNFBPs is a recurrent partner, due to its role as a company registrar and as a supervisor. As noted in IO.8, co-operation with Customs is also close and effective. The FID also cooperates and exchanges information at an international level and further details of this are provided under IO.2.

169. Communication is generally easy given the nature and placement of LEAs, all within the MOI and the size and context of Bahrain. Exchanges of information occur in a secure and confidential manner. For example, notwithstanding that the FID and all LEAs are within the MOI and have access to some of the same databases, such as the Najem system, as discussed in Chapter 1 of this report and R.29, the Najem system has different levels of access and the FID's information is adequately protected. The FID has secure channels to disseminate information, including encrypted email service to communicate with other LEAs in certain countries. Authorities are also bound by the provisions of Decree law No. 4, Art. 2.6 and other confidentiality provisions.

### *Overall conclusions on IO.6*

170. **Bahrain is rated as having a substantial level of effectiveness for IO.6.**

## *Immediate Outcome 7 (ML investigation and prosecution)*

### *ML identification and investigation*

171. The identification and preliminary investigation of ML cases are conducted by the FID and subsequently referred to the PPO for judicial investigation. The majority of ML investigations are triggered by investigations into associated predicate offences or STRs filed to the FID.

172. Domestic co-operation between LEAs is strong in the course of ML investigations and prosecutions. During the investigation process (both initial and judicial), the FID and PPO work closely with other police units within the MOI, the CBB and the MOICT. Bahrain provided a number of case examples which indicates that co-operation between authorities is robust while pursuing ML investigations, including the use of joint investigations.

173. As noted in IO.6, the FID, a law enforcement FIU, is embedded within the MOI and has direct access to a wide-range of financial intelligence and other police units' databases, which supports its preliminary ML investigations. As noted in R.31, the relevant authorities in Bahrain possess powers to conduct investigations into ML and associated predicate offences. In practice, Bahrain utilises its full range of coercive and non-coercive investigative techniques and tools when conducting ML investigations. In regard to coercive measures, authorities require a court order, which can take up to 24 hours. Bahrain states that orders are relatively easy to obtain and are often obtained within hours.

174. In general, there is an integrated approach to ML investigations within the MOI. When a financial component is identified in relation to an investigation into a predicate offence, the specialised directorates of the MOI (e.g. Anti-Corruption Directorate, Immorality and Human Trafficking Directorate) exchange information with the FID. The specialised directorates also have embedded officers trained in the identification of ML. The majority of exchanges of information is informal and, therefore, undocumented. Statistics are unavailable to demonstrate the true extent of this co-operation.

175. The decision to conduct parallel financial investigations is at the discretion of LEAs and the PPO. The PPO states that it pursues parallel investigations when proceeds are obtained from a predicate offence, and when the perpetrator uses or engages in transactions with the proceeds obtained from the predicate offence. However, based on the number of investigations into predicate offences compared to the number of ML investigations, it does not appear that parallel investigations are systematically pursued. Bahrain states that this is due to the fact that many of the predicate offence cases involved small amounts of money (mostly related to fraud). Where the amounts of proceeds are higher, the PPO would undertake a parallel investigation. The authorities provided a number of case studies where parallel investigations were pursued, a recent example is provided below (See Box 1). However, the assessment team considers that there is a disproportionate focus on the investigation of predicate offences, at the expense of ML investigations or parallel investigations. There are also concerns that Bahrain does not identify complex ML cases.

**Box 1. Parallel Investigation Case (2017)**

This case was triggered as a result of a notification to the FID from the PPO. Suspect A was an executive manager in Company A and illegitimately increased his shares in Company A from 15% to 32% and illegally obtained profit by signing contracts with other companies, which harmed Company A's interests. Further investigations were conducted by the PPO and led to the discovery of Suspect A's illegal activities, leading to ML charges for Suspect A, as well as Suspect B who was a member of the Board of Directors and authorised to sign on behalf of Company A. This case is currently in the High Criminal Court.

176. Since 2012, Bahrain has initiated 43 ML investigations, involving 115 individuals. Of these investigations, 10 cases resulted in convictions (involving 34 individuals), four cases are presently in the prosecution stage, 10 cases are currently under investigation, and the remaining 19 investigations are closed (See Table 10). While these figures represent total ML cases, multiple persons may be involved in each case. Further, multiple underlying predicate offences may exist for each case (which accounts for the total number of cases equalling 50 rather than 43).

Table 10. **ML Cases (2012-2017*)**

| Underlying Predicate Offence | Total Number of Cases | Current status | | | |
|---|---|---|---|---|---|
| | | Closed | Investigation Stage | Prosecution Stage | Convictions |
| **Fraud** | 10 | 2 | 2 | 3 | 3 |
| **Cash courier** | 6 | 1 | 4 | | 1 |
| **Illegal fund raising** | 11 | 6 | 2 | | 3 |
| **Tax evasion** | 1 | 1 | | | |
| **Foreign corruption** | 1 | | 1 | | |
| **Prostitution** | 5 | 1 | | 1 | 3 |
| **Human trafficking** | 1 | | | | 1 |
| **Counterfeiting** | 2 | | | 2 | |
| **Breach of trust** | 6 | 4 | | | 2 |
| **Narcotics** | 3 | 3 | | | |
| **Suspicious transfer (unknown predicate offence)** | 3 | 3 | | | |
| **Illegal trade of work permits** | 1 | 1 | | | |
| Total cases | **50** | **22** | **9** | **6** | **13** |

*Note*: *Data from 2017 is from 1 January to 22 November 2017

177. In terms of the trend of ML convictions over the period 2012-17, ML convictions peaked in 2016, with four cases resulting in convictions (See Table 11).

Table 11. **ML convictions by year (2012-17)**

| Year | # ML cases resulting in conviction | Total # of individuals convicted of ML |
|---|---|---|
| **2012** | 2 | 2 |
| **2013** | 1 | 15 |
| **2014** | 3 | 9 |
| **2015** | 0 | 0 |
| **2016** | 4 | 8 |
| **2017** | 0 | 0 |
| Total | **10** | **34** |

178. To provide a contrast to table 10, the below table indicates the frequency of predicate offence investigations, prosecutions, and convictions during the same sample period. Based on table 12, it is evident that ML charges are not consistently initiated when investigating/prosecuting predicate offences. This is especially clear in the case of fraud (including corruption and breach of trust) where 3 222 convictions were secured for the predicate offence, yet only four ML convictions were secured where this was identified as the underlying predicate offence.

Table 12**. Predicate Offence Cases (2012-2017)**

| Offence | Total Number of Cases | Current Status | | | |
|---|---|---|---|---|---|
| | | Closed | Investigation Stage | Prosecution Stage | Conviction |
| **Fraud (including breach of trust)** | 6 190 | 1 747 | 578 | 648 | 3 222 |
| **Cash courier** | 17 | 12 | 4 | 0 | 1 |
| **Illegal fund raising** | 19 | 12 | 3 | 0 | 5 |
| **Prostitution** | 221 | 8 | 67 | 17 | 129 |
| **Human trafficking** | 44 | 4 | 25 | 4 | 11 |
| **Counterfeiting** | 353 | 161 | 147 | 1 | 44 |
| **Narcotics** | 537 | 7 | 37 | 64 | 429 |
| **Illegal trade of work permits** | 1 | 0 | 0 | 0 | 1 |
| Total cases | **7 382** | **1 951** | **861** | **734** | **3 842** |

179. In terms of resources, the FID has eight staff dedicated to carrying out ML analysis. The PPO has 12 staff who conducts ML investigations and prosecutions. The PPO is currently working on reforming its organisational structure to establish a specialised prosecution office dedicated to ML. Authorities state that this unit would be established by the last quarter of 2018 and would help further enhance their capabilities in conducting complex financial investigations going forward. The assessment team encourages Bahrain to establish this specialised prosecution unit as an increase in resources will allow authorities to adjust their focus on ML cases, particularly in high risk areas.

3

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

180. The shortcomings identified under IO.1 impact the extent to which ML activity is being investigated and prosecuted consistently with Bahrain's threat and risk profile, and national AML/CFT policies. For example, the ML analysis does not include a detailed analysis of the ML risks emanating from organised crime, the cross-border element of ML risks to Bahrain, and the risk posed by legal persons and arrangements. As a result, the assessment team questions whether the investigative resources are appropriately allocated to high risk areas, and whether Bahrain is adequately investigating ML consistent to its risk profile.

181. As noted in Chapter 2, The NPC (with its subcommittee, the Legislation/Policy Committee) sets and coordinates AML/CFT policy and counterterrorism efforts. The assessment team was advised that the current AML/CFT strategy was developed in 2012, and was primarily aimed at addressing AML/CFT related deficiencies identified in the 3rd round mutual evaluation. In addition to the national policy activity on AML/CFT, there are also other positive national frameworks which address key areas of predicate criminality or other themes. In particular, a national anti-corruption strategy and an anti-corruption committee were introduced in 2015.

182. As noted in IO.1, the draft NRA identifies the highest risk predicate offences for ML as: investment fraud; smuggling of cash and cash equivalents; and immorality and prostitution. Medium risk offences for ML are: narcotic crimes; human trafficking; illegal trade in work permits; and corruption. Only illegal fundraising was identified as low risk.

183. When comparing the number of ML investigations with the identified highest ML risks outlined in the draft NRA, it is unclear whether Bahrain investigates and prosecutes ML in line with its risk profile. For example, Bahrain identifies investment fraud as a high risk for ML, yet it is unclear how many investigations were initiated into investment fraud as Bahrain does not maintain statistics specific to investment fraud cases; instead, it is reflected in the general fraud category. As a result, it is not possible to determine how many investment fraud cases included a parallel investigation into ML. Nevertheless, Bahrain states that all investment fraud cases result in a ML investigation. As noted in Table 10, however, there were only two ML convictions where fraud was the underlying predicate offence (which covers all types of fraud, including investment fraud).

184. In regard to the smuggling of cash and BNIs, which was also identified as high risk for ML, Bahrain's Customs is well is well resourced and active in detecting cash of illegal origin. In 2008, Customs moved to MOI (from Ministry of Finance), which includes other key authorities for Bahrain's AML/CFT regime, such as the FID to further strengthen its capacity and resources. It fully benefits from access to the police databases there is a strong co-ordination and co-operation between FID, Customs and Police. Bahrain initiated 17 investigations between 2012 and 2017. Of these 17 investigations, six resulted in a corresponding ML investigation (resulting in one ML conviction). Given the use of cash within Bahrain, cross-border risks, and the total number of non-disclosed carriage of cash and BNIs into Bahrain (95 incidents identified between 2012 and 2016); the assessment team believes that

Bahrain could enhance the frequency of ML investigations in relation to cross-border cash of illicit origin.

185. That considered, Bahrain has recently strengthened its legislative regime for cross-border transportation of currency and BNIs, and authorities are optimistic that the new framework will enhance their capacity to deal with this issue. Further, Bahrain has some measures in place to mitigate the risks posed by cash, such as requiring FIs and DNFBPs to identify and verify the source of funds of cash transactions over BHD 6 000 (EUR 12 945).

186. Finally, in regard to immorality and prostitution, 221 investigations were initiated between 2012 and 2017, yet only five of these investigations resulted in a corresponding ML investigation, resulting in two ML convictions. Bahrain states that the low number of ML investigations/prosecutions related to proceeds generated from prostitution is a result of a focus to pursue prostitution rings and their organisers/managers. Bahrain states in its draft NRA that the managers of prostitution services maintain their proceeds in the form of cash, and do not inject it into the financial system, making it difficult to detect. Based on these figures, the assessment team has concerns that the Bahraini authorities are not adequately pursing ML charges in this high risk area.

187. In contrast to these three high risk areas, Bahrain identified illegal fundraising as the only low risk predicate offence for ML. Illegal fundraising in this context relates to fundraising fraud (and not TF). Between 2012 and 2017, 19 investigations into illegal fundraising resulted in 11 parallel ML investigations (resulting in three convictions). Thus, nearly half of all illegal fundraising cases include an ML investigation. This raises concerns as to Bahrain's assessment of risk and a potential misallocation of resources, considering that an identified low risk area for ML is resulting in a number of parallel ML investigations and ML convictions.

188. The assessment team also notes that narcotic crimes, which occur relatively frequently in Bahrain (on average, 88 cases per year investigated by LEAs), rarely result in ML investigations, and no ML prosecutions or convictions have been obtained. It appears that Bahrain pursues this predicate offence without consideration to possible ML charges. Bahrain's National Committee for Combating Narcotic Drugs and Psychotropic Substances Crimes assesses that drug-trafficking within Bahrain involves small-sized drug traffickers and not larger criminal organisations that generate large amounts of cash.

189. Anti-corruption measures have caught the attention of authorities since 2010. These efforts resulted in an increase in the number of corruption cases, which peaked in 2015 (See Table 13 below). In regard to ML related to corruption, Bahrain conducted six ML investigations related to breach of trust, resulting in one conviction. However, these ML cases do not appear to relate to the public corruption cases in Table 13. Instead, the majority of the cases are related to misuse of corporate vehicles for embezzlement and laundering. Based on this information, the assessment team concludes that parallel ML investigations are not systematically initiated by the Anti-Corruption Directorate within the MOI.

Table 13. **Corruption Cases (2012 to 2017*)**

| Status | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 |
|---|---|---|---|---|---|---|
| **Investigation closed** | 6 | 16 | 29 | 57 | 12 | 30 |
| **Under Investigation by Anti-Corruption Directorate** | - | - | - | - | 2 | 2 |
| **Under investigation by PPO** | - | - | - | 3 | 8 | 15 |
| **Convictions** | 9 | 8 | 9 | 7 | 12 | 5 |
| Total | **15** | **24** | **38** | **67** | **34** | **52** |

*Note*: *Data from 2017 is from 1 January to 22 November 2017

190. Based on the above analysis, the assessment team concludes that ML investigation and prosecution is not entirely in line with the ML risks faced by Bahrain.

### *Types of ML cases pursued*

191. In recent years, Bahrain has pursued more complex ML investigations. Among the ML cases provided, both small and large-scale ML cases exist but it appears that not all of the major proceeds generating offences are systematically pursued for possible ML prosecution and that ML charges are not vigorously pursued when ML is committed in a complex manner. As discussed above, it is unclear if authorities are systematically "following the money" while conducting predicate offence investigations. Moreover, there are few investigations involving complex ML and ML involving proceeds generated from foreign predicate offences (See Table 14 below).

192. The below table illustrates the breakdown of the 43 ML investigation cases by type. It should be noted that some cases are classified into two types of ML offences as a result of the activity of the perpetrator.

Table 14**. ML investigations by type (cases)**

| ML Type | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | Total |
|---|---|---|---|---|---|---|---|
| **Self-laundering** | 2 | 2 | 6 | 3 | 10 | 5 | **28** |
| **3rd Party ML** | | 1 | 1 | | 3 | 1 | **6** |
| **Stand-alone ML** | | 1 | 1 | | 1 | 3 | **6** |
| **ML involving foreign predicate offence** | | 1 | | | 3 | 2 | **6** |

193. The most prevalent types of ML cases pursued in Bahrain relate to the self-laundering of domestically generated criminal profits. Given that Bahrain is a regional financial hub, there are concerns that the country is not adequately pursuing cases involving foreign proceeds of crime. For example, of the 43 ML investigations conducted between 2012 and 2017, only six ML cases involved foreign criminal proceeds and of these six, only one resulted in a conviction.

194. The statistics and case studies provided by Bahrain demonstrate that while there is some effort to prosecute ML, many of the cases identified were not

sophisticated or complex. For instance, six 3rd party ML investigations were pursued within the sample period (See Box 2 as an example), and one investigation resulting in conviction was obtained in relation to stand-alone ML involving a legal person (See Box 3).

**Box 2. Foreign Predicate Offence and 3rd Party ML (2017)**

Police notified the FID of a suspect bringing funds into Bahrain through Country X. Further investigation led to the source of funds resulting from tax evasion in Country X, and subsequently sent through Bahrain to Country Y through the remittance sector, and eventually sent to Country Z. This case is currently under judicial investigation by the PPO.

**Box 3. Stand-Alone ML (involving legal person) Conviction (2013)**

The FID initiated investigations based on suspicious remittances conducted by Remittance Company A, upon notification from the CBB. Remittance Company A was suspected of knowingly handling suspicious funds obtained from unknown sources. Upon investigation, it was determined that the funds entered Bahrain from Country X and disbursed to specific individuals, and subsequently retransferred from these individuals via Remittance Company A to Country Y. The underlying criminal activity which generated these proceeds was unknown. Investigations discovered that Remittance Company A was complicit in this ML scheme, in addition to 15 individuals.

The case was ruled in the Lower Criminal Court, and appealed in the Higher Appellate Court. Remittance Company A was fined BHD 200 000 (EUR 431 077); BHD 2 197 484 (EUR 4 741 454) were confiscated; 15 individuals were ordered to pay a fine (BHD 20 000 (EUR 43 115 each), and to serve imprisonment terms ranging from three months to five years.

195. In terms of the 34 individuals convicted of ML, the majority of the cases involved the purchase of tangible assets with illegal proceeds, and two cases involved the transfer of illegal funds through the remittance sector. While all of these cases included a foreign nexus (incoming or outgoing transfers of illicit proceeds), none of the convictions represent 3rd party ML cases, however one case included a stand-alone ML conviction, and one case involved a legal person.

### *Effectiveness, proportionality and dissuasiveness of sanctions*

196. A wide range of sanctions are imposed for ML offences for natural and legal persons. Sanctions of imprisonment up to seven years, judicial fine up to one million BHD, and confiscation of proceeds or their equivalent values are available. In practice, of the 34 individuals convicted of ML, the average sanction applied was four years, with the highest sentence applied being seven years' imprisonment and

included fines up to BHD 200 000 (EUR 431 077) (See Table 15). Penalties of predicate offences and ML are imposed independently. The perpetrator must serve the full sentence of both offences until they are eligible for release. However, there are exceptional cases such as parole or pardon, which may result in early release. Other than these situations, the perpetrator cannot be released even if the fine is paid, as the pecuniary sentence shall be executed separately from the penalty of imprisonment.

Table 15. **Penalties applied in ML convictions (2012-2016)**

| Year | Number of persons convicted of ML | Average Imprisonment Penalty (years) | Average Judicial Fine (BHD) |
|---|---|---|---|
| **2012** | 2 | 5 | 70 000 (EUR 150 994) |
| **2013** | 15 | 6.5 | 90 000 |
| **2014** | 9 | 3.5 | 104 00 |
| **2015** | - | - | - |
| **2016** | 8 | 3 | 102 000 |
| **2017** | - | - | - |

197. In regard to the proportionality of the ML sanctions applied, authorities provided the penalties of some major economic crimes. The penalties for the ML offence are higher than prostitution (five years' imprisonment), embezzlement (five years' imprisonment), and illegal fundraising (monetary fine), fraud (three years' imprisonment), but lower than bribery (up to ten years' imprisonment). In general, sanctions imposed in cases of ML convictions are generally effective, proportionate and dissuasive.

198. Of the 10 cases that resulted in ML convictions, one case included a conviction of a legal person. The legal person received a criminal fine of BHD 200 000 (EUR 431 077) (see Box. 3 above for details pertaining to this case), as well as an administrative penalty from the CBB. The assessment team concludes that this sanction applied to a legal person was proportionate, dissuasive, and effective.

### *Extent to which other criminal justice measures are applied where a ML conviction is not possible*

199. Non-conviction based confiscation is possible in Bahrain within the context of criminal proceedings, such as when the suspect dies, or absconds. Moreover, the PPO may order the confiscation of instrumentalities when the accused is unidentified or there is insufficient evidence to pursue a prosecution. Bahrain demonstrated that this has been pursued in absentia.

200. Bahrain provided a case study which demonstrates that settlements occur between the accused and victims. Specifically, in this case approximately EUR 607 million was returned to victims of fraud. While settlements are initiated by the affected parties, they are approved at the discretion of the authorities upon determination of the greatest benefit to the victim. Authorities noted that the objective pursued in such cases is to return the money to the victims by settling and avoiding a lengthy criminal process. This is also pursued where amounts are

considered too small to action the confiscation process. It is unclear how often settlements were initiated during the sample period.

201. Bahrain also states that it has been successful in dismantling organised groups conducting cash courier violations through seizures at the border, and by prohibiting certain individuals from entering the country. Insufficient information as provided to the assessment team to demonstrate how this prohibition works in practice, and why it is pursued in lieu of criminal charges.

### *Overall conclusions on IO.7*

202. **Bahrain is rated as having a moderate level of effectiveness for IO.7**.

## *Immediate Outcome 8 (Confiscation)*

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

203. Bahrain's legal framework for seizing, freezing and confiscating assets is adequate and has been used to some extent, for confiscating proceeds, instrumentalities and property of equivalent value in ML, associated predicate offences and TF.

204. There is no specific policy or guidance that requires LEAs to pursue confiscation as a policy objective, but based on the assessment team's discussions with authorities including judges and the cases reviewed, authorities seem to pursue the confiscation of assets as part of a proceeds-of-crime approach to combat crime, including ML. Whenever ML is suspected, the PPO and the FID work together to identify bank accounts and other types of assets, belonging not only to the suspect, but the family and relatives of the suspect (see search warrants by the FID below), with a view to identify opportunities for freezing and subsequent confiscation. The FID would also use the Egmont and Interpol channels to expand its enquiries, when needed.

Table 16. **Search warrants issued by the FID**

| Year | Search warrants | Seizure of assets* (number of instances) |
|---|---|---|
| **2012** | 85 | 11 |
| **2013** | 72 | 8 |
| **2014** | 94 | 13 |
| **2015** | 91 | 12 |
| **2016** | 113 | 19 |
| **2017** | 191 | 27 |
| Total | **646** | **90** |

*Note*: * Amounts were not provided.

205. It is not clear if the same approach is followed systematically and more generally across the law enforcement community as they pursue predicate offence

investigations, though the statistics provided do indicate that authorities pursue seizure and confiscation in some instances (Table 18 below).

206. The FID has the power to temporarily freeze identified assets, which has occurred in practice, and as shown in table 18 below, seizures have also been made pursuant to MLA requests.

207. Different types of property have been confiscated both in Bahrain and abroad, including: cash; bank accounts; cars; and real estate. Table 18 below illustrates the types and value of property confiscated during the assessment period. In at least three cases, the detected amount (estimated proceeds) was entirely recovered. The total amount of proceeds confiscated for all offences during 2012-2016 reaches over EUR 32 million, out of which according to the cases presented by Bahrain and as shown in the tables below, over EUR 12 million relates to ML.

208. Bahrain has procedures to manage seized but not confiscated assets. The PPO can appoint an appropriate third party to undertake the management of seized assets and given the nature of assets seized thus far (cars and real estate properties, apart from funds) and discussions with authorities, Bahrain has not faced any challenges in managing and preserving the value of assets.

209. Non-conviction based confiscation is available and has been used in absentia. Bahrain has no impediments to provide and receive MLA with regard to asset tracing, recovering and sharing. Requests have been made and fulfilled in this regard, as noted in IO.2.

Table 17. **Amounts confiscated and deposited in Bahrain's Treasury for all offences (including ML and TF)**

| Year of sentence | Confiscated amount in BHD | EUR Equivalent |
|---|---|---|
| 2012 | 1 764 930 | 3 815 126 |
| 2013 | 1 776 230 | 3 839 179 |
| 2014 | 631 731 | 1 361 107 |
| 2015 | 5 0096 57 | 10 827 974 |
| 2016 | 2 478 248 | 5 357 090 |
| 2017 | 3 469 840 | 7 498 897 |
| **Total for the period under review in EUR** | **32 699 375** | |

Table 18. **Amounts seized and confiscated and deposited in Bahrain's Treasury for ML**

| Years | Amounts involved as identified or estimated by authorities (in EUR) | Amounts seized (in EUR) | Actual confiscated amount (in EUR) | Predicate offence | Currencies involved | Number of cases |
|---|---|---|---|---|---|---|
| 2012 | 80 935 | 0 | 0 | Fraud & illegal fund rising | USD | 2 |
| | 10 623 028 | 0 | 0 | Breach of trust | USD | |
| 2013 | 4 948 713 | 4 948 713 | 4 948 713 | Cash courier violation | SAR | |
| 2014 | 282 500 | 0 | 0 | Prostitution | BHD | 3 |
| | 485 913 | 485 913 | Not available | Fraud | USD& BHD | |
| | 649 119 | 0 | As cash was not available, the authorities initiated a process to obtain real estate and others for an equivalent value; process is ongoing | Prostitution | BHD | |
| 2015 | 8 693 048 | 0 | Ongoing case (has been prosecuted now in the High Court) | Prostitution | BHD | 1 |
| 2016 | 87 306 and 3 cars | 87 306 and 3 cars | 87 306 and 3 cars | Prostitution | BHD | 3 |
| | 24 625 | | 24 625 | Illegal fund raising | BHD | |
| | 10 843 476 | 7 302 650 and 2 properties | 7 302 650 and 2 properties | Illegal fund raising | BHD | |
| 2017 | 31 652 142 | 1 6 41 363, plus shares of a company | Ongoing investigation | Fraud and illegal editing of data. | BHD | 5 |
| | 5 152 779 | 5 152 779 | Ongoing investigation | Fraud and banking operations without permit | USD | |
| | 10 784 | 4 499 | 0 | Tax evasion and illegal income sale of alcohol | SAR | |
| | 6 851 942 | 6 851 942 | Ongoing investigation | Fraud and illegal seizure of public property (related to a MLA request) | USD and CHF | |
| | 128 057 | 128 057 | Ongoing | Cash courier violations | SAR | |
| Total (in EUR) | | | 12 363 294 and other assets | | | |

210. Authorities provided evidence that instrumentalities of crime are systematically confiscated for all offences and especially for terrorism and TF, where

all elements used in the commission of the act would be confiscated, regardless of their low value as a deterrent to further acts. The FID discussed a case where it had noted that a TF incident had been conducted using welfare benefits and where authorities coordinated actions to stop these payments.

211. Instrumentalities of crimes (terrorism and TF) confiscated during 2012-2017 included mobile phones, laptops, computers, cars and a boat, GPS device, hard discs, cameras, explosives, fire arms, machinery items and other related material. Their total value amounted to EUR 6 575 involving 33 cases and 380 convicted individuals. This amount though small relative to the amounts confiscated for ML, is in line with what authorities explained often occurs with terrorism and TF, which is that terrorist acts are self-funded, using very little resources, such as those required to build a self-made explosive device.

212. Bahrain presented only one case where property of equivalent value was confiscated for ML. Bahrain has also confiscated assets from legal persons for ML.

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

213. Table 17 and 18 above, as well as cases presented in IO.2, show that authorities have confiscated the proceeds of both foreign and domestic predicates, such as fraud and embezzlement, and are pursuing proceeds located abroad. In addition, those figures do not include any amounts returned to victims. Authorities explained during onsite discussions, that that they prioritise returning funds to victims, particularly in cases of fraud and this has been done in several instances and is relevant to Bahrain considering investment fraud as one of its highest threats.

214. Bahrain presented one case to the assessment team which involved EUR 607 million returned to victims. Authorities noted that the objective pursued in such cases is to return the money to the victims by settling and avoiding a lengthy criminal process. This is also pursued where amounts are considered too small to action the confiscation process.

215. No other information was provided to the assessment team in terms of tax related recoveries, fines, or other types of data to show how criminals are being deprived from their assets and instrumentalities. This was however not given significant weighting by the assessment team, given Bahrain's context, where there is no income tax except for corporates, establishments, or companies directly associated to the oil and gas sector (according to Bahrain's draft NRA) and where the level of compliance was deemed high by authorities; no sanctions needed or imposed for non-compliance thus far.

216. Bahrain provided detected proceeds of crime in its draft NRA, of BHD 44 million (EUR 95 million), for ML, for the period under review, and while the amounts confiscated according to Table 17 for instance, resulted in just above EUR 12 million, the total amounts confiscated for all offences is EUR 32 million. This can however be considered modest in the context of Bahrain as a major business and regional financial centre.

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

217. Bahrain routinely seizes falsely and undeclared currency at its borders as noted in the table below, although confiscation numbers are not significant. The use of cash, not necessarily of illegal origin, is still prominent in the region and cash smuggling is one of Bahrain's key threats according to its draft NRA, with over EUR 400 million transported through the borders (incoming and outgoing) in cash of different denominations (Omani Rial, Iranian Rial, Kuwaiti Dinar, among others), apart from gold and pearls. BNIs have not been seized or confiscated.

218. Bahrain's Customs is well aware of the illegal movement of cash, is well resourced and is active in detecting cash of illegal origin. Customs was initially in the Ministry of Finance and then moved in 2008 to the MOI, which includes other key authorities for Bahrain's AML/CFT regime, such as the FID, to further strengthen its capacity and resources. It fully benefits from access to the Najem system and there is a strong co-ordination and co-operation between FID, Customs and Police.

219. The illegal carriage of assets through borders is criminalised by law, and a designated section within the FID is delegated to police this particular area of risk. Disclosures and any cash seizure are communicated by Customs directly to the FID, and urgent communication can and does occur even via telephone, radio or in person seamlessly. Authorities narrated a number of instances when exchanges between Customs and FID took place in such cases. For instance, to assist with background checks of persons or shipments.

220. Bahrain significantly amended its legislation (Decree No.12 2017, November 2017) while the team was on site, to further strengthen its disclosure system for "funds" entering or exiting Bahrain by natural and legal persons. The term "funds" cross-references the definition of property in Decree No.4 (2001), which captures currency and BNIs and it includes funds imported or exported through shipments or parcels transported by courier services in favour of natural or legal persons or any other organisations.

221. As noted in R.32, regulatory changes explicitly granted custom authorities the power to require a disclosure of funds being carried across the border. In case of false or non-disclosure of funds, customs officials were also empowered to demand additional information about the source of funds, their owners and other parties related thereto, reasons of their entry or exit and are also able to seize the funds, upon suspicion of ML/TF, or when not being convinced with the reasons or explanation provided for carrying the funds (Art. 4 and 5 of said Decree). Authorities agreed that these legislative changes will significantly improve Bahrain's performance with regard to seizure and confiscation going forward as they reverse the burden of the proof.

Table 19. **Total Number of Instances of Non-Declared currencies seized/returned/confiscated on borders**

| | Port | 2012 | | 2013 | | 2014 | | 2015 | | 2016 | | 2017 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | In | out | In | out | In | out | In | out | In | out | in | out |
| Number of instances / reports | King Fahad Causeway | 12 | 0 | 8 | 6 | 10 | 0 | 3 | 2 | 3 | 0 | 16 | 2 |
| | Bahrain Int. Airport | 0 | 13 | 0 | 8 | 4 | 9 | 1 | 5 | 1 | 5 | 2 | 9 |
| | Air Cargo | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 2 | 0 | 0 | 1 | 2 |
| | **Total** | **25** | | **22** | | **23** | | **14** | | **9** | | **32** | |
| Value in Euro (Approximately) and number of reports | Returned | 1 653 165 (22) | | 1 732 718 (19) | | 1 338 847 (21) | | 560 946 (11) | | 315 003 (8) | | 1 971 001 (26) | |
| | Still Seized | 0 | | 0 | | 0 | | 0 | | 129 336 (1) | | 672 698 (6) | |
| | Confiscated | 77 034 (3) | | 103 004 (3) | | 118 545 (2) | | 123 240 (3) | | Nil | | Nil | |
| Main currencies involved | | BHD, SAR, USD, IRR, INR | | BHD, SAR, USD, IRR | | SAR, AED, BHD, USD, EUR, OMR, KWD, QAR, CHF, DKK, CAD | | SAR, AED, IRR, USD | | SAR, USD, BHD, | | SAR, USD, BHD, AED, EUR | |

222. Co-operation between the FID and Customs has also been key in achieving results in the area. Typologies of cash smugglers relating to cash courier cases were disseminated by the FID in the form of intelligence reports. That aided in an increase in the seizures at the borders (See case referred to in IO.7, which ultimately resulted in dismantling a group of smugglers that used Bahrain as a hub to transfer money that was used to launder tax evasion related funds).

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

223. Bahrain identified the smuggling of cash and its equivalents as one of the highest threats to Bahrain in its draft NRA and cash courier violations as one of the major proceeds of crime generating offences. Attention placed on Customs, revisions to its legislation and the results noted above seem to be in line therefore, with the ML/TF risks and national policies and priorities.

224. The possibility of further regulating the use of cash may be an issue that authorities could further explore as noted in other sections of this report.

225. Bahrain has also taken actions to recover proceeds of crime for other significant threats such as fraud (particularly investment fraud) and prostitution and immorality although in the case of fraud, it has also pursued the policy of

returning the money to victims rather than confiscation as explained under section 3.4.2 above.

### *Overall conclusions on IO.8*

226. **Bahrain is rated as having a moderate level of effectiveness for IO.8.**

3

# CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION



## Key Findings and Recommended Actions

### Key Findings

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

**Bahrain achieved a moderate level of effectiveness for IO.9.**

1. As noted in R.5, Bahrain's terrorism offence includes an exemption which is cross-referenced in its TF offence, and is inconsistent with the TF Convention. This exemption significantly impacts Bahrain's compliance at the technical level. This exemption, however, has no impact on effectiveness as it has not been used as a defence in court or by authorities to limit their identification or investigation of TF.
2. TF activities are identified and investigated by LEAs, though TF is mostly identified as a result of terrorism investigations; however, one case study was provided where a TF investigation was initiated through a cash courier violation. As a result, the assessment team has concerns that Bahrain is not proactively pursing TF investigations and prosecutions as a preventive measure to identify and financially disrupt terrorists.
3. TF investigations are referred to the FID by other relevant authorities within the MOI and the NSA as a result of terrorism investigations. Given the strong domestic co-ordination in Bahrain, information and intelligence is rapidly exchanged in all cases.
4. The FID has immediate access to a wide range of information and intelligence and has a comprehensive set of investigative powers to investigate TF.
5. Bahrain has secured 33 terrorism conviction cases, which include 22 cases resulting in TF convictions. Each of these cases involves multiple defendants. The total number of individuals involved in the 22 TF conviction cases is 58. TF penalties are effective, proportionate and dissuasive.
6. Bahrain uses disruption tactics in regard to TF. Bahrain has invalidated passports and revoked the citizenships of 26 FTFs; used international outreach to obtain the detention of Bahraini citizens at risk of facilitating or engaging in TF; and established a rehabilitation program for persons who have engaged, or are at risk of engaging in, terrorism and its facilitation.

4

*Preventing terrorists from raising, moving and using funds (Immediate Outcome 10) and Proliferation Financing (Immediate Outcome 11)*

**Bahrain achieved a moderate level of effectiveness for IO.10 and IO.11.**

7. As indicated in R.6 and R.7, TFS (both TF and PF) obligations do not explicitly extend to all natural and legal persons in Bahrain. Instead, Bahrain states that existing offences prohibit persons from making funds or other assets and economic resources to UN-designated persons and entities but there is no explicit TFS obligation for all natural and legal persons.
8. Financial institutions in Bahrain immediately implement the relevant UNSCRs related to TFS, as they are legally obliged to comply with UN Chapter VII designations without the need for additional orders from Bahraini authorities. In practice, the CBB separately disseminates legally enforceable directives that require financial institutions to report whether assets were frozen pursuant to changes to the relevant UN lists. However, in some cases, it can take almost two months before financial institutions are notified of such changes by the CBB.
9. DNFBPs supervised by MOICT [real estate agents which are structured as companies (until September 2017 at which point, the real estate sector was transferred to a separate authority, RERA under SLRB), DPMS and accountants and auditors] have a legal obligation to implement TFS (both TF and PF TFS). However, unlike financial institutions, this obligation starts at the time of notification from MOICT of changes to the UN lists. In practice, changes to the relevant lists were not communicated without delay by MOICT; however, prior to the end of the onsite visit, MOICT instituted a policy where communication was automised though the use of RSS feeds.
10. Lawyers, notaries, and real-estate brokers do not receive notification of changes from their respective supervisors.
11. The CBB and MOICT verify their respective reporting entities' compliance with all UNSCR obligations (both TF and PF TFS) during onsite and offsite inspections. Understanding and implementation is varied and limited, particularly outside the financial sector. The assessment team took note of a case where a financial institution repeatedly permitted access to an account by a UN 1267 listed individual. This case demonstrates that supervision and guidance related to TFS is not sufficiently proactive, especially given the persistence of the violation that occurred in this case.
12. Bahrain has made a number of domestic designations pursuant UNSCR 1373, which are communicated to the general public (via gazetting, and in newspapers) and to financial institutions, and MOICT registered entities. Bahrain states that these domestic designations have resulted in assets frozen by financial institutions but only provided two examples of assets frozen with limited success. This is inconsistent with Bahrain's TF risk profile and its number of TF convictions.
13. Bahrain identified a subset of high risk NPOs for potential terrorism abuse. Yet, there are a number of restrictive obligations placed on all NPOs

operating in Bahrain, regardless of their identified risk profile. While these measures may be effective at mitigating TF abuse of the NPO sector, they are not applied on a risk-basis and may unduly or inadvertently restrict NPO's ability to access resources, including financial resources, to carry out their legitimate activities. Moreover, outreach to NPOs is not conducted on a risk-basis.

14. In regard to PF, Bahrain has no trading relations with Iran or the DPRK; however given the geographical proximity to Iran, PF exposure risks do exist. Detailed guidance or outreach on PF has not been issued by the relevant supervisors to help mitigate this risk. Bahrain's customs officials have an advanced understanding of the risks of proliferation and PF, including diversion and sanctions evasion. This understanding has resulted in the successful interdiction of goods manufactured by DPRK, which were identified by the UN as a revenue generating activity for the DPRK. Nevertheless, co-operation between relevant authorities on PF could be improved to further prevent possible future instances of sanction evasions.
15. Bahrain also provided a significant case study that demonstrated that the competent authorities are monitoring and ensuring compliance with PF-related TFS, including the application of the CBB's most severe administrative penalties, as well as the pursuit of criminal charges.

### *Recommended Actions*

#### *Immediate Outcome 9*

1. Bahrain should urgently amend its terrorism offence to remove the exemption for "peoples struggle, including armed struggle against foreign occupation, aggression, colonialism, and hegemony, aimed at liberation and self-determination in accordance with the principles of international law".
2. Bahrain should urgently finalise its TF risk in order to investigate and prosecute TF activity consistent with its TF risk profile.
3. Consistent with its risk profile, Bahrain should seek to identify and investigate TF as a distinct criminal activity instead of investigating TF as part of terrorism cases, as they do currently.
4. Bahrain should continue to prioritise measures to disrupt TF activities where a TF conviction is not possible or cannot be secured.

#### *Immediate Outcomes 10 and 11*

5. Bahrain should implement explicit measures to ensure that neither their nationals, nor anyone within their territory (regardless of nationality), makes any funds, financial assets or economic resources available for the benefit of a UN listed person or entity, whether directly or indirectly. Currently, this prohibition only extends to financial institutions and some DNFBPs.
6. Bahrain should more clearly extend the TFS obligations to all DNFBPs, and the MOJ and RERA should notify its registered entities of changes to the

relevant UN lists.

7. The CBB should clarify the legal obligation of financial institutions to implement TFS without delay by defining "without delay" consistent with the FATF definition. This implementation obligation should be distinct in law from the separate requirement to respond to notices from the CBB to report whether assets have been frozen.
8. The CBB should take steps to improve its supervisory activities as they relate to TFS, including providing guidance and conducting outreach on TFS obligations. The CBB should issue dissuasive sanctions in instances of TFS violations, and should consider publishing future penalties regarding TFS violations. Similarly, the MOICT, MOJ, and RERA should conduct outreach and provide guidance on TF and PF sanction obligations to its supervised entities.
9. The MLSD should implement mitigation measures that are commensurate to the risks identified through its review of the NPO sector and understanding of the TF risks in the sector. The MLSD should conduct targeted outreach and provide guidance on how to identify, prevent and report TF, with a focus on those NPOs assessed as high risk for potential TF abuse.
10. The CBB, with the assistance from Customs, should provide guidance to financial institutions regarding PF typologies and threats.

227. 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)*

### *Prosecution/conviction of TF consistent with the country's risk-profile*

228. As noted in R.5, Bahrain's TF offence includes an exemption for "peoples struggle, including armed struggle against foreign occupation, aggression, colonialism, and hegemony, aimed at liberation and self-determination in accordance with the principles of international law." This exemption, however, has not yet had a discernible impact on effectiveness as it has not been used as a defence in court or by authorities to limit their investigations into terrorism and TF. When asked why the exemption had not been used to defend individuals accused of terrorism and TF, attorneys asked by the national bar association to respond to questions from the assessment team said they were not familiar with the exemption.

229. The authorities have an evolving understanding of TF threats in Bahrain. According to the authorities, the risk of terrorism and TF is high. Though the understanding of risk is still being finalised, Bahrain identifies high risk TF areas as: cash smuggling via land and sea (i.e. foreign funding); NPOs; fundraising; and, FTFs (see Table 20).

Table 20. **TF Risks in Bahrain from draft NRA**

| Risk rating | Domestic | Foreign |
|---|---|---|
| **High** | Cash (includes 'Drop Box Method') | Cash smuggling across land borders (includes religious expeditions) |
| | Religious Contributions or donations | Cash smuggling via sea |
| | | Training camps |
| **Medium** | NPOs | Transfer and laundering of funds through the financial system |
| | Fundraising | |

230. Based on Table 20, the majority of TF risks identified by authorities relate to the physical transfer of cash. The authorities also stated that the majority of TF cases investigated and prosecuted involved cash smuggling from individuals with connections to Iran, Iraq, and Hezbollah in Lebanon. Bahrain identified the abuse of the financial system as a medium risk in regard to foreign funding (see IO.1).

231. As noted in Chapter 1, terrorism is a significant threat to Bahrain, particularly from armed militants targeting Bahraini security forces. During 2012-17, Bahrain experienced 99 terrorist incidents, with recent incidents committed by the local terrorist organisation, the Al Mukhtar Brigade, which authorities state receives support (including financial) from Iran and Iraq. According to authorities, local terrorist groups sympathise and identify with the ideology of Hezbollah, and Asa ib Ahl al-Haq in Iraq. Moreover, TF in Bahrain is directly linked by the authorities to Hezbollah and the Iranian Revolutionary Guards Corps. Domestic terrorist attacks often involve homemade explosive devices, and are, therefore, low-cost and do not require substantial financing.

232. The decision to prosecute TF or terrorism-related offences rests with the PPO, which works closely with investigators from the MOI (including the FID) and the NSA. More than half of all terrorism prosecutions in Bahrain include a TF component. The authorities stated that TF charges are not pursued in terrorism cases where the death penalty is sought by the PPO (maximum penalty for terrorism offences is the death penalty).

233. During the sample period, Bahrain secured terrorism convictions in 33 cases. Of these 33 cases, 22 included convictions for TF (see Table 21). Five cases were still before the courts at the end of the onsite period. It should be noted that each case involves multiple individuals, with two cases from 2013 involving approximately 50 individuals. The total number of individuals convicted of TF during the sample period is 58. Only one of the cases below represents a TF case independent of other terrorism related charges. Instead, the majority of TF charges were included in cases where other terrorism charges were filed (e.g. belonging to a terrorist group, and/or committing a terrorist activity). Of these cases where terrorism charges were pursued, six individuals were convicted of TF only.

Table 21. **TF and terrorism investigations/convictions (2012-2017*)**

| | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | Total |
|---|---|---|---|---|---|---|---|
| **TF Investigations (cases)** | 1 | 9 | 5 | 5 | 1 | 1 | **22** |
| **TF Convictions** | 1 | 9 | 5 | 4 | 1 | 1 | **21** |
| **TF Convictions (individuals)** | 4 | 34 | 8 | 10 | 1 | 1 | **58** |
| **Terrorism Investigations (cases)** | 4 | 12 | 8 | 7 | 6 | 1 | **38** |
| **Terrorism Convictions (cases)** | 4 | 11 | 7 | 4 | 6 | 1 | **33** |
| **Terrorism Convictions (individuals)** | 22 | 160 | 57 | 90 | 50 | 1 | **380** |

*Note*: *Data from 2017 is from 1 January to 22 November 2017

234. The TF investigations and convictions occurring during the sample period relate to the provision of physical cash to: purchase weapons, ammunition, and other equipment to manufacture explosive devices for use in domestic terrorist attacks; finance travel abroad to receive training; provide living expenses abroad and in Bahrain; illegal fundraising; and the receipt and transfer of funds to a terrorist organisation. However, it was apparent in the examples provided to the assessment team that while Bahrain is investigating and prosecuting TF cases, the TF cases were part of terrorism investigations (i.e., TF cases were not independent from terrorism cases). Further, Bahrain does not routinely identify and investigate TF cases that are not part of a terrorism investigation despite indications of TF activity. Nevertheless, the assessment team has concerns that Bahrain is not adequately investigating and prosecuting TF cases independent from the prosecution of other terrorist-related offences. The assessment team is of the view that more foreign TF cases could be initiated as there appears to be some domestic support to foreign terrorist organisations, as evidenced by the number of FTFs leaving Bahrain.

235. An example of a TF case is outlined below (See Box.4). In this case, six individuals were convicted of TF (in addition to the offence of assisting a terrorist organisation).

**Box 4. TF Case involving collection, movement, and distribution of funds (2013)**

In 2013, an LEA received intelligence related to a foreign terrorist organisation training several members on the use of weapons and explosives to conduct terrorist activities in Bahrain. The suspects in Bahrain were collecting, moving, and using funds obtained by the foreign terrorist organisation to organise domestic terrorist acts.

The authorities arrested all individuals involved in the smuggling process of the funds. The facilitator, as well as individuals involved in collecting, moving, and using such funds was also apprehended. The perpetrators also included suspects that belonged to the foreign terrorist organisation.

Four individuals were convicted of treason (attempt to assist a foreign country to overthrow the government), and received a sentence of life imprisonment. Six individuals were convicted for assisting terrorist organisations in training, financing and facilitating the funding with intent to support the ideology of a terrorist organisation. These individuals were sentenced to 15 years' imprisonment.

236. As noted above, during the sample period, Bahrain prosecuted one TF case independent of other terrorism-related charges (see Box 5. below). This case demonstrates that LEAs have the capacity to identify TF cases in the absence of a specific terrorist activity, or a completed terrorist attack. As noted above, the assessment team has concerns that only one such case exists during the sample period, particularly given the TF risks present in Bahrain. Further, the majority of TF cases occurring within the sample period were reactive rather than proactive, and only one case was provided that demonstrated that TF investigations and prosecutions were pursued as a preventive measure to identify and financially disrupt a terrorist network.

**Box 5. Standalone TF Case (2015)**

In 2015, intelligence from the FID indicated that Suspect H was involved in financing individuals related to terrorist acts. The FID with LEAs started an initial investigation to determine the connection of Suspect H and the terrorists. The FID analysed bank statements, front companies, and drafted intelligence reports in co-operation with other LEAs. This resulted in further intelligence, which identified the sources of funds.

Further intelligence reports by LEAs also helped the FID to relate Suspect H to terrorists. The operational analysis of the FID led to clear evidence that proved that Suspect H intentionally facilitated financing individuals arrested for terrorist acts or who have committed terrorist acts. Specifically, the FID's analysis demonstrated that BH 14 000 was deposited to the suspect's bank account which was then dispersed to individuals related to terrorist acts.

On 29 March 2017, the defendant was convicted of TF and sentenced to 10 years' imprisonment and received a BHD 100 000 penalty. Furthermore, the defendant was charged for collecting funds without a license from the competent authorities with the sole intent of financing terrorists.

### *TF identification and investigation*

237. TF investigations are primarily identified as a result of terrorism investigations, but a case exists where TF investigations were initiated through information obtained by Customs officials at the border (i.e. non-disclosures of currency). Terrorism investigations are led by the MOI, with input from the NSA. The General Directorate for Criminal Investigations (CID), within the MOI, is responsible for leading the investigation of terrorism activities. The NSA, Bahrain's intelligence agency, provides intelligence to the MOI, including the FID, to support its terrorism and TF investigations. The CID also works closely with the FID, and builds task forces when conducting terrorism investigations, which could include the FID, NSA, PPO, JCTC, and Customs. When an investigation includes a financial element, the FID is responsible for leading the TF component of the investigation. The FID closely coordinates with CBB where bank statements and other related information is required for investigation. Communication and co-ordination between relevant law enforcement agencies (including FID and PPO) and CBB is very well established. In the case of investigations that include international investigations, the PPO sends MLA requests to collect additional information or to seize any financial or non-financial assets domestically or internationally.

238. As a law enforcement FIU, the FID has direct access to a wide range of financial intelligence and other systems, and possesses investigative powers, including surveillance and seizure powers (see IO.6), which it demonstrated that it actively uses in practice. LEAs also have additional authority when investigating

suspicion of TF. Specifically, during the course of a TF (or terrorism) investigation the FID, without prior approval of the PPO, has the authority to:

- issue a travel ban;
- freeze funds, bank accounts, and other assets;
- imprison a suspect up to 28 days; and
- conduct wiretapping.

239. Relevant LEAs have the appropriate resources and expertise to identify and prosecute TF. Specifically, the FID and other relevant LEAs responsible for assisting in the investigation of TF, have participated in a number of domestic and international training courses, including courses specific to identifying Hezbollah financing, and investigating and prosecuting terrorism more generally. Further, the FID has nine staff dedicated to TF, the PPO has a specialised unit dedicated to counterterrorism cases (including TF), which is staffed with 17 individuals (including nine prosecutors and eight support staff), and CID has 105 staff dedicated to counterterrorism.

240. As noted above, all of the TF conviction cases secured during the sample period formed part of a larger case, where all but one case involved other terrorism-related charges. The authorities stated that all possible financial aspects are considered in each terrorism investigation. Based on the frequency of terrorism cases involving charges for TF (see Table 21), it is clear that this is indeed the practice.

241. Most terrorism cases and related TF activity are identified through intelligence received from the NSA (which includes foreign intelligence), or from the CID following a terrorist attack. This information is shared with the FID in order to initiate a parallel TF investigation. Between 2012 and 2016, the FID received a total of 225 reports from LEAs for TF investigation (see Table 22 below).

Table 22. **Cases referred to the FID for TF investigation (2012-2017*)**

| Years | Cases referred to the FID from LEAs |
|---|---|
| 2012 | 7 |
| 2013 | 21 |
| 2014 | 37 |
| 2015 | 53 |
| 2016 | 46 |
| 2017 | **61** |
| Total | **225** |

*Note*: *Data from 2017 is from 1 January to 22 November 2017.

242. As noted in IO.6, the FID also receives TF-related STRs for analysis. These STRs could be flagged by reporting entities as comprising TF suspicions, or identified by the FID as having possible TF linkages based on internal TF indicators. These indicators include whether there is any correlation to other STRs categorised as TF, or any existing enquiries by LEAs. Between 2012 and 2017, the FID received 29 TF-related STRs from reporting entities (see Table 23).

Table 23. **TF-related STRs sent to the FID (2012-2017*)**

| Year | TF STRs |
|---|---|
| 2012 | 3 |
| 2013 | 5 |
| 2014 | 8 |
| 2015 | 7 |
| 2016 | 4 |
| 2017 | 2 |
| Total | **29** |

*Note*: *Data from 2017 is from 1 January to 22 November 2017

243. By comparing Table 22 and Table 23, it is evident that the majority of the TF cases are initiated as a result of information referred to the FID from other LEAs, primarily the CID. Indeed, the authorities stated that no STRs have initiated TF prosecutions. Instead, STR information is analysed by the FID and used to supplement existing TF cases, or corroborate intelligence. The FID states that it considers all TF STRs in the course of each TF and terrorism investigation.

### *TF investigation integrated with—and supportive of—national strategies*

244. In terms of domestic co-ordination on TF, Bahrain has a Joint Counter Terrorism Centre which brings together the FID, Bahrain's Interpol liaison unit and the NSA, among other security related agencies, which meets regularly to exchange information on potential terrorists and TF information. Exchanges within this joint group led to the identification of 26 Bahraini FTFs.

245. Bahrain has a counterterrorism strategy, which includes components of a CFT strategy. Moreover, the National Policy Committee sets and coordinates all AML/CFT policy and counterterrorism efforts (see IO.1). The Committee develops 3-5 year AML/CFT strategies, which may be updated as needed. During the onsite visit, the authorities stated that the current AML/CFT strategy was developed in 2012, but the strategy was not provided to the assessment team. Bahrain stated that this strategy included addressing the deficiencies identified in Bahrain's last mutual evaluation. Bahraini authorities also said that there are multiple action plans, but the assessment team was not provided with these documents. Bahrain further stated that its CT policy and strategy are adapted through consultation with other GCC member states. Therefore any policy or strategy that is adopted by the GCC is also implemented in Bahrain. However, Bahrain did not provide the assessment team with any GCC-related CT policies or strategies or discussed its core elements with the assessment team, in order for the assessment team to determine whether its CFT activities are integrated with, or supportive of, these strategies.

246. In its draft NRA, Bahrain states that Hezbollah, Asa ib Ahl al-Haq in Iraq, and the Iranian Revolutionary Guards Corps represent the most significant TF risk. Bahrain also notes that the existence of other terrorist groups in the region, such as Al Qaida and ISIL, pose a significant TF threat. However, the as noted in IO.1, the assessment of risk posed by Al Qaeda, ISIL, and FTFs, could be further elaborated upon.

247. In regard to countering ISIL-related activities, Bahrain is part of the international Global Coalition to Counter Daesh "ISIL" and joined the Saudi-led Islamic counterterrorism alliance and committed partnership with the recent Terrorist Financing Targeting Centre based in Riyadh.

### *Effectiveness, proportionality and dissuasiveness of sanctions*

248. According to law, TF is punishable by a term of imprisonment not less than 10 years and up to life imprisonment. In addition to a term of imprisonment, fines no less that BHD 100 000 (EUR 215 588) are available.

249. As noted above, during the sample period, there were 22 terrorism cases which included TF convictions. The total number of individuals convicted of TF during the sample period is 58. 52 of these individuals were also convicted of other terrorism-related offences, where the sentences are much higher. Therefore, the higher penalties were often applied (predominately life imprisonment and revocation of citizenship). As noted above, six of the 58 individuals were only convicted of TF. The penalties applied in these cases ranged from 10-15 years' imprisonment and a fine of BHD 100 000 (EUR 215 588). Detailed information on the sanctions applied during the sample period is outlined below (see Table 24). It should be noted that in the cases below, multiple individuals were also convicted of standalone terrorism activities and are therefore omitted.

Table 24. **Sanctions applied in TF cases (2012-2017*)**

| Number of individuals | Sanctions applied in cases which TF charges and terrorism charges | Sanctions applied for only TF charge |
|---|---|---|
| 2012 | | |
| **4** | 4 persons received BHD 100 000 (EUR 215 588) fine and ten years' imprisonment | |
| 2013 | | |
| **2** | 1 person received 15 years' imprisonment and a BHD 200 000 (EUR 431 077) penalty<br>1 person received 10 years' imprisonment and a BHD 100 000 (EUR 215 588) penalty | |
| **8** | 5 persons received 15 years' imprisonment<br>3 persons received 10 years' imprisonment | |
| **1** | Life imprisonment | |
| **1** | Life imprisonment | |
| **2** | All received life imprisonment | |
| **7** | 4 persons received life imprisonment | 3 persons received 15 years' imprisonment |
| **4** | All received life imprisonment | |
| **7** | 3 persons received life imprisonment<br>1 person received 15 years' imprisonment<br>3 persons received 10 years' imprisonment and a fine of BHD 500 (EUR 1077) and BHD 10 000 (EUR 21 550) | |

| | | | |
|---|---|---|---|
| | **2** | 1 received life imprisonment<br>1 received the abolition of nationality | |
| 2014 | | | |
| | **1** | 15 years' imprisonment and fine of BHD 200 000 (EUR 431 077), and the abolition of nationality | |
| | **1** | Life imprisonment | |
| | **2** | Both received 15 years' imprisonment and a fine of BHD 20 000 (EUR 43 115) | |
| | **2** | Both received 15 years' imprisonment and a fine of BHD 100 000 (EUR 215 588), and the abolition of nationality | |
| | **2** | Both received life imprisonment and a BHD 100 000 (EUR 215 588) penalty | |
| 2015 | | | |
| | **3** | 1 person received the death penalty.<br>2 persons received life imprisonment, a fine of BHD 200 000 (EUR 431 077), and the abolition of nationality | |
| | **2** | Both received life imprisonment, a fine of BHD 200 000 (EUR 431 077), and the abolition of nationality | |
| | **3** | | 3 persons received 10 years' imprisonment and a fine of BHD 100 000 (EUR 215 588) |
| | **2** | Both received life imprisonment and the abolition of nationality | |
| 2016 | | | |
| | **1** | 1 person received 10 years' imprisonment, a fine of BHD 100 000 (EUR 215 588), and the abolition of nationality. | |
| 2017 | | | |
| | **2** | 1 person received 10 years' imprisonment<br>1 person received 7 years' imprisonment and a fine of BHD 100 000 (EUR 215 588), and the abolition of nationality | |

*Note*: *Data for 2017 is from 1 January to 22 November 2017

250. Based on the above table, it is clear that the sanctions applied in practice are dissuasive and effective. However, as noted above, the majority of the penalties represent cumulative penalties for TF and other terrorism offences, with the latter resulting in more severe sanctions. As indicated in the table, the sanctions range from 10 years' imprisonment to the death penalty. Monetary fines are also applied and range from BHD 500 (EUR 1077) to BHD 200 000 (EUR 431 077). Bahrain indicated that the BHD 500 (EUR 1077) fine was sought for an individual who also engaged in riot activities. As indicated above, Bahrain also has the authority to

revoke the citizenship of its nationals; however, this penalty is only available for serious terrorism offences, and not TF.

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

251. Bahrain has taken a number of alternative measures to prevent and disrupt TF activities where it was not practicable to secure a conviction. Specifically, in regard to FTFs, authorities have revoked the passports and nationalities of 26 Bahraini FTFs and included their names on the Interpol watch list. Any assets belonging to these FTFs have been frozen. Persons who were pre-empted from traveling through outreach and rehabilitation are closely monitored by security forces. Bahrain also reaches out to countries when it is aware that its citizens are there and at risk of conducting terrorism, or facilitating or financing terrorism. Bahrain has also taken actions to stop social welfare payments of those suspected of TF, including FTFs.

252. Moreover, Bahrain participates in regular meetings with Saudi Arabia to discuss regional TF matters and to exchange the names and entities associated with terrorist organisations such as Hezbollah, thereby prohibiting these individuals from entering the country.

253. Bahrain also has a rehabilitation program to prevent high risk persons from developing into terrorists or terrorist sympathisers or financiers. The program also includes preventive measures targeted to all citizens to educate them and protect them from extremist ideologies. A total of 23 individuals have undergone rehabilitation during the sample period.

254. In cases where prosecution for TF offences are not practical, suspected persons are also added to domestic watch-lists. These lists also result in asset freezing measures via circulars issued by the CBB and MOICT.

### *Overall conclusions on IO.9*

255. **Bahrain is rated as having a moderate level of effectiveness for IO.9.**

## *Immediate Outcome 10 (TF preventive measures and financial sanctions)*

### *Implementation of targeted financial sanctions for TF without delay*

UNSCRs 1267/1988 (and successor resolutions)

256. As noted under R.6, pursuant to the CBB's FC Modules, all financial institutions are required to freeze, without delay, the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the UN Security Council under Chapter VII of the UN Charter. Therefore, once an entity is added or removed from the 1267 and 1988 lists, financial institutions' obligations take immediate effect and no additional transpositions are required to give legal effect to a designation.

257. Registered entities of the MOICT [real estate agents which are structured as companies (until September 2017 at which point, real estate sector was transferred to a separate authority, RERA under SLRB), DPMS, accountants and auditors] also

have a legal obligation to follow guidance, issued by the MOICT in 2014, to implement UN TFS regarding the UN 1267 and 1988 lists upon notification by the MOICT. Changes to the relevant lists were not communicated without delay by MOICT; however, prior to the end of the onsite visit, MOICT instituted a policy where communication was automised though the use of RSS feeds. Lawyers, notaries (supervised by MOJ), and real-estate agents/brokers (supervised by the RERA since September 2017) do not have legal requirements in relation to searching and freezing obligations to implement TFS, nor do they receive notifications of changes to the UN lists from their respective supervisors.

258. All changes to the Consolidated UN Sanctions List are notified to Bahrain through its Permanent Mission to the UN in New York and directly to the MoFA in Manama, which circulates the changes immediately to the members of the National Committee on the Implementation of UNSCRs (hereinafter referred to as the National Committee).

259. While financial institutions are automatically required to implement the relevant UNSCRs, separately the CBB issues legally enforceable directives that require financial institutions to report whether they have frozen assets pursuant to changes to the UN lists. Bahrain states that it provides these directives to establish a requirement to report nil or positive responses, and to open the lines of communication between institutions and the CBB in regard to TFS implementation. These directives are often sent to financial institutions well after the changes have been made by the relevant UN Committee, in some cases one month after a designation by the UN. Nevertheless, the freezing obligation (and available penalties for non-compliance) takes immediate effect prior to the issuance of these directives. These directives refer to the legal requirements established in the FC Module to search, freeze, and report to the CBB any assets held by designated entities. These Directives also establish a requirement to report nil responses within two weeks after receipt of the directive. In practice, financial institutions respond to these directives by providing nil responses, which indicates that they are screening their databases upon receipt of these CBB directives.

260. In 2012, Bahrain established the aforementioned National Committee to coordinate sanctions implementation and other UN obligations. The composition of this National Committee is adequate for sanctions implementation as all relevant authorities implicated in the operationalisation of TFS (both TF and PF) are included (including the CBB and MOICT). The National Committee meets four times per year (and when necessary) to discuss operational and policy issues related to UNSCRs, including the communication of UN sanction lists to reporting entities.

261. The Committee is also responsible for identifying possible entities for designation to the relevant UN Committees. The Committee has written internal guidelines related to recommending listings/delistings to the UN, and the criteria for listing. To date, Bahrain has not recommended any entities to be added to the UN lists pursuant to UNSCR 1267 and 1988 (and successor resolutions). This Committee also considers requests for the potential removal from the relevant UN lists. During the review period, the Committee supported the delisting requests of two Bahraini nationals. These individuals were removed from the list pursuant to UNSCR 1267 in 2015 and 2017, respectively. There is currently one Bahraini national listed on the UN 1267 list.

262. Since 9 October 2015, the penalty for non-compliance with CBB laws or directives is a maximum of 100 000 (EUR 431 077), up from BHD 20 000 (EUR 43 115). These penalties can be multiplied by the number of violations, which means that the penalties imposed could be much higher in cases of multiple violations. In addition to monetary penalties, the CBB has the power to impose conditions, including appointing an observer member on the board of directors or placing the licensee under administration (see c.27.4). In practice, TFS violations (related to TF) have only resulted in a penalty of BHD 20 000 (EUR 43 115) (see Box 6 below). Given that this violation was reoccurring and spanned nearly five years, the assessment team concluded that the sanctions applied in this particular case were not proportionate or effective. Moreover, while the CBB has the authority to publish penalties imposed for noncompliance, in practice, it has not chosen to do so. Nevertheless, licensees are required to include the details of penalties in their annual reports, which are public documents.

263. Registered entities of the MOICT [real estate agents which are structured as companies (until September 2017 at which point, real estate sector was transferred to a separate authority, RERA under SLRB), DPMS, accountants and auditors] also receive email notifications from the MOICT upon any changes to the UN lists, but are not required to report positive matches or nil responses. These email notifications are legally enforceable as they are issued pursuant to enforceable guidance on TFS issued by MOICT in 2014. Prior to the onsite visit, the MOICT provided these email notifications to its registered entities only twice a month. However, by the end of the onsite visit, the MOICT had instituted a policy to check the Consolidated UN sanctions list on a daily basis, and subscribed to the RSS feed on the UN website.

264. As part of its internal controls, the MOICT prevents listed persons or entities from registering in the Sijilat system, as all persons (including shareholders) are screened against the relevant UN lists prior to registration. In addition, the Sijilat system automatically searches its database when there are changes to the consolidated UN list, and those listed are unable to conduct any transaction within the Ministry system.

265. As noted in the TC Annex (c.6.5b), lawyers, notaries, and real estate agents brokers (since September 2017), do not have legal requirements in relation to the screening/reporting of designated persons or entities. Moreover, they do not receive notifications of any changes to the UN lists and, in practice, are not searching their customers against the relevant UN lists.

Supervision of TFS Compliance

266. The financial institutions met during the onsite had a good understanding of their screening obligations regarding TFS and generally implemented sanctions without delay. In practice, many financial institutions largely rely on commercial data feeds to check their databases of customers against lists of designated persons. DNFBPs, however, do not have a good understanding of their obligations (see IO.4).

267. While the supervision of TFS implementation is part of the CBB's onsite and offsite supervisory process, the assessment team has concerns regarding the priority attached to it. For example, the assessment team noted a significant lapse of supervision that, while only a singular case, negatively impacts Bahrain's effectiveness regarding TFS implementation and supervision (see Box 6).

**Box 6. TFS noncompliance by Bank X (2012-2017)**

In 2012, Terrorist A was added to the list pursuant to UNSCR 1267, and its successor resolutions. During an onsite examination on Bank X in 2012, the CBB examination team identified a violation where the account belonging to Terrorist A was not frozen. Bank X attributed this violation to an IT error.

In 2013, an account belonging to Terrorist A was discovered to be unfrozen. This new violation was discovered through an onsite examination by the CBB. The unfreezing of the account was attributed to an IT error in the Bank's AML/CFT system. The account remained unfrozen until 2017, when the CBB inquired about the status of the account due to a delisting petition from Terrorist A. During the period when the account was unfrozen, Terrorist A received and withdrew funds of approximately BHD 6 000 (EUR 13 000). The account activity did not include international transfers. Instead, the majority of the activity was from deposits from the account of a Bahrain government-issued pension fund at Bank Y.

Between 2012 to early 2017, Bank X only received one onsite inspection from the CBB. While the CBB made inquiries to the bank regarding other matters, it did not make any inquiries regarding this account. During this period, Bank X was also audited annually by a global accountancy firm which also did not observe the problems regarding this unfrozen account.

Upon learning that the account was unfrozen, in 2017, the CBB issued a BHD 20 000 (EUR 43 115) fine to Bank X. Subsequently, Bank X submitted an appeal request to the CBB. In accordance with the CBB's rules and regulations, the CBB convened an Appeal Panel which considered the merits of the initial decision. After thorough consideration of all the factors, the CBB accepted the appeal by Bank X and replaced it by a formal warning. The appeal was accepted as Bank X provided a written representation explaining that the incident was due to the limitations in the Bank's AML system which was neither intentional nor due to negligence. Since issuing the finding until the end of the onsite visit, the CBB had not conducted an onsite inspection to Bank X.

The CBB did not issue a penalty to Bank Y for transferring the government pension. Bank Y is categorised as a domestically systematic important bank, meaning that it has an annual CBB onsite. As a result, during the period from 2012-2017, when Terrorist A was receiving Bahrain government pension funds, Bank Y was inspected and the CBB did not identify the disbursement of funds to Terrorist A.

Following the onsite visit, the CBB reported that it has hired an expert team which includes a forensic technology specialist to conduct an in-depth investigation on both Bank X and bank responsible for issuing the government pension fund.

268. The assessment team has concerns regarding the proactiveness of supervision and guidance related to TFS due to the persistent violation that occurred between 2012 and 2017, as outlined in Box 6.

269. The assessment team also has a concern regarding effectiveness of the offsite supervision in this case. The IT system which contributed to the failing mentioned in the Case Study 1 is common to several banks in Bahrain but there appears to have been no outreach to these other banks to ascertain whether there had been any TFS issues or breaches. Authorities maintain that the lapse was contained in that particular bank and other banks, having the same IT system, were subject to onsite inspections at different times and no such deficiencies were observed. The assessment team is, however, of the view that other banks should have been proactively alerted to avert such a possibility.

270. Moreover, the assessment team notes that the CBB has not provided detailed guidance to help financial institutions regarding TFS compliance. In the absence of competent authorities being able to collect and disseminate information relevant to identifying sanctioned parties controlling assets indirectly, it is not possible for financial institutions and DNFBPs to fully comply with TFS. Merely screening the names of designated entities against customer and account lists is insufficient for effective TFS implementation.

271. In practice, financial institutions check and scan their client database against the UN list, and have a good understanding of their obligations. This was made evident through discussion with representatives from this sector during the onsite visit. The CBB also has a webpage dedicated to AML/CFT and links to relevant UN sanctions websites, however, at the time of the Bahrain onsite, most of the information was out of date and many of the links were inactive. These concerns were raised by the assessment team, and were subsequently addressed by Bahrain prior to the end of the onsite visit.

272. In regard to DNFBPs, the MOICT has not issued any sanctions for noncompliance by its registered entities with their TFS obligations, and no registered entities of MOICT have had positive hits against the relevant UN or domestic lists during the sample period. Further, the guidance issued by MOICT is clear on the TFS obligations, but not clear who it applies to, nor does it define without delay.

UNSCR 1373 (and its successor resolutions)

273. As noted in R.6, Bahrain has the legal framework to implement UNSCR 1373, though identification and co-ordination by the National Committee. Bahrain has made a number of domestic designations, which has the same searching and freezing obligations as UN TFS. Many of the domestic designations resulted from requests coming from other countries, particularly as a result of joint GCC-designations. Bahrain has not sent any requests to third countries to consider giving effect to its freezing actions.

274. Domestic designations are notified to the public through official gazetting and the publication of these lists in the local newspaper. The CBB also circulates directives to financial institutions, and the MOICT circulates email notifications to its registered entities. Bahrain reports that there have been a number of positive hits

related to its domestically designated list; however, the total number of accounts and assets frozen was not provided to the assessment team.

### *Focused and proportionate measures to NPOs vulnerable to TF abuse*

275. As set out in Chapter 1 of this report, Bahrain has three types of NPOs: associations; private institutions; and special committees. These NPOs are regulated by the Support Directorate within the MLSD. As of 1 January 2017, there were 618 NPOs registered with the MLSD. MLSD maintains a robust database of all NPOs registered in Bahrain. Separately, Bahrain has charity waqfs that are supervised by the MOJ, however no particular measures have been applied to these entities in relation to risk as they do not engage in fundraising activities.

276. As noted in IO.1, the authorities identify the abuse of NPO sector as medium risk in the draft NRA as some NPOs have had ties to Hezbollah and other terrorist organisations. Charities (political, social, or religious) are assessed as low risk. Religious donations were assessed separately, with one being assessed as high risk and the other as low risk.

277. In 2016, the FID initiated TF investigations against three NPOs registered with the MLSD. One investigation resulted in the dissolution of an NPO, and the two other cases were before the courts at the time of the onsite.

278. As noted in Chapter 1, to protect the public from fraud, Bahrain introduced additional requirements that apply to all NPOs in 2013. Specifically, NPOs are required to be licensed in order to open a bank account, and must receive a license to raise and disburse funds (both domestic and internationally). Bahrain applies these measures to all NPOs regardless of the type of activity undertaken, or whether the NPO operates domestically or abroad. The authorities also consider all international transfers as high risk regardless of the destination country or the amount being received or transmitted. Thus, a BHD 1 (EUR 2.15) and a BHD 1 million (EUR 2 156 420) transfer are treated the same in terms of amount of documentation required before the transmission or receipt of such funds is allowed. While the MLSD has developed risk ratings to categorise NPOs as low, medium, or high risk, these risk profiles do not affect the types or frequency of measures imposed on NPOs by the MLSD. The assessment team concluded that Bahrain's application of the same restrictive measures to all NPOs is not consistent with a risk-based approach.

279. In 2016, the MLSD received technical assistance to train MLSD staff and implement risk assessment tools to risk-profile the NPO sector in Bahrain. As a result of this exercise, the MLSD classified 417 NPOs as low risk, 106 as moderate risk, and 95 as high risk. The indicators for risk are outlined in the table below (see Table 25). The MLSD then applied filters to create an additional group, categorised as "at TF risk", which includes approximately 50 NPOs. The filters for this category are: (1) conducts overseas financial transactions; and (2) holds more than BHD 200 000 (EUR 431 077).

Table 25. **MLSD risk factors for NPOs**

| Low risk | Medium Risk | High Risk |
|---|---|---|
| • Unsubstantiated allegations<br>• Other minor or straightforward issues<br>• Minor breach of NPO law | • Significant financial loss to an NPO with no apparent reason<br>• Inadequate systems for checking trustees, where appropriate<br>• Major governance failures<br>• Major breach of NPO's governing documents/constitution<br>• Financial mismanagement<br>• Major fundraising irregularity<br>• Poor financial controls<br>• Matters affecting public trust and confidence<br>• Major breach of NPO law | • Fraud<br>• Other serious criminal activity<br>• Abuse of, or serious harm to, vulnerable beneficiaries<br>• Conducts overseas financial transactions<br>• Reserve amount (= BHD 100 000 (EUR 215 588)<br>• NPO deliberately being used for significant private benefit |

280. However, the MLSD has not communicated its risk analysis or outcomes to the NPO sector. As a result, high risk NPOs are not aware of their risk classification, vulnerabilities, or possible mitigation measures they can take to protect themselves from abuse. The MLSD developed a risk-based outreach plan for the NPOs categorised as "at TF risk", however it has not been fully implemented. The elements of the plan that have been implemented include, setting up consultation hours through the MLSD's Support Centre (established in 2006); holding periodic workshops to enhance the financial management of NPOs; and conducting visits to NPOs' premises to assess and audit financial performance. Shortly before the onsite visit, the MLSD also held a workshop for those NPOs it considered had higher TF risk.

281. The guidance issued by the MLSD to date does not include guidance or typologies on how to counter TF abuse in the sector. Instead, the guidance relates exclusively to financial management. The NPOs met by the assessment team confirmed that they have received this guidance, but have not received any CFT-specific information.

282. All NPOs are required to submit their financial reports for auditing if revenues or expenses exceed BHD 10 000 (EUR 21 550), and to provide annual activity reports to the MLSD. Depending on the NPOs governance, they are also required to hold annual meetings every two or three years to nominate the board of directors, and all the reports, forms and meetings minutes have to be submitted to the MLSD. In addition, the MLSD conducts onsite and offsite inspections, starting with high risk NPOs. The below table illustrates the number of inspections conducted during the sample period by the MLSD.

Table 26. **MLSD Inspections of NPOs (2012-2017*)**

| Years | Number of Onsite Inspections | Number of Offsite Inspections |
|---|---|---|
| 2012 | 101 | 265 |
| 2013 | 82 | 284 |
| 2014 | 85 | 295 |
| 2015 | 37 | 340 |
| 2016 | 241 | 307 |
| 2017 | **68** | **324** |
| Total | **614** | **1804** |

*Note*: *Data from 2017 is from 1 January to 22 November 2017

283. Based on the above table, between 2012 and 2017, 614 onsite and 1804 offsite inspections were undertaken by the MLSD. Further statistics provided by the MLSD indicate that these inspections resulted in three cases being transferred to the PPO for investigation, 98 cases where new board of directors were appointed, 11 cases of dissolution and liquidation. Also, 631 NPOs' bank accounts were frozen until the NPO corrected the situation, and 469 letters were issued to NPOs regarding financial reporting issues. These activities indicate that Bahrain is supervising NPOs in line with its assessment of risk of the NPO sector. However, the assessment team is of the view that Bahrain could benefit from a more detailed risk-based approach to supervision of the NPO sector in order to make the most efficient use of its resources.

284. As noted above, the MLSD also reviews all applications to conduct fundraising activities and overseas transactions. The below table illustrates the total number of applications and decisions rendered between 2012 and 2017. Based on the below table, in the last years two years, the MLSD has rejected nearly half of all applications to conduct fundraising activities and applications to transfer money abroad.

Table 27. **Applications submitted to the MLSD and outcomes (2012-2017*)**

| Application Type | Year | Number of applications received | Confirmed | Rejected |
|---|---|---|---|---|
| **Fundraising** | 2017 | 210 | 107 | 103 |
| | 2016 | 185 | 99 | 86 |
| | 2015 | 204 | 193 | 11 |
| | 2014 | 339 | 308 | 31 |
| | 2013 | 259 | 230 | 29 |
| | 2012 | 159 | 149 | 10 |
| **Cross-border Sending Money** | 2017 | 563 | 195 | 368 |
| | 2016 | 371 | 175 | 196 |
| | 2015 | 496 | 247 | 249 |
| | 2014 | 96 | 67 | 29 |
| | 2013 | 56 | 56 | 0 |
| | 2012 | 34 | 34 | 0 |

| | | | | |
|---|---|---|---|---|
| **Cross-border Receiving Money** | 2017 | 80 | 76 | 4 |
| | 2016 | 180 | 177 | 3 |
| | 2015 | 180 | 171 | 9 |
| | 2014 | 58 | 56 | 2 |
| | 2013 | 55 | 46 | 9 |
| | 2012 | 31 | 28 | 3 |

*Note*: *Data from 2017 is from 1 January to 22 November 2017

285. The NPOs met during the onsite stated it was difficult to obtain a license to conduct fundraising activities or to send money abroad. They also stated that it can take between three weeks and two months for a license to be reviewed. When an application is denied, the NPOs stated that no justification or feedback was provided. While the measures put in place by the MLSD may protect NPOs from TF abuse, a more proactive approach in communication and outreach would enhance NPOs understanding of TF risk, and help them establish appropriate mitigating measures.

### *Deprivation of TF assets and instrumentalities*

286. According to Bahraini authorities, the majority of TF cases investigated and prosecuted involved cash smuggling from individuals involved in Iran, Iraq, and Hezbollah in Lebanon (see IO.9). Given that the majority of TF in Bahrain has an international nexus, the authorities state that it is difficult to confiscate assets and instrumentalities in TF cases, particularly given that the main terror threat comes from a country with which they do not have a diplomatic relation, and this renders asset recovery difficult. Nevertheless, of the 22 TF convictions secured between 2012 and 2017, a total of EUR 6 575 has been confiscated. This amount, though small, is consistent with Bahrain's TF risk profile as TF is mostly related to the execution of domestic terrorist attacks often involving homemade explosive devices, and are, therefore, low-cost and do not require substantial financing.

287. Authorities also provided evidence that instrumentalities of crime are systematically confiscated for all offences, especially for terrorism and TF, where all elements used in the commission of the act would be confiscated, regardless of their low value as a deterrent to further acts. For instance during 2012-17, instrumentalities of TF and terrorism included mobile phones, laptops, computers, cars and a boat, GPS device, hard discs, cameras, explosives, fire arms, machinery items and other related material.

288. The FID also provided a case where it had noted that an attack had been conducted using social welfare payments and where authorities coordinated actions to halt these payments.

289. Bahrain also identified and froze assets of a UN designated individual. Specifically, Box 6 demonstrated that Bahrain froze assets belonging to a Bahraini national listed pursuant to the UN 1267 list (albeit the assets were unfrozen due to IT failures), and financial institutions have frozen accounts belonging to individuals and entities domestically designated by Bahrain.

290. Based on these actions, the assessment team concludes that Bahrain deprives terrorists of assets and instrumentalities in line with its risk profile to a large extent.

### *Consistency of measures with overall TF risk profile*

291. Bahrain has a legal framework for the implementation of TFS by financial institutions, and some DNFBPs, but there are gaps in the application of TFS requirements on all natural and legal persons in Bahrain (see R.6). The CBB conducts its TFS supervisory activities on a risk basis, yet in light of the persistent sanction breach noted in Box 6, it is evident that these activities can be improved.

292. Given that Bahraini nationals have been designated by the UN to the 1267 list, the total assets frozen is consistent with Bahrain's risk profile.

293. Bahrain does not implement a targeted and proportionate approach to overseeing NPOs of higher risk. Outreach to financial institutions, DNFBPs, and NPOs is not conducted on a risk basis. This is concerning to the assessment team given the TF risks present in Bahrain.

### *Overall conclusions on Immediate Outcome 10*

294. **Bahrain is rated as having a moderate level of effectiveness for IO.10.**

## *Immediate Outcome 11 (PF financial sanctions)*

### *Implementation of targeted financial sanctions related to proliferation financing without delay*

295. As noted in R.7, the obligation to implement PF TFS does not apply to all natural and legal persons in Bahrain.

296. Bahrain has no trading relations with Iran or the DPRK; however, given the geographical proximity to Iran, PF exposure risks do exist. Indeed, in 2011, Bahraini authorities successfully interdicted and confiscated dual-use technologies destined to Iran and prohibited by the relevant UNSCRs. In July 2016, Bahraini authorities also interdicted and seized goods manufactured by the DPRK en route to Eritrea, and prohibited pursuant to UNSCR 1718 (and its successor resolutions). The latter interdiction was identified by the UN Panel of Experts established by UNSCR 1874 (2009) as a revenue generating activity organised by DPRK's intelligence agency, which relate to its PF activities.

297. Pursuant to the CBB's FC Modules, all financial institutions are required to freeze, without delay, the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the UN Security Council under Chapter VII of the UN Charter. Therefore, once an entity is added or removed from the relevant lists related to proliferation financing, financial institutions' obligations take immediate effect and no additional transpositions are required by authorities.

298. Registered entities of the MOICT [real estate agents which are structured as companies (until September 2017 at which point, real estate sector was transferred to a separate authority, RERA under SLRB), DPMS, accountants and auditors] also have a legal obligation to implement PF TFS upon notification by the MOICT. Changes to the relevant lists were not communicated without delay by MOICT; however, prior to the end of the onsite visit, MOICT instituted a policy where

communication was automised though the use of RSS feeds. Lawyers, notaries (supervised by MOJ), and real estate agents/brokers (supervised by the RERA since September 2017) do not have legal requirements in relation to searching and freezing obligations to implement TFS, nor do they receive notifications of changes to the UN lists from their respective supervisors.

299. Similar to IO.10, Bahrain has additional measures in place to communicate UN sanctions to financial institutions. While financial institutions are automatically required to implement the relevant UNSCRs, the CBB issues legally enforceable directives that require financial institutions to report whether assets were frozen pursuant to changes to the UN PF lists. However, the CBB issues these directives weeks after changes have been made to the UN lists. These Directives also establish a requirement to report nil responses within two weeks after receipt of the CBB Directive. In practice, financial institutions respond to these directives by providing nil responses, which indicates that they are screening their databases upon receipt of these CBB directives.

300. Based on the below table, it is evident that the CBB notifies financial institutions of changes to the relevant PF-related UNSCRs; however, in some cases, it can take almost two months before financial institutions are notified of such changes. Nevertheless, and as noted above, the CBB's FC Module establishes the legal requirements for financial institutions to search, freeze any assets held by designated entities. As a result, this legal obligation gives immediate legal effect to changes to all UNSCRs, regardless of whether a directive was issued by the CBB at a later date. In practice, financial institutions largely rely on commercial data feeds to check their databases of customers against lists of designated persons.

Table 28**. CBB Directives sent to FIs**

| UNSCR | Date issued by UN | Date CBB Directive Issued |
|---|---|---|
| *Recent UNSCRs related to DPRK* | | |
| **UNSCR 2375** | 11 September 2017 | 19 September 2017 |
| **UNSCR 2371** | 5 August 2017 | 20 August 2017 |
| **UNSCR 2356** | 2 June 2017 | 11 June 2017 |
| **UNSCR 2321** | 30 November 2016 | Not available |
| **UNSCR 2270** | 2 March 2016 | 10 March 2016 |
| *Recent UNSCRs related to Iran* | | |
| **UNSCR 2231** | 16 January 2016 | 13 March 2016 |

301. Registered entities of the MOICT receive email notifications from the MOICT upon any changes to the UN PF lists, but are not required to report positive matches or nil responses. Prior to the onsite visit, the MOICT provided these email notifications to its registered entities only twice a month. However, by the end of the onsite visit, the MOICT had instituted a policy to check the Consolidated UN sanctions list on a daily basis, and subscribed to the RSS feed on the UN website.

302. As noted under IO.10, as part of its internal controls, the MOICT prevents listed persons or entities from registering in the Sijilat system, as all persons (including shareholders) are screened against the relevant UN lists prior to

registration. In addition, the Sijilat system automatically screens against the consolidated UN list, and those listed are unable to conduct any transaction within the Ministry system.

303. Lawyers and notaries (supervised by MOJ), and real estate agents/brokers (supervised by the RERA since September 2017) do not have legal requirements in relation to searching and freezing designated persons or entities' funds or assets, and do not receive email notifications from their supervisors in relation to changes to the relevant PF lists.

### *Identification of assets and funds held by designated persons/entities and prohibitions*

304. Financial institutions in Bahrain have identified and frozen funds and other assets of designated persons, and prevented these funds from being used. For example, during the sample period, Bahrain held frozen assets over EUR 64 600 000 of an Iranian designated entity listed pursuant to the relevant UNSCR.

305. Bahrain has a robust regime for enforcing trade restrictions with regard to Iran and DPRK. This is administered by Customs (which is a part of the MOI) in close co-operation with the National Policy Committee, the NSA and MOFA. Customs officials have an advanced understanding of the risks of proliferation and PF, including diversion and sanctions evasion. Although trade restrictions are not directly tied to proliferation finance under IO.11 and R.7, these efforts are relevant to Bahrain's overall efforts to prevent PF. For example, the aforementioned interdiction and seizure of prohibited DPRK goods in 2016, was linked to the illicit financing activities of the DPRK regime by the UN Expert Panel.

### *FIs and DNFPBs' understanding of, and compliance with, obligations*

306. Large financial institutions have a good understanding of their freezing obligations, including with respect to PF. They generally have staff dedicated to the implementation of TFS and regularly check the UN lists. To ensure this understanding, the CBB checks sanctions screening during their onsite inspections and imposes fines for non-compliance, as indicated in the case study found under IO.10 and the below case study specific to PF TFS non-compliance. DNFBPs, however, are generally not aware of PF-related targeted financial sanctions and as a result, no assets have been frozen.

307. In 2017, the CBB issued a questionnaire to assess the banking sector's governance, risk, and compliance structure, including an assessment of the overall implementation of the TF and PF sanctions framework. The questionnaire was sent to all bank licensees. Based on this questionnaire, it was found that all banks licensed by the CBB are conducting financial sanctions screening (including TF and PF TFS screening), and 69% of institutions used automated screening systems. Additionally, 75% of all banks are subscribed to a commercial sanction screening database. The below table illustrates the frequency of conducting financial sanctions screening.

Table 29. **Frequency of TFS screening by banks**

| Frequency | Share |
|---|---|
| **Real Time Basis** | 57% |
| **Daily** | 22% |
| **Quarterly** | 10% |
| **Monthly** | 6% |

### *Competent authorities ensuring and monitoring compliance*

308. The CBB checks TFS implementation as part of its onsite and offsite supervisory process, as does the MOICT. As noted in IO.3, these inspections are conducted on a risk-basis. The CBB states that its onsite supervisory activities include a comprehensive review with regard to the screening procedures implemented by the licensees to ensure that licensees implement and comply with the UNSCR resolutions, without delay. At the time of the onsite, the MOJ and the RERA did not supervise its entities for TFS.

309. The CBB has applied penalties for violations of its FC Module and Directives in relation to PF TFS (see boxes 7 and 8 below). This demonstrates that the CBB is taking some positive steps to ensure the effective implementation of PF TFS by its licensees.

**Box 7. Bank X noncompliance with PF TFS (2017)**

The CBB identified a breach of its circulars in relation to PF TFS, which resulted in the release of funds to a designated person upon exiting of the banking relationship in 2015. Given the severity of this violation, the CBB took action against Bank X, including the imposition of a monetary penalty of BHD 20 000 (EUR 43 115).

**Box 8. Bank Y non-compliance with PF TFS (2017)**

Bank Y was placed under the CBB's administration on 30 April 2015, due to numerous counts of violations of domestic law. An in-depth investigation by the CBB revealed a number of violations of international and Bahraini Law.

The violations included a range of financial crimes that involved the deliberate alteration and concealment of bank documents to mask illicit trade between Iran and its partners in breach of international sanctions. Bank Y was involved in the process of "wire stripping", a practice referring to the removal of material information from wire transfer instructions. The authorities state that Bank Y was involved in more than 4,500 instances of wire-stripping with the aim to conceal Iran's role as the sender or recipient of funds. The amount of money attributed to such transactions totalled USD 4.7 billion.

The findings of the investigation have been submitted to the Permanent Court of Arbitration in The Hague for deliberation.

310. Detailed guidance or outreach on PF have not been issued or conducted by the CBB to enhance the understanding of, and compliance with, PF TFS. Further, the information on the CBB's website related to PF is out of date. Bahrain has advised that as part of its national action plan, it would conduct a more comprehensive outreach and issue detailed guidance to financial institutions on such issues.

311. In regard to DNFBPs, the MOICT, MOJ, and RERA have not issued any guidance regarding PF to their registered entities. Similar to IO.10, prior to the onsite, the MOICT circulated email notifications to its registered entities twice a month. However, by the end of the onsite visit, the MOICT had instituted a policy to check the Consolidated UN sanctions list on a daily basis, and subscribed to the RSS feed on the UN website. This Consolidated list includes all sanctions approved by the UN Security Council, including PF TFS.

### *Overall conclusions on Immediate Outcome 11*

312. **Bahrain is rated as having a moderate level of effectiveness for IO.11.**

# CHAPTER 5. PREVENTIVE MEASURES

## Key Findings and Recommended Actions

### Key Findings

**Bahrain achieved a moderate level of effectiveness for IO.4.**

1. Bahrain has a diverse financial industry with banks as the key players. FC modules are recognised as a solid base for understanding and complying with AML/CFT obligations across financial sector. Understanding of ML/TF risks across FIs and DNFBPs varies depending on the nature of the sector. Banks, MVTS, insurance and securities have a good understanding of ML risks, and in some instances, less understanding of TF risks. The level of understanding of ML/TF risks seems varied across DNFBP constituents.

2. Major FIs have relatively strong AML/CFT measures commensurate with their understanding of the risks. Entities other than FIs have less robust measures to mitigate the risks, including those emanating from the use of cash transactions relating to the real estate and dealers in precious metals and stones sectors and also from the lawyers being involved in high value complex transactions.

3. Generally, FIs and regulated DNFBPs have CDD measures relative to the size of their business. Major FIs have more robust CDD requirements to identify the beneficial ownership and ongoing monitoring. CDD measures are relatively less robust in the DNFBP sector. Many FIs and DNFBPs often rely primarily on information held in the Sijilat system when identifying a beneficial owner and in verifying the identity of the beneficial owner and they do not seem to independently ascertain whether the purported persons are indeed in control of the entity.

4. STR reporting by the majority of DNFBPs is low and there are concerns about STR quality filed by both DNFBPs and smaller FIs given the varying level of understanding their obligations that might, in some cases, lead to defensive reporting. Record-keeping requirements are generally well understood by the financial sector.

### Recommended Actions

1. Bahrain should further develop the understanding of the ML/TF risks being faced by the financial sector and DNFBPs, in particular by communicating the findings of NRA once finalised and through proactive engagement.
2. Bahrain should provide more guidance on implementing preventive

measures, including on identifying beneficial owners, typologies and red flags on possible ML/TF suspicious activities, to FI and DNFBP in order to improve the quality and quantity of STRs.
3. FIs and DNFBPs should more proactively understand and mitigate the higher risk areas identified, including those emanating from cross-border financial flows and TF risks.
4. Bahrain should work on mitigating the risk arising out of use of cash in the financial industry; especially in the insurance, DPMS, and real estate industry given their significance and level of risk accompanied by the risk of cash smuggling.
5. Bahrain should further enhance the process on identifying ultimate beneficial owners by DNFBPs.
6. In particular, Bahrain should take urgent steps to raise awareness among lawyers, who are now subject to comprehensive AML/CFT obligations, especially as they are involved in high-end and complex real estate transactions and formation of companies and holding customers' funds.

313. 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)*

314. In terms of risk and context, not all sectors are of equal importance in Bahrain. As a result, the assessment team did not place the same weight on the implementation of preventive measures (both positive and negative) equally across sectors. The assessment team's views of the relative importance of each sector, based on risk and context are set out below, and informed the overall conclusions about the implementation of preventive measures.

315. The banking sector (comprising 29 retail banks and 76 wholesale banks) plays a dominant role in Bahrain, with an asset base of BHD 72 billion (EUR 155 billion) as at November 2016. Banks offer a wide variety of products, service a diversified client base, hold substantial foreign assets, and maintain business relationships with cross-border customers. Retail banks have been identified as high risk and wholesale banks as medium/high risk in the draft NRA.

316. Next in line of relative importance are money changers and MVTS providers. The sector comprises eleven small scale and eight large scale businesses. Considering Bahrain's status as a regional financial centre, cross-border flows and the relative importance of cash in Bahrain, this constitutes an important segment.

317. The securities sector in Bahrain is relatively small with daily average number of trades at 43. The life insurance sector is also relatively small with the share of life insurance in gross premium amounting to 19% compared to 81% for non-life. The total average annual gross premium for the entire sector is around BHD 0.52 billion.

318. Among DNFBPs, DPMS are large in number (more than 350) and generate significant amount of business. Real estate agents which are more than 4000 in number also play a significant role in Bahrain, considering expansion of the sector

and ongoing opening of the property market for foreign investors. Lawyers are generally involved in high-end and complex real estate transactions and company formation process. Accountants and auditors are considered as low risk due to requirements for experience and qualifications and restrictions on business.

319. The assessment team based their conclusions on IO.4 on, inter alia, discussions with a range of types and sizes of FIs and DNFBPs correlating to the sectors defined by the FATF, on how they understand, manage and mitigate their risks, and implement preventive measures; reviews of their internal manuals and procedures; discussions with supervisors and SRBs, their understanding of risks; and by reviewing the draft NRA and guidance issued by authorities.

### *Understanding of ML/TF risks and AML/CFT obligations*

#### *Financial institutions (FIs)*

320. The FC Module is a comprehensive framework of rules and guidance issued by the CBB and sets out detailed requirements for FIs. The Module provides a sound basis for FIs to develop their understanding of AML/CFT obligations and conduct ML/TF risk assessment. Requirements set out in the Module are generally well understood by most FIs, and the sector as a whole has a positive view about the approach taken by the CBB to consolidate the AML/CFT requirements in one place and update as needed.

321. FIs generally have a good understanding of their exposure to ML risks. They implement processes and procedures to identify, assess and document these risks. The majority of FIs met have undertaken risk analysis, based on various risk factors including customers, products, geographic exposure, and distribution channels. In addition, FIs determine risk mitigation measures for identified inherent risks, and make use of monitoring systems to determine the adequacy of controls implemented to mitigate risks. In most cases, this risk assessment is conducted on an annual basis. Overall, banks, MVTS, insurance and securities have a good understanding of ML risks though understanding of TF risks is relatively less developed in FIs other than major banks.

322. The implementation of a risk-based approach (RBA) is still relatively new for some FIs, and models are being further improved. Overall, the understanding of risks seems the most developed in large banks and MVTS providers that are part of international financial groups. Many banks have implemented comprehensive business-wide risk assessments and ML/TF risks inform their decision on expansion of business operations and whether to enter new markets.

323. Implementation of a risk-based approach in smaller institutions needs improvements, for example in areas such as cross-border financial flows and TF risk. The CBB has performed a cross-cutting analysis of the risk assessments of FIs. While in many cases, banks have developed a client risk rating mechanism, areas of improvement include more effective procedures to properly identify customers classified as high risk, and to properly document internal risk assessment mechanisms.

324. The CBB provided some indicators for determining risk factors in FC Modules. This has helped FIs enhance their understanding of the RBA and

contributed to a better understanding and implementation of the requirements. The NRA questionnaire circulated by the CBB among FIs to collect information to assist in the development of the draft NRA has also led to better appreciation of ML/TF risks within the sector. These questionnaires had quantitative-based questions which covered the bank's size, business activity, complexity of products and geographical dispersion. This exercise aimed to qualitatively assess the bank's governance, risk and compliance structure including an assessment of the overall implementation of the AML/CFT framework within the broader context of the bank's business.



### *Designated Non-Financial Businesses and Professions (DNFBPs)*

325. The level of understanding among DNFBPs varies between sectors; some have a relatively good understanding (e.g. accountants and auditors), while others (e.g. high-value DPMS and real estate sectors) seem to limit their understanding to certain risk elements only (i.e. PEPs), while underestimating others such as potential use of cash in their sector and its vulnerability. They would rarely ask their customers about the source of their funds, even when large amounts of cash are involved. AML/CFT obligations have recently been issued for legal professions and that illustrates why their understanding of risk is still limited.

326. Overall, most DNFBPs, other than legal professions, have a basic understanding of the need to conduct due diligence on their customers and to report suspicious transactions where required. While MOICT engages with the DNFBPs under its supervision, understanding of ML/TF risks needs to be further developed within the sector as a whole.

327. The understanding of ML/TF risks across the private sector will be further developed as Bahrain finalises its draft NRA and shares its findings with the private sector. This will be an important step to set out a national position on key threats and vulnerabilities and measures needed to address them.

## *Application of risk mitigating measures*

### *Financial institutions*

328. FIs across sectors categorise their customers based on risk (usually low, medium, and high) that require different CDD measures and monitoring procedures in accordance with the level of risk identified. Mitigating measures seem commensurate with the risks identified (i.e. more scrutiny is carried out by FIs in higher risk cases, such as obtaining additional information, escalation procedures while on-boarding higher risk clients, and stricter monitoring rules). The understanding and sophistication of implemented measures are most developed in larger institutions, particularly banks as well as others belonging to international financial groups such as larger MVTS. Major FIs thus have relatively strong AML/CFT measures commensurate with their understanding of the risks. The understanding is also frequently updated upon changes to the CBB's rulebooks, and based on further guidance provided by authorities.

329. The CBB has highlighted common deficiencies observed in certain banks concerning risk management models, such as insufficient profiling of the customers,

lack of verification of the identity of the beneficial owners for corporate customers, and expired original identification documents.

330. Overall FIs have in place a risk mitigation policy that includes AML/CFT policies and procedures. Comprehensive Management Information Systems (MIS) exist to ensure that the AML/CFT program is operationally effective, including in identifying unusual activity. This aims at effectively identifying, managing and mitigating ML/TF risks posed by the business; including risks connected to customers, products/services, geographical location, and distribution channels. Policies and procedures include customer acceptance, updating of customer data, monitoring and reporting of STRs, handling of high risk customers, businesses, products/services, delivery channels, and customers based in high risk geographic areas.

331. All financial institutions are subject to an annual external AML/CFT compliance audit. Internal and external auditing seems to be effective in checking compliance with the CBB regulations. Compliance function of FIs reports to the Board or Board committee.

### *DNFBPs*

332. Entities other than FIs have relatively less robust measures to mitigate the risks, including those emanating from the use of cash transactions relating to the real estate and DPMS. DNFBPs reported that they are required to have a set of internal controls and procedures to fulfil their obligations regarding AML/CFT, and to review and keep these controls updated. In addition, external auditors are required to ensure the proper implementation of those internal controls and report an opinion about them in the audited financial statements.

333. Measures to mitigate potential risk of the use of cash in the DNFBPs sector (particularly in DPMS and for real estate transactions) warrant further attention from the sector as well authorities; especially given the significance and volume of real estate industry in the country and the trend in the formation of partnerships between Bahraini individuals and citizens from the GCC region through the establishment of real estate and construction companies and the threat of cash smuggling.

## *Application of CDD and record-keeping requirements*

### *Financial Institutions*

334. Overall, FIs have implemented adequate risk-based mitigation measures concerning CDD, record-keeping, and monitoring. However, one of the insurance companies met stated that they would accept cash in buying single premium products with limited CDD process. FIs are aware that they should refuse or terminate client relationships if the CDD process cannot be completed, but did not demonstrate that they were aware of the obligations to file an STR in such cases. Deficiencies regarding basic AML/CFT obligations were still noted by the CBB in its supervisory inspections (e.g. regarding proper keeping of identification documents, and due diligence identification requirements). The CBB stated that such deficiencies get rectified by FIs subsequent to the CBB's recommendation and the

rectification is later confirmed through the different follow-up mechanisms used by the CBB.

335. Most FIs use automated models and systems for building different scenarios and rules, which are integrated in transactions monitoring systems to identify abnormal or unusual patterns. The alert thresholds are more stringent for high risk situations as identified by FIs through their risk profiling. Additional scenarios are also developed according to the risk level of the client. Similarly, the understanding and sophistication of implemented measures are relatively better developed in larger FIs as well as those belonging to international financial groups.

336. Regarding the identification of beneficial owners, FIs make use of the publicly available "Sijilat" system that contains updated information on the beneficial ownership of the legal entities registered with the MOICT. FIs also use the government card reader information, which is available free of charge and constitutes reliable and authenticated information about individuals. FIs reported that they would also ask for more information from their customers if they felt unsatisfied with the information and documents presented during the account opening or update process.

337. For legal structures, FIs are required to identify the ultimate beneficial owner. The assessment team noted that some FIs limit their understanding of the beneficial ownership to the shareholders of the legal persons, without necessarily identifying the ultimate natural person in that regard. This might be due to the fact that the definition of the ultimate beneficial owner was added to the FC module glossary just before the end of the onsite visit. Some FIs also rely on the Sijilat system, which may not necessarily have the information of the natural person who ultimately control the legal person in all cases (see IO.5). The names of beneficial owners separately captured in Sijilat can only be extracted from Sijilat through the privileged users of the MOICT. FIs generally reported that they obtain the basic CDD requirements prior to the disbursement of funds and do not commence business relationships prior to the completion of the relevant CDD requirements. However, some failures have been observed by the CBB during its inspections where application of necessary CDD requirements prior to the commencement of the business relationship was found inadequate. Main deficiencies include insufficient profiling of the customers, non- verification of source of funds, lack of relevant CDD documentation such as Memorandum and Article of Association and verified identity of the beneficial owners for corporate customers.

338. FIs in general across the sector have strong record-keeping procedures in place, in line with FC module requirements and their internal AML/CFT procedures and manuals. Records are maintained for at least five years. This includes accounting and identification records, annual compliance reviews reported to or conducted by MLRO and records showing how these reports were dealt with and what action, if any, was taken as a consequence of those reports. Furthermore, FIs generally provide prompt access to documents required by authorised persons internally within the group and to competent authorities.

### *DNFBPs*

339. The level of compliance is varied among DNFBPs. Most implement basic CDD identification and record-keeping measures. Some DNFBPs that are part of a

financial group are subject to CDD requirements similar to these of FIs and their understanding and compliance are relatively better. Most of the MOICT regulated DNFBPs (accountants, auditors and DPMS) have an AML/CFT policy in place and they seem to check the "Sijilat" System to verify the shareholders information provided in the course of the business relationship. Like FIs, DNFBPs also use the government card reader information, which is available free of charge and constitutes reliable and authenticated information about individuals. Some DNFBPs seem to be aware that they should refuse or terminate client relationships if the CDD process cannot be completed, and then consider filing an STR. It was not clear to the assessment team if it was being done in practice.

340. Concerns also exist on the effectiveness of the process for identifying beneficial ownership details by DNFBPs and their understanding was uneven. However, further efforts are needed by all relevant authorities (MOICT, MOJ and RERA) to enhance understanding in respective sector.

### *Application of EDD measures*

#### *Financial Institutions*

341. AML/CFT policies provided to the assessment team during the onsite visit and discussions with FIs indicate that FIs across sector have an adequate understanding of specific high risk situations, specifically risk areas associated with Politically Exposed Persons (PEPs), Targeted Financial Sanctions (TFS), higher-risk countries, introduced businesses, non-face to face transactions, and new technologies, charities, clubs and other societies which require additional enhanced measures. However, many FIs met would limit their understanding of the high risk customers to the PEPs. The understanding and implementation of measures is relatively more mature in in banks and MVTS providers belonging to financial groups, though there is room for improvement in application of EDD measures as identified by CBB inspections.

#### *Politically exposed persons (PEPs), Targeted financial sanctions (TFS), and higher risk countries identified by the FATF*

342. FIs are aware of the enhanced measures required for PEPs, and do not usually distinguish between domestic and foreign PEPs. They have put in place systems to identify PEPs, their family members, and close associates. Generally, FIs make use of open sources and commercial databases for the screening process and conduct their own research. The assessment team could not verify whether an approval of senior management is sought before on boarding PEPs as clients. However, insurance companies do not inform the senior management before the pay-out of the policy proceeds where higher risks are identified because it is not a requirement. FIs across sector generally exhibited good understanding of requirements and seem to implement measures to mitigate risks. Discussion with private sector and the CBB revealed that there have been improvements in compliance levels over the past few years as earlier inspections by the CBB found instances of gaps, particularly in properly identifying customers classified as PEPs, their source of funds, and beneficial ownership details in certain cases.

343. FIs seem aware of their requirements in relation to TFS, and have measures in place to comply and screen before the establishment as well as during the course of the business relationship. They are aware that they should freeze without delay, any funds or assets made available directly or indirectly for or to the benefit of the designated persons and entities. However, there have been instances where the CBB found some FIs failing to screen customers prior to the commencement of the business transaction, and a limited number of FIs violating the TFS requirements. The CBB also provided an example of an FI that overlooked TFS requirements and, therefore, allowed for the movement of funds (see IO.10 case study).

344. FIs also stressed that they apply effective and proportionate enhanced measures where customers residing in countries or territories identified as higher risk by the FATF or as notified by the CBB as high risk. They would also notify the CBB/FID of any suspicions related to ML/TF when dealing with such customers.

### *Correspondent banking, wire transfers, and new technologies*

345. For FIs with cross-border correspondent banking relationships, enhanced AML/CFT requirements seem to be well understood which include on-going due diligence on customers with direct access to the account, and consideration of factors such as regulation and supervision in respondent institutions countries. FIs in general are also aware of the requirements to verify the identity of any third party that will have direct access to the correspondent banking services. Also, correspondent banks must obtain confirmation that the respondent bank is able to provide relevant CDD information upon their request.

346. As part of the on-site supervision, correspondent banking relationships questionnaires are reviewed by the CBB to verify whether all information stipulated in the FC Module are included. Where correspondent banking relationships are commenced with customers residing in jurisdictions with lower KYC standards or classified by the FATF as non-cooperative, FIs demonstrated satisfactory CDD measures to duly verify the AML/CFT internal controls. However, some relatively smaller local banks and foreign branches failed to apply adequate EDD for respondent banks in higher risk jurisdictions. As stated earlier, CBB stated that these deficiencies are addressed through follow up processes; however this warrants further preventive and proactive actions from authorities, rather than focusing on remedial approach, to curb higher risk transactions.

347. FIs in general also demonstrated a good level of understanding of the ML/TF risks associated with wire transfers and new technology and implemented additional measures to ensure risk mitigation. Such measures include formation of a cross functional team (compliance, risk, business and technology) while developing any new products and services and embedding AML/CFT requirements during the process. There are instances of some wire transfers having incomplete or missing originator information as per CBB findings. The assessment team concludes that Bahrain needs to further develop understanding and corresponding mitigating measures, within the private sector on new products and services.

### *Designated Non-Financial Businesses and Professions (DNFBPs)*

348. DNFBPs have some knowledge of EDD requirements applicable in the presence of higher risks, specifically in relation to PEPs. The DPMS sector indicated

that they could use their system to check sanctions lists, making use of the email notifications disseminated by the MOICT. However, their understanding is relatively less developed. For example, implementation of requirements relating to TFS or customers associated with high risk jurisdictions identified by FATF or otherwise needs improvements. Accountants and auditors demonstrated a good understanding and seem to have built in these requirements as part of their standard operating procedures.

349. Requirements for other sectors, such as lawyers, have been significantly updated very recently and it is unclear at this stage the extent to which these are applied in practice.

### *Reporting obligations and tipping off*

### *Financial institutions*

350. The STR requirements are well understood, and FIs met maintain risk-based monitoring systems relative to their size, number of customers, complexity, geographical exposure and type of transactions. Where significant or abnormal transactions were detected, they would seek to verify the source of funds specifically for transactions above BHD 6 000. Where the FIs are unable to determine the economic purpose of customer behaviour, they file an STR to the FID and CBB through the online STR system. FIs have user access to submit the required details related to the STR, including relevant background documentation.

351. There have been concerns from FID about the quality of STRs across reporting entities and there is room for improvement especially in the non-banking sector. Authorities also noted that the general trend is improving. FIs also stated that they include all relevant information and might be contacted sometimes by either FID or CBB to get more information on the STRs filed. STRs filed by some of the sectors within FIs are seen either low in number or non-existent (such as investment business firms and securities sector) given the volume of the reporting entities that operate in Bahrain.

352. The following STRs were submitted by FIs from 2013 to October 2017:

Table 30**. STRs submitted by FIs**

| Reporting Entities | 2013 | 2014 | 2015 | 2016 | Oct- 2017 |
|---|---|---|---|---|---|
| **Banks** | 226 | 238 | 281 | 374 | 434 |
| **Insurance and insurance brokers** | 9 | 18 | 18 | 12 | 10 |
| **Money changers and MVTS providers** | 170 | 564 | 758 | 534 | 393 |
| **Money brokers and mediators** | 0 | 3 | 0 | 0 | 1 |
| Total | **405** | **823** | **1057** | **920** | **838** |

353. Banks, money changers and MVTS providers are the largest contributor to STRs with five banks filing nearly 52% of the total STRs filed by the whole banking sector. This is in line with the overall risk and context of Bahrain, however, authorities should continue further outreach to the rest of the sectors to enhance the reporting requirements. While the majority of STRs are filed in time, one of the FIs met during the onsite indicated that it may take up to one month to file an STR, since

the processing of transactions takes place at the head office, which in turn would assign the STR to the MLRO for reporting, if needed. The FID and CBB reported improvements in the quality of STRs, though concerns still exist (see IO.6).

### *Designated Non-Financial Businesses and Professions (DNFBPs)*

354. Some of the DNFBPs understand the requirements of STR reporting and need to include information on the customer's identity and other supporting documents (i.e. invoice, CDD, other records related to transaction). The below table outlines to level of STR reporting by DNFBPs.

Table 31. **STR reporting by DNFBPs**

| Sector | 2013 | 2014 | 2015 | 2016 | October 2017 |
|---|---|---|---|---|---|
| DPMS | 185 | 1 | 4 | 0 | 1 |
| Others | 8 | 0 | 1 | 3 | 1 |
| Total | **243** | **43** | **18** | **4** | **5** |

355. Both the level and quality of reporting done by DNFBPs needs major improvements. Authorities indicated that the quality has improved over last few years and the level of defensive reporting from the sector has reduced. However, this does account for the very low level of reporting by DPMS and absence of any reporting by the real estate sector during last 5 years, even though these sectors are identified as vulnerable for ML. Given the significance of the real estate sector to Bahrain's economy, the FID and RERA need to enhance understanding around potential red flags and typologies especially with regards to the risk of use of cash. Lawyers have recently been subject to reporting obligations, and consequently were not previously reporting STRs. This raises concerns as they are involved in real estate transactions and formation of companies and hold customers' funds.

356. In some cases, authorities directly reach out to reporting entities for additional information or clarification about a filed STR or other possibly linked subject that might maintain account or have transactions in that institution. FIs and DNFBPs are generally satisfied with the feedback that they receive from the FID, but are of the view that it could be further improved through the provision of information on the final decision on cases reported.

357. Both FIs and DNFBPs met indicate difficulties in detecting suspicious transactions related to TF and would welcome additional guidance from authorities in this regard. FIs could not recall any distinct characteristics of the STRs filed related to TF. It would be useful if Bahrain issues further guidance to the reporting entities, specifically DNFBPs, including typologies and red flag indicators, including for TF given the level of risk TF poses in Bahrain.

#### ***Tipping off***

358. Both FIs and DNFBPs met seem to understand the requirement not to tip-off their customers, the beneficial owner or other subjects of the STR when information relating to them is being reported to the relevant authorities. As part of offsite supervision, the CBB and MOICT also reported that, in its capacity as a supervisory authority, it would verify the policies and procedures of supervised entities, which include practical measures to prevent tipping off.

### *Internal controls and legal/regulatory requirements impending implementation*

#### *Financial Institutions*

359. In general, FIs illustrated a good understanding and implementation of the controls and procedures. This was apparent, in particular by larger banks and other FIs that are members of expanded affiliated group. Such policies, procedures and controls are documented, reviewed, updated and approved by the Board of Directors on a regular basis (at least once a year and also when needed). The documentation, and the Board's review and approval, are made available upon request to the CBB.

360. FIs are subject to internal and external audits as per the CBB requirements. While there are some gaps as revealed by CBB inspections (e.g. failure to promptly update compliance manual, absence of approval of Board of Directors in certain cases and EDD related deficiencies, specific to charities, clubs and other societies), there is also an ongoing improvement in compliance levels.

361. FIs have AML/CFT group-wide programs in place to cover branches and subsidiaries operating within and outside Bahrain. Financial secrecy does not seem to impede implementation of the AML/CFT requirements; therefore FIs can and do share information within the group for AML/CFT purposes. For example, specific instances were cited by banks where information was shared within financial groups for transaction monitoring and reporting purposes. Such programs establish and maintain appropriate systems and controls for compliance with the regulatory requirements to limit their vulnerability to financial crime.

#### *DNFBP*

362. Some of the DNFBPs (DPMS, accountants and auditors) shared copies of their respective brief AML/CFT internal controls and procedures and confirmed that these must be at least annually reviewed, assessed, and updated to ensure their effectiveness. In addition, external auditors are required to ensure whether such internal controls are being implemented.

363. Lawyers do not yet have written AML/CFT controls and procedures because the ministerial order to include them as regulated entities for AML/CFT purposes was significantly updated on 5 November 2017. As regards to real estate, the assessment team could not verify whether this sector has instituted AML/CFT controls.

### *Overall conclusions on IO.4*

364. **Bahrain is rated as having a moderate level of effectiveness for IO.4.**

# CHAPTER 6. SUPERVISION

## Key Findings and Recommended Actions

### Key Findings

**Bahrain achieved a substantial level of effectiveness for IO.3.**

1. The CBB has strong controls to prevent criminals from beneficially owning a significant or controlling interest or holding a management function in a FI. The MOJ has reasonable controls in relation to the fitness and properness at initial licensing and thereafter; the MOICT also has reasonable controls at initial registration and thereafter to prevent criminal ownership and control of its registered entities.
2. The CBB generally understands the ML risks of the sectors it supervises; the MOICT generally understands the ML risks of the sectors it supervises although it is in a less solid position than the CBB. The assessment of the risks of the lawyer sector needs to be reconsidered. Overall, understanding of TF risks is developing.
3. The CBB has strong elements of a risk-based approach to supervision and it reviews significant offsite information (including STRs which it receives), which informs onsite inspections and the use of other supervisory tools to address risk. The overall approach is not yet a comprehensive AML/CFT risk-based approach and the assessment team has a concern about the level of supervision. The MOICT has put in place a framework for, and a largely risk-based approach, to supervision (it too reviews STRs and, in addition, auditors' reports on the quality of AML/CFT controls). There is strong momentum by the MOJ to introduce supervision of lawyers and to ensure that the new RERA/SLRB will meet its responsibilities for supervision of all real estate brokers.
4. The CBB requires remediation of AML/CFT breaches and has imposed a range of sanctions and made referrals for prosecution but there is scope to increase the use of sanctions as the level of onsite supervision increases. The MOICT also requires remediation and has imposed sanctions including, in particular, the suspension of commercial registrations. The MOJ has revoked the licences of lawyers who do not meet statutory requirements of fitness and propriety.
5. The CBB has noted improvements in compliance culture and understanding of risk of FIs over the period since 2012. The MOICT has also noted improvements in compliance by DNFBPs under its supervision.
6. The CBB has consistently provided guidance and other information on AML/CFT to FIs during the period under review, although this could usefully

be enhanced. The MOICT has provided information to DNFBPs although its level of resources reduces its capability to issue guidance and conduct outreach.

7. All the existing operational supervisory authorities require additional staff resources.

*Recommended Actions*

1. Bahrain should, as is already proposed, ensure that additional staff resources are provided for the CBB, the MOICT, the MOJ and the RERA/SLRB so that they have a suitable number and quality of staff to undertake comprehensive risk-based supervision.
2. Supervisory authorities should further develop their understanding of TF risks.
3. The CBB and the MOICT should enhance their existing risk-based approaches and monitor the effectiveness of the use of sanctions, so as to ensure that risk-based supervision is comprehensive, including by taking account of the NRA and a more defined approach to TF risk. The MOJ and the RERA/SLRB should introduce comprehensive risk based supervision and effective sanctions frameworks.
4. Once the NRA has been published: the CBB should issue guidance on emerging trends, trade based ML and FinTech; and the MOICT should extend its existing outreach by issuing comprehensive guidance on the AML/CFT measures to be adopted by entities it supervises and review its approach to outreach so as to ensure that it is AML/CFT risk-based and effective. The MOJ and the RERA/SLRB should also issue comprehensive guidance on the AML/CFT measures for its supervised entities and establish a programme of effective outreach.

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

## *Immediate Outcome 3 (Supervision)*

366. In terms of risk and context, not all sectors are of equal importance in Bahrain. As a result, the assessment team did not place the same weight on supervision (both positive and negative) equally across sectors. The assessment team's views of the relative importance of each sector, based on risk and context are set out in IO4, and informed the overall conclusions about the implementation of supervisory measures in respect of those sectors.

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

#### *Financial Institutions*

367. The CBB has strong controls to prevent criminals from beneficially owning a significant or controlling interest or holding a management function in a FI.

368. The CBB has a licensing directorate of seven officers; it is adequately resourced. It receives detailed information for applications for licences, controllers in relation to those licensees (and those seeking to decrease or increase their level of control) and approved persons (senior individuals, individuals designated a head of a function or with specific functions such as board members, heads of compliance, compliance officers, MLROs and risk management related functions).

369. Control includes legal and beneficial ownership. Information on the group structure is required and analysed by the CBB. The CBB considers applicant controllers' financial standing, judicial and regulatory records, standards of business practice and reputation, and their track record. The level of scrutiny differs depending on the level of control (control starts from a 10% threshold for banks).

370. All prospective controllers are checked against the internet, a database provided by an external service provider and the CBB's own records. There is close liaison between the licensing directorate and other directorates of the CBB. Source of funds is reviewed. Limits are set on the level of control permitted for individuals and unregulated legal persons. For regulated legal persons proposed to be controllers, this includes checks with the home country supervisory authority that home country prudential requirements are satisfied and that the supervisor will be willing to exchange information for AML/CFT purposes. The CBB always contacts foreign supervisory bodies where the controller (whether a firm or an individual) has, or had, an involvement. A reference is required for each controller which is an individual registered with another authority; individuals are checked with a credit reference agency and also interviewed unless already known to the CBB. In addition, the CBB requires a confirmation of good conduct from the MOI to be provided by Bahraini controllers who are individuals. In some cases a reference from previous employers is required.

371. Some associates are directly covered in the CBB's checks. These include close family members, other undertakings of which the applicant controller is a controller; employees or partners of the applicant; and persons with whom the controller has entered into to agreement on the control of the licensee. The overall system of review would capture other forms of apparent associate relationship.

372. The checks for controllers who are individuals mentioned above also apply to approved persons. For key functions, the CBB also obtains a letter from the previous employer on the individual's duties.

373. The statutory deadline for dealing with applications has not presented any problems to the CBB.

374. The CBB has rejected applications for, insurers and other FIs during the period 2014-2017 (statistics on the total number are not maintained) as a result of not being fit and proper and/or inadequate financial standing. Applications to be a

controller of a bank have been rejected on the same grounds. Fourteen applications to be an MLRO have been rejected since 2012; although these rejections were mainly due to insufficient training or lack of qualifications, they reflect the CBB's commitment to high standards and willingness to reject applications.

375. Approval of changes of controller and the appointment of approved persons after licensing of an FI is dealt with by individual sectoral supervisory directorates. There is close liaison between the supervisory directorates and the licensing and compliance directorates. The approach taken is the same as for applications for licences although contact with foreign supervisory authorities is not as systematic; requests for input have been made by use of the IOSCO MMOU. The supervisory directorates demonstrated to the assessment team that some persons had been rejected for approval on the basis of criminal or other misconduct issues or professional competence in relation to banks and mostly on grounds of professional competence in relation to the insurance sector.

376. The accuracy of controller information in the CBB's records is checked upon receipt of a report which must be provided by each licensee each year on the identity and the extent of the interest of each controller and during onsite inspections; approved persons must inform the CBB where there is a material change to the information already provided, and the accuracy of information about such persons and the suitability of their conduct is also checked during onsite inspections. The CBB has uncovered issues which could be relevant to criminality (although these have been rare), such as one case where it found through a review of financial statements that exceptional remuneration was being paid to a board member (leading to the imposition of a formal warning by the CBB). In other cases, the CBB has been advised of issues; it has successfully sought prosecution of two banks where there was misconduct by controllers. Findings during onsite inspections have also led to the dismissal of approved persons by banks (see sanction analysis below). The MOICT advises the CBB about changes of beneficial owner when it becomes aware of them; the CBB checks its records upon receipt of this information. Changes to the information on a FI in the Sijilat system cannot be made without CBB approval.

377. The CBB advised that it has been very rare in the period under review for a new controller or approved person to have been appointed without approval – there was one case some years ago when the management of a bank had not been advised of the sale of an interest in the bank. Recently, in light of consideration of the totality of information about a listed entity, an inspection focussed on controllers and found that information on all controllers and their related parties had not been provided to the CBB.

378. With regard to potential unlicensed business, the insurance supervisory directorate (but not other directorates) takes active steps to police the perimeter. This directorate has checked advertisements and information on legal persons on the MOICT's website. It has followed up four potential unlicensed businesses with the MOICT; three of these cases were found to be transacting unlicensed insurance broking and were referred to the MOICT as the registrar of those businesses. The MOICT has referred these cases for prosecution. In one other case the CBB was able to provide information to the FID following an initial enquiry with that authority. This was in connection with a consultant undertaking investment business without a

licence. Action by the CBB resulted in a conviction, asset freeze and imprisonment for the individual. More generally, the CBB is aware of the need to address unlicensed business when it becomes aware of it – the case involving seven money changers mentioned in the sanctions table below being a case in point. The MOICT will not issue a CR for a legal person engaging in financial activity unless it has checked first that a licence has been issued by the CBB.

### *DNFBPs*

379. The MOICT is responsible for registering real estate agents which are structured as companies, DPMS and accountants and auditors. Applications (specifically beneficial owners and other controllers) are checked with the MOI through the Sijilat system and, in addition, the system automatically checks names on the system on an ongoing basis with lists of persons designated under UNSCRs. Licences are reissued each year and the MOI is also requested to provide input at that stage (and when there is a change of ownership or control). The MOI's checks include reviews of international closed source databases. During onsite inspections the MOICT checks that information on beneficial owners, legal owners and controllers is consistent with its records (and the MOICT is aware that auditors also conduct a check). It is felt that this activity would uncover associations with criminals. It does not take active steps to police the perimeter in relation to possible unlicensed businesses although it has established a national complaints system (TAWASUL), which can be used by members of the public to make a complaint to the MOICT about such business.

380. The MOJ has reasonable controls in relation to lawyers at both the licensing stage and thereafter. The MOJ requires applicants to provide a certificate of good standing from the MOI and considers that its checks would uncover any issues of association between lawyers and criminals. Negative feedback is provided by the MOI in relation to 5/6 individuals each year (of the circa 150 applications) and their applications are refused. As a result of a ministerial edict the MOJ expects court officials to advise it where a lawyer is convicted, and licences have been revoked by the MOJ in two cases during the period under review. Licences are reissued annually; the MOI check is conducted again before a licence is reissued. The same approach applied to real estate brokers until September 2017; it remains responsible for renewals of real estate broker licences until the new regulatory authority (RERA/SLRB) is operational in February 2018 and no new licences will be issued until that time.

381. All notaries are civil servants. Prior to employment the MOJ obtains a certificate of good standing from the MOI. There is no requirement for this certificate to be updated but, on the basis of a ministerial edict which has been issued, the MOJ expects that, if a notary were to be convicted, it would be advised by court officials so that it could take appropriate disciplinary action (potentially including removal of the certificate).

## *Supervisors' understanding and identification of ML/TF risks*

### *Financial Institutions*

382. The CBB generally understands the ML risks of the sectors it supervises. Its understanding of TF risks is less strong than for ML but is clearly developing. It receives less information from licensees on TF compared with ML and TF has not yet had the same level of sectoral analysis as ML. The completion of the NRA and a greater volume of onsite inspections will benefit understanding of both ML and TF risk.

383. The NRA questionnaire for banks covered consideration of discussion of AML/CFT at board meetings; policies and procedures; training; overall risk profile (the location of the FI's operations and customer base; and the size of the customer base); risk assessment by the bank; sanctions, including TFS; STRs; PEPs; and the risk-based approach (including monitoring). The CBB consolidated the 67 responses into a single report and met with banking sector representatives in working groups. Similar questionnaires were issued to the other FI sectors (with two questionnaires being issued to the insurance sector) and consolidated reports produced by the CBB. The CBB also receives or develops significant other offsite information (see the section immediately below) to inform its views on risk.

384. The CBB was articulate in discussion on the ML client and product risks presented by each part of the banking sector. The sector is seen as high risk. The higher client risks are considered to be high net worth individuals; PEPs and their associates; consultancy firms; complex legal structures; real estate companies; non-resident persons; cash intensive businesses; and charities, clubs and other societies. It was also articulate on the higher product risks (private banking, correspondent banking relationships, current accounts and introduced business). This analysis might require more focus as medium/high or high risk areas cover large parts of the banking sector. For example, they cover all current accounts and all NPOs rather than those which are higher risk. TF risk has not had the same depth of analysis as ML and the national level of understanding of TF more generally means that it is not as developed as for ML.

385. MVTS remittances to other jurisdictions are made mostly by workers from those jurisdictions. Remittances are often funded by cash. There are large volumes of payments although the values of the payments are low. The CBB had clear views on the new products being launched by the sector and the level of AML/CFT compliance by MVTS, with larger firms having better compliance than family owned businesses. The specialised licensee directorate also receives statistics on remittance flows by currency and country, and was aware of reasons for changes in the magnitude of the figures. All problem cases to date have been ML cases. The CBB considers that the risk of ML is medium. With regard to MVTS, it was initially indicated by the CBB that the small amounts transferred by MVTS indicate a low level of TF risk, with confirmation being provided after the assessment team visited Bahrain that the CBB considers the risk to be high and that this is evidenced by consistency of understanding by the CBB and MVTS over the importance of scenario analysis of, for example, a single individual receiving small funds from several sources and a single individual continuously transferring small funds to several other individuals.

386. The CBB sees the highest risk of ML in the insurance sector as emanating from the life sector. The life sector is not large and few STRs are received. Although cash is accepted, life insurance premiums are small. The sector is seen as being more vulnerable to fraud than to ML, although little fraud has been seen in practice; ML risk is seen potentially arising from products requiring the payment of regular premiums and the payment of single premiums with an investment component to the policy. The use of brokers and agents is not seen as affecting the risk as insurance companies remain responsible for the AML/CFT measures undertaken for each customer relationship. The CBB considers that corporate governance in the insurance sector is good, with MLROs who understand their responsibilities, and that the sector understands the ML risks of its products. Kidnap and ransom insurance is available. It did not appear to the assessment team that particular consideration had been given by the CBB to the TF risks presented by the insurance sector.

387. The capital markets sector is very small with a daily trading volume of some USD 1 million representing a little over 40 trades. The greatest risk perceived by the CBB arises from the fact that brokers receive money from clients but the CBB sees the sector as low risk in light of the AML/CFT controls at banks and the requirement for brokers to have client accounts at banks, combined with restrictions on cash transactions and transactions with customers being undertaken through banks. It appeared to the assessment team that there was some reliance on controls by banks (notwithstanding requirements for capital markets participants to have AML/CFT countermeasures). The capital markets sector is not known to have been used for ML and/or TF.

388. With regard to individual FIs, the CBB has a good knowledge of FIs which have been subject to onsite inspection in more recent years and risk graded. It also has significant information about other FIs. Nevertheless, in the absence of a completed NRA and a comprehensive risk grading for all FIs, its knowledge of FIs cannot be fully developed.

### *DNFBPs*

389. The MOICT has prepared a DNFBPs risk assessment document. It is positive that the MOICT is seeking to conduct risk assessments and, while the current document is limited, it is a stepping stone for more in depth analysis. It has also prepared a basic document on the risk of auditors (based on face to face discussions with two firms and written input on draft legislation from large firms); this document focusses on the levels of qualified and unqualified audits. Potential indicators of ML (and therefore of ML risk) have also been issued in relation to DPMS. The MOICT is also informed by quantitative reviews of STRs and financial statements, together with high level reports from auditors on each DNFBP's systems for reporting suspicion and verification of identity at the time of the audit. The introduction of the statutory reporting process by the MOICT for auditors is commendable.

390. In addition, the MOICT has risk graded each DNFBP it supervises (see paragraph 410). Overall, the MOICT is aware of the AML/CFT standards of the sectors it supervises from onsite inspections and the auditors' reports, and it generally understands the ML risks of the sectors for which it has responsibility

albeit that it is in a less solid position than the CBB. Its knowledge of TF is developing.

391. Accountants and auditors are perceived as having low ML/TF risk on the basis of the requirements for experience and qualifications, restrictions on business, the quality of the audit reports reviewed by the MOICT and the inspections undertaken by the MOICT.

392. The risk of jewellers is seen as medium low by virtue of the requirement for gold sold by jewellers to be authenticated, the MOICT's discouragement of the use cash by DPMS, the inspection measures which are in place, the low number of STRs made by the sector, and the low number of DPMS. It is a moot point whether 350 DPMS is a small number, as the firms generate significant business value. It appears to the assessment team that the analysis would benefit from more in depth study as the NRA process develops.

393. Real estate companies are rated as medium risk in light of the size of the sector compared with other DNFBP sectors, the expansion of the sector and the opening of the property market to foreign investors. The Bahrain authorities also point to the establishment of the new regulatory framework and consequential risk mitigation to support their view.

394. Lawyers are considered to be low risk on the basis that they do not accept cash and do not feature in any intelligence, investigation or prosecution. In light of the absence of routine supervision and knowledge of lawyers in Bahrain, the analysis of risk should be re-examined. At this stage, the risks of individual legal practices are not known.

### *Risk-based supervision of compliance with AML/CFT requirements*

#### *Financial Institutions*

395. The CBB has put in place a framework with strong elements of a risk-based approach to supervision, albeit that the totality of the framework is not yet comprehensively risk based. The compliance directorate of the CBB, which is responsible for all onsite and offsite AML/CFT supervision, has 17 staff; 13 of these are engaged in AML/CFT. Members of the directorate were well versed in their responsibilities. While training has been provided, more systematic and regular training would be helpful. The CBB requires more resources in order to undertake comprehensive risk-based supervision.

396. The CBB has risk rated all FIs which have been subject to onsite inspections and special assignments since 2012 (special assignments being focussed, ad hoc, inspections, which arise as a result of offsite supervisory processes). The ratings of these FIs (including 27 banks) are based in part on a risk matrix and in part on other factors. The matrix includes reference to clients (individuals and legal persons); international and local PEPs; trade finance; geographic presence of the bank (and its branches and subsidiaries) and its customers; wire transfers; non-face to face business; introduced business; correspondent banking; wealth management and private banking; the IT system; the size and number of staff relative to the FI; and the quality and number of STRs. It is positive that the matrix is based on measures relevant to AML/CFT. The other factors include: cross-jurisdictional activity

(including total foreign liabilities and claims), size (including total exposures), interconnectedness (including assets, liabilities and funding ratios, complexity (including OTC derivatives, assets and trading book value and available for sale value); the results of previous inspections; and prudential matters such as internal and external audit reports, annual compliance reviews, relevant internal CBB memos and the history of enforcement action).

397. While the CBB has not risk rated a number of banks in a formal way, the banks it has subjected to onsite inspections (including special assignments) are those which it considers to present the greatest ML/TF risk. As noted above, the CBB receives and reviews substantial information to form the basis for this judgment. These 27 banks comprise 46% of the banking sector measured by total assets (with domestically systemically important banks (DSIBs)) alone comprising approximately 30% of total assets.) These banks also comprise 66% of all STRs received from the beginning of 2016 with the DSIBs comprising 59% of all STRs received during that period.

398. Only the first three ML/TF risk rating categories (i.e. high, medium high and medium low) have been used since 2012. More than half of the inspected entities have been rated as high risk, two FIs have been classified as medium low risk and none has been rated as low risk. This pattern of rating suggests that the model should be enhanced so as to allow a greater use of each rating and to allow a more differentiated approach in practice. This should include consideration of whether the risk matrix and other factors are excessively weighted towards size as a number of the elements measure the size of a FI in various ways or are more to do with prudential supervision rather than with AML/CFT supervision). The CBB has decided to appoint a consultancy firm to develop a more comprehensive matrix to inform its AML/CFT onsite and offsite supervision.

399. A risk rating is reviewed when a FI is subject to another onsite inspection (including special assignments).

400. The onsite inspection programme is formulated on an annual basis, using information considered during offsite supervision (see below), with the thematic reviews of the results of inspections already undertaken being a major factor (such reviews allowing the CBB in general to articulate themes which might be of importance and, in particular, to consider whether an issue at one FI might be relevant to another FI). The annual plan includes a combination of licensees not yet examined, licensees already inspected, licensees who have a poor STR record, licensees involved in an ongoing investigation, and one DSIB. While the plan is based on risk considerations, the programme cannot consider all relevant risk elements, as all licensees have not yet been formally risk rated (also see the comments above on the model). The assessment team notes that the approach in and arising from, the written materials provided by the CBB to the team needs to be enhanced to support the approach being applied in practice.

401. The CBB has carried out the following number of onsite inspections:

Table 32. **Inspections by the CBB**

| Year | Number of inspections to banks (of which special assignments) | Number of inspections to money changers (of which special assignments) | Number of inspections to insurers | Number of inspections to investment companies |
|---|---|---|---|---|
| **2012** | 8 (2) | 3 | 0 | 0 |
| **2013** | 8 (1) | 2 (1) | 2 | 0 |
| **2014** | 7 (1) | 9 (1) | 0 | 0 |
| **2015** | 6 | 4 (2) | 2 | 1 |
| **2016** | 7 (2) | 2 (1) | 1 | 0 |
| **2017** | 0 | 8 | 0 | 0 |

402. Most inspections undertaken are of banks and money changers, which is in line with the risks identified. DSIBs, which comprise a very large part of the banking sector, are subject to more frequent AML/CFT inspections than other FIs. Ad hoc, focussed inspections (special assignments) are carried out. Overall, relatively few onsite inspections are carried out in relation to the number and identified risk of licensees. For example, 27 banks have been subject to inspection since 2012. All licensees which present a concern during offsite supervision are inspected soon afterwards or are subject to other tools used by the CBB such as the appointment of external auditors or onsite inspections by the sectoral supervisory directorates to address its concern.

403. More generally for FIs as a whole, during inspections there is more focus on areas of risk identified in the CBB rulebook and those identified by the FI. The CBB recognises that a different approach is needed for different sectors, different parts of each sector and different products/services with, for example, wealth management and retail banking being subject to different approaches. Higher risk FIs are subject to greater sampling of customer files, greater analysis of their risk assessments and monitoring systems and a greater number of interviews of staff.

404. Inspections take approximately two weeks, with four/five staff for a large FI and two/three staff for a small FI. Customer files are reviewed during inspections. The conduct of inspections is guided by a series of templates structured as spreadsheets. The post inspection reports, case studies provided by the CBB and the assessment team's interviews with the CBB (together with the time taken for the inspections) indicate that inspections are generally much more in depth and comprehensive than is suggested by the templates. However, the combination of the material received and the TFS case mentioned in IO.10 indicates that there should be more focus on CFT (and its risks) in the round and also the FI's overall assessment and mitigation of ML/TF risk.

405. A significant level of offsite information is received and offsite supervision undertaken (see the following paragraphs). Risks and issues raised in offsite processes inform the onsite supervision programme and use of other supervisory tools such as additional meetings and special assignments.

406. Annual external AML/CFT audits are required of all FIs. There would be merit in enhancing the scope of the audits in relation to risk identification,

assessment and mitigation and CFT. The external audit reports are complemented by the annual thematic reviews of inspections undertaken by the CBB in the year under review in order to facilitate its understanding of ML/TF risks. These reviews contain recommendations for future areas of focus. The reviews are commendable but the assessment team is cautious as to what extent the analysis and conclusions can be substantiated for sectors which have no or few inspected representatives in that calendar year. In addition, the CBB receives annual internal audit reports from each FI, together with an annual compliance review by the MLRO. The CBB also collects information from banks on a quarterly basis on the nationality of depositors and their geographic region and currency, and uses this information to analyse trends in the private sector and inform its understanding of risk.

407. Each FI's STRs are reviewed upon receipt and the CBB compiles quarterly reports with a quantitative description of the pattern of STRs in the quarter. Consideration of individual STRs has led to special assignments. The CBB meets routinely with licensees at least once a year (sometimes much more frequently depending on risks). AML/CFT onsite and offsite supervision is complemented by information provided to the compliance directorate by the supervisory directorates. The compliance directorate maintains close links with the sectoral supervisory directorates so as to be informed and provide input if matters relevant to AML/CFT arise. FIs are prioritised for an AML/CFT inspection if weak controls are identified by the supervision teams during their inspections, or if public information or information received from whistle blowers indicates an inspection is needed. Special assignments have also been carried out on the basis of information received from other authorities such as the FID and Customs. An enhancement of the CBB's approach to thematic reviews so that all offsite supervisory information is analysed by sector so as to more comprehensively drive risk-based supervision would be a very powerful tool - it is already proposed to enhance the thematic reviews so that they take greater account of an FI's controls. As part of this, analysis of the reasons for the annual pattern and quality of STRs would be beneficial.

408. The assessment team has a concern that there have been circumstances where offsite supervision has not been sufficiently proactive. This arises from the TFS case study mentioned in IO10. Nevertheless, while The IT system which contributed to the failing mentioned in the case study is common to several banks in Bahrain, the CBB strongly believes that the IT issue was attributable to the implementation of the system by the bank referred to in the case. This is on the basis that other banks with the same system were subject to inspection and a similar deficiency was not identified.

### *DNFBPs*

409. Reflecting a considerable increase in staff resources in the last year, the MOICT has been able to put in place a framework for a largely risk-based approach to supervision albeit that the assessment team does not consider the totality of it to be comprehensive. The MOICT has a dedicated AML/CFT unit of four staff (there being only one member of staff in October 2016 and the increases made in stages). Nevertheless, this is still a shortfall in the resources necessary for the unit to undertake its responsibilities and the MOICT has therefore endeavoured to maximise its use of IT. Steps are being taken to remedy the shortfall. New staff are subject to an in-house training programme lasting more than two weeks.

Subsequent to this, training is provided when there are changes to the AML/CFT regime or when appropriate external training is held. There would be merit in the establishment of a systematic ongoing training programme.

410. The MOICT has risk graded each DNFBP it supervises into one of five categories using its market share and capital investment, which can be derived from their financial statements, together with other CR data, auditors' reports (see above), the results of previous inspections, and STRs received (see footnote[4]). It appears to the assessment team that the risk rating model mostly comprises ML/TF risk based elements and a small minority of elements which the assessment team is not persuaded have much or any AML/CFT value. Risk ratings of each DNFBP are conducted annually and also at the time of onsite inspections.

411. There are annual onsite inspection plans. The decision on which inspections to undertake is based on the risk rating, the reports from auditors and STRs. In practice, this leads to all DNFBPs in each risk category being visited in sequence, commencing with high risk entities. All four members of staff participate in inspections; two days onsite is typical for a firm of auditors while half a day would be usual for a jeweller. Offsite supervisory information informs the content of inspections. High risk entities are subject to more than one inspection a year and to longer inspections than other businesses, with more customer files being reviewed. Supervision of real estate brokers structured as companies ceased a few months prior to the assessment team assessment team's visit to Bahrain in light of the enactment of legislation for the new supervisory authority, RERA/SLRB.

412. The number of inspections is as follows:

Table 33. **Number of Inspections by the MOICT**

| Sector | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 |
|---|---|---|---|---|---|---|
| **Accountants and auditors** | 0 | 0 | 0 | 0 | 0 | 10 |
| **DPMS** | 2 | 4 | 33 | 30 | 64 | 101 |
| **Real estate sector** | 0 | 0 | 0 | 5 | 15 | 13 |
| Total | **2** | **4** | **33** | **35 plus 24 ad hoc** | **79 plus 17 ad hoc** | **124 plus 15 ad hoc** |

413. The number of inspections has increased as the MOICT has increased the resources devoted to AML/CFT. The conduct of inspections is guided by a template methodology. This document would benefit from more detail, including additional focus on risk identification, assessment and mitigation at both the business and customer levels; verification of identity and TF. It would also be helpful for more narrative to be included as the document is completed so as to provide information which the MOICT can use in its own risk assessment, informs risk-based supervision,

[4] Registered area, owner nationality, legal type, currency and value of capital, compliance officer experience, compliance officer age group, asset base, audit report opinion, previously reported violations among others.

substantiates any enforcement action and also demonstrate the depth and intensity of the inspections and the quantum of any problems found.

414. With regard to offsite supervision, the MOICT reviews STRs upon receipt, including checking its registry databases. Financial statements of individual businesses are broken down by sector and reviewed. Comparisons are made with sector averages and outliers are investigated. The ownership information in the statements is also considered. In addition, the MOICT has recently begun to require provision to it of copies of businesses' procedures for review. The overall approach is not comprehensively articulated in writing and the completion of the NRA will allow the MOICT both to enhance its approach and better articulate it.

415. AML/CFT supervision of other DNFBPS does not yet take place but is proposed. The legislation framework for lawyers and notaries was strengthened while the assessment team was in Bahrain and the MOJ estimates that it will need five additional staff. Further, as legislation has also been amended at the time of the visit to Bahrain to allow the entry of private notaries, the MOJ would need to enhance its capacity to effectively supervise the sector. The RERA/SLRB has been established to supervise all aspects of real estate brokers (both individuals and companies). Legislation has been enacted and it is apparent that the intention is to ensure that the RERA/SLRB has sufficient staff of the right quality to ensure that it meets its responsibilities.

### *Remedial actions and effective, proportionate, and dissuasive sanctions*

#### ***Financial Institutions***

416. The CBB's inspection reports require remedial actions to be undertaken and FIs to provide a formal response to the reports, including an action plan. Where severe deficiencies have been found during an inspection, the CBB conducts follow up inspections within six months (or more depending on the severity of the issues identified). In addition, all licensees are subject to an offsite review within12 months of the inspection to consider progress by the FI in undertaking the remedial actions; remedial actions are monitored by correspondence and the CBB has also required remediation reports by external auditors or the MLRO have also been required from some FIs.

417. Sanctions are imposed by an enforcement committee. The table below specifies the sanctions arising from AML/CFT violations imposed by the CBB between 2012 and 2016:

Table 34**. Sanctions imposed by the CBB**

| Institution Type | Year | Violation | No. of months from discovery of issue to application of penalty | Enforcement |
|---|---|---|---|---|
| **Specialised licensee-money changer** | 2013 | Facilitation and processing of transactions for illegal movement of cash across the borders, failures in CDD and other requirements, and failure to provide documentation required by the investigation team. | Investigation conducted in December 2013 and January 2014. Sanctions imposed in November 2015 following final court verdict. | CBB administrative penalty of 20 000 ((Euro 43 115); CBB penalty of BHD 200 000 (Euro 431 077); Requirement by the CBB to remove MLRO and management (11 individuals) following court verdict; termination by the CBB of import and export of currency (notes); Court order for the confiscation of BHD 2 million (Euro 4.3 million). |
| **Specialised licensee - money changer** | 2013 | High volume of cash transactions processed without completing AML/CFT procedures and failure to be suspicious. | Issues were discovered in December 2013. Sanctions imposed in March 2014. | CBB financial penalty of BHD 20 000 (Euro 43 115); requirement by the CBB to remove MLRO, general manager and branch manager; termination by the CBB of import and export of currency (notes). |
| **Conventional bank** | 2015 | Bank currently under administration. | Under administration. | Bank put into administration by the CBB. |
| **Islamic retail bank** | 2017 | Refer to the case study in IO10. | | Formal warning. |
| **Specialised licensee - money changer*** | 2017 | Promotion and provision of regulated services without a licence | Issue reported in February 2017 and the financial penalty was imposed in May 2017. | CBB financial penalty of BHD 20 000 (Euro 43 286). |
| **Conventional retail bank** | 2017 | Bank in breach of freezing of fund requirements and release of funds. | Issue discovered in February 2017. Penalty imposed in March 2017. | CBB financial penalty of BHD 20 000 (Euro 43 115). |

*Note:* *This single case resulted into seven separate sanctions of BHD 20 000 (Euro 43 286) each against seven entities involving promotion and provision of regulated services without a licence.

418. Sanctions have been applied in particular to money changers; only five banks have been the subject of penalties. Relatively few sanctions have been imposed since 2012 and, of these, a small number relates to breaches of ML/TF counter-measures required of FIs (as opposed to, for example, breaches of wider requirements relevant to AML/CFT such as licensing requirements). In two cases sanctions imposed on FIs requiring them to remove individuals from their posts but no such penalties have been imposed since 2014. Sanctions are not published. The case study mentioned in IO.10 raises concern that the system for applying sanctions is

not robust. Overall, the CBB has the appetite to apply sanctions and it has imposed a range of sanctions and made referrals for prosecution (see the text above on prevention of criminals from entering the market); there is scope to apply further sanctions as the number of onsite inspections increases.

### *DNFBPs*

419. The MOICT is willing to impose sanctions and make referrals for prosecution. It has referred cases for prosecution since 2012 as follows: 2012: 9; 2013: 3; 2014: 4; 2015:3; 2016: 7; 2017:21. These referrals derive from the entirety of the CR database and are mostly for fraud of various kinds, particularly forged documents. Sixteen of the cases involved DNFBPs (real estate brokers) but none of these appear to have involved AML/CFT issues. It is not clear to the assessment team whether the prosecutions resulted in convictions.

420. Within the period under review, the MOICT has suspended the registration of an audit firm for non-compliance with UNSCR requirements and removed a real estate broker from the register due to a failure to provide it with information relevant to AML within a specified time frame. In addition, the MOICT has advised that, in 2016 and 2017, 210 gold dealers and 9 auditors were suspended from the register because of a failure to notify or routinely update the MOICT of the appointment of an AML/CFT compliance officer; 38 of these registrations (all gold dealers) are still in suspension due to a continuing failure to appoint a compliance officer. Suspension of registration has the consequence of preventing a firm from being able to undertake business but there would nevertheless be merit in the MOICT reviewing whether it should revoke suspended licences within the three years permitted for suspension. The MOICT has required all of the DNFBPs which applied for reinstatement on the register to pay an administrative penalty of between BHD 110 and BHD 830 depending on the length of the suspension.

421. During the period under review, The MOJ has applied penalties in connection with failings in registration requirements, including convictions (of which there have been two, one in relation to drugs offences and one in relation to kidnapping and assault). It has sought disciplinary measures in 74 cases since 2012. A range of measures has been applied, including warnings, blame (a more serious form of warning), and suspension and revocation of registration. The MOJ appears to be proactive in seeking sanctions. However, 26 of the 74 cases brought have been rejected by the disciplinary committee of judges and lawyers appointed in each case by the MOJ and of the remaining 48 cases, 7 cases were lost on appeal and on 6 occasions the sanction proposed was reduced on appeal. The MOJ is of the view that this pattern of application, rejection, appeal and reduction of sanction is satisfactory and accounted for by the judicial-like burden of proof and the neutrality and independence of the process. The MOJ has advised that it takes some two to three months between receipt of information on an issue and the application of a penalty.

422. The MOJ provided two examples of sanctions cases with regard to breach of notarial duties; these were the issue of a verbal warning in 2014 while the second case, in 2015, led to the resignation and early retirement of two individuals.

### *Impact of supervisory actions on compliance*

#### *Financial Institutions*

423. The CBB has noted an improvement in the compliance culture of, and understanding of risk by, FIs since 2012. The quality of STRs has also improved. The more frequent onsite inspections of DSIBs have led to a gradual but steady improvement of their AML/CFT compliance. Some FIs have adopted more stringent measures than that required by supervisory enforcement after inspections. In addition, the CBB has indicated that its placing of two FIs under its administration in 2015 is known to FIs, has emphasised the importance of AML/CFT compliance and has made them more cautious.

#### *DNFBPs*

424. The MOICT has noted improvement in the compliance culture of DNFBPs through its onsite inspections, review of their procedures, auditors' reports on AML/CFT and STRs made to it. It regards its social media awareness programme and mobile app as important in improving CDD, The assessment team also notes that the MOICT has struck off a significant number of DNFBPs which had not appointed a MLRO, thus removing DNFBPs with poor compliance culture from the system.

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

#### *Financial Institutions and DNFBPs*

425. The CBB and the MOICT have conducted outreach.

426. Except in one respect, the CBB financial crime modules contain limited guidance, though there are other ways in which the CBB provides guidance to its regulated entities. In addition, each of the modules includes a section entitled "AML/CFT Guidance and Best Practice", which refers to guidance produced by international bodies and their websites. The one exception referred to is an appendix comprising guidelines on detecting suspicious transactions. In addition, the CBB disseminates information each month via its website on types of, and trends in relation to, suspicious transactions.

427. The CBB also works annually with the Bahrain Institute of Banking and Finance on the provision of AML/CFT related training courses. Seminars have included trade finance, correspondent banking, introduced business, high risk customers, internal controls and risk assessment. They appear to be well attended by representatives of the banking and insurance sectors in particular.

428. The annual reviews by external auditors and onsite inspections by the CBB also promote understanding. The CBB also holds bilateral monthly, quarterly or annual and ad hoc meetings with licensees. These have covered AML/CFT compliance issues such as sanctions, identification and verification of identity, beneficial ownership, PEPs and STRs, as well as providing responses to questions. The CBB also responds on a daily basis to queries directed to it by FIs. In addition, the CBB meets with the banking association on an annual basis and conducts outreach to explain new standards when they are issued.

429. Turning to ad hoc outreach, information was provided to the banking sector on the subject matter and outcomes of a major international governmental conference held in Bahrain in 2015. Amongst other matters, this event addressed TF, particularly ISIL issues. The event was also attended by some bank CEOs. The questionnaires provided by the CBB to licensees for their input for the NRA are regarded as part of the overall programme to promote understanding of risk.

430. The CBB intends to consider the NRA when it has been completed and has already decided to issue guidance on trade based ML and FinTech.

431. The MOICT has provided some information to assist DNFBPs, particularly focussing on suspicion. It has made its risk assessments public although the assessment in relation to auditors has been redacted as it included firm-specific information. It has also participated in events for each of the sectors which it supervises and issues circulars on matters such as the filing of STRs, STR trends and the introduction of new standards. Onsite inspections and emails are also used to increase understanding of STRs. The Ministry's website contains general information on the existence of the AML/CFT framework, and some information on suspicion and how and where to make STRs. Social media are also used to promote understanding of AML/CFT. The MOICT does not receive many queries but responds to those it does receive (from compliance officers).

432. The MOJ conducted outreach in 2008 and proposes to undertake briefings to lawyers before the end of 2017 and in 2018 in light of the new legislation.

### *Overall conclusions on IO.3*

433. **Bahrain is rated as having a substantial level of effectiveness for IO.3.**

# CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS

## Key Findings and Recommended Actions

### Key Findings

**Bahrain achieved a moderate level of effectiveness for IO.5.**

1. Information on the creation and types of legal persons such as companies is publicly available in Bahrain. Information on the creation and types of legal arrangements is publicly available, considering the provisions contained in the Trust Law and the CBB Law, for trusts, and in the Ministerial Order 03/2017, as well as the Shari'a Courts, for waqfs.
2. Bahrain is yet to conduct a comprehensive assessment of the ML/TF risks posed by legal persons created in the country.
3. Bahrain has a centralised registry for companies, partnerships and individual establishments (Sijilat system). Basic and legal ownership information is accurately and adequately kept. The registry is frequently updated, searchable on different parameters, and available without a fee. The development in this area is commendable.
4. The registry includes information on authorised signatories, board of directors and shareholders. The registry also separately captures names of all shareholders who own 5% and above in company shares as well as names of ultimate natural person who is the beneficial owner of the shares (however it lacks reference to those who may control a legal person through means other than ownership). The beneficial ownership is relatively easily traced through the Sijilat system where no foreign ownership or control is involved.
5. Sanctions applied for failure to comply with obligations do not seem fully effective or dissuasive.
6. MOICT has a dual role in Bahrain's AML/CFT regime: as DNFBP supervisor and as registrar of legal persons and needs further resources to fulfil its mandate effectively.

### Recommended Actions

1. Bahrain should do a comprehensive analysis of the ML/TF vulnerabilities of all its legal persons. All competent authorities, including FID, PPO, and CBB should feed into this risk assessment. Bahrain should also review the existing mechanism for preventing the potential abuse of waqfs for ML/TF and apply additional measures as appropriate.
2. Bahrain should further ensure that beneficial information in respect of legal persons registered in Sijilat is accurate.
3. Bahrain should review the existing sanction regime and apply effective

and dissuasive sanctions in case of violations observed.

4. In line with the recommended actions under IO.3 and to further develop its role as Registrar from an AML/CFT perspective, the MOICT should be adequately staffed.

434. 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.[5]

## *Immediate Outcome 5 (Legal Persons and Arrangements)*

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

435. Information on the creation and types of legal persons, such as companies, is publicly available. It is contained in the Commercial Companies Law and in the Sijilat system, which is the online central register for companies in Bahrain. Legal persons which include Bahrain shareholding companies, single person companies and foreign companies can be identified through searches by the Commercial Registration (CR) number, name or activity. As of October 2017, there were 769 foreign companies, mostly owned by Indians (nearly 31% of all foreign companies, as reported by authorities). Information on the total number of legal persons registered in Bahrain is available in Chapter 1. The registry includes legal person's name, address, contact details, invested capital, details of board of directors, shareholders/partners and authorised signatories. The same information is also available through a MOICT mobile application which is available free of charge. There are no specific company formation agents in Bahrain, nor is it mandatory to appoint them to complete the registration process. In practice this service is often provided by lawyers.

436. Other types of legal persons include associations, cultural clubs and other NPOs governed by Law Decree No. (21) 1989 and whose details are provided under R.8. Bahrain does not have foundations.

437. The requirements for the creation of trusts are publicly available, as Bahraini trusts must be registered with the CBB. The registry of trusts is maintained in the trust registry office within the CBB. Information contained by the registry follows the same rules of confidentiality that apply to banking and financial products but is available to competent authorities, through the CBB's inspection powers or a court order, if needed.

438. There are three trust service providers in Bahrain, which are part of international groups specialised in trust formation services. 43 trusts were

[5] 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.

registered as of November 2017. Both Bahraini and foreign trusts are subject to scrutiny when entering in a business relationship with a FI or DNFBP.

439. The actual owner of the assets (which often also acts as settlors) and their beneficiaries are not only known to the trustee, but also to the CBB, as their details are provided for in the trust instrument, and is submitted to the CBB as part of the registration process. Any amendments to the instrument must also be submitted to the CBB. The settlors and beneficiaries can be residents or non-residents. The trustee is responsible to perform CDD checks on settlors and beneficiaries as part of its obligations under Trusts laws as well as FC module.

440. As regards other legal arrangements, Bahrain has waqfs, which are an Islamic type of legal arrangement regulated by Shari'a and particularly through MO No. 3 of 2017, which includes the procedures for waqf creation. Information regarding the creation and formation of waqfs is also available in the Shari'a Courts, where the deed of a waqf needs to be registered to be valid and it is overseen by the MOJ. Waqfs are legal arrangements where property or money can be kept in favour of (endowed to) the public or a particular individual, for a permanent period (normally a lifetime).

441. There are three types of waqf in Bahrain, depending on how the waqf is set[6] and there are currently 1681 waqfs in Bahrain. Authorities stressed that the waqf councils execute the terms of the waqf, together with administrator (s) of the waqf (the nather). There is an agreement that obliges the administrator to open a bank account for the waqf and biannually submit reports of income and expenses and audited financial statements to the council annually. The administrator of the waqf manages the waqf and must apply to the waqf council if there is a requirement to spend monies outside the day to day expenses of the waqf. All government departments, such as water, electricity, public works and the municipalities require the approval of the waqf council before conducting any transaction. These measures are in place to secure the waqf's money and not necessarily for countering ML/TF; however, they do provide a sense of control measures in place.

442. The assessment team was not able to obtain information on the exact amount of assets held under waqf, nor on the distinction between the assets associated with individuals or entities inside or outside Bahrain; however Bahrain noted that most of Bahrain's waqfs are real estate. Also, there is no available information on other preventive measures that are pursued to combat ML/TF through waqfs.

6 Charity waqf: The waqif (donator) allocates money that he owns for the benefit of a public or charitable entity such as charitable institutions. Family waqf: The waqif (donator) allocates money that he owns in favour of his own children according to the criteria stipulated by the waqf in the waqf document, such as identifying the classes of beneficiaries from the waqf (i.e. for instance all the sons of a father). Joint waqf: The waqif (donator) divides the waqf money in favour of a charity as well as for the benefit of his family.

### *Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal entities*

443. There has been no comprehensive risk assessment of the ML/TF vulnerability of legal entities created in Bahrain nor was any analysis included as part of Bahrain's draft NRA, except for a brief mention of concerns with regard to the use of consultancy firms, for laundering criminal proceeds. Bahrain presented a report containing statistical analysis of activity type, capital base and number of legal entities registered under different categories. However, Bahrain has not comprehensively assessed ML/TF risks of all categories of legal persons. One ML case involving a company (See Box 1 in IO.7 and several investigations regarding companies in IO.2) was presented to the assessment team which showed misuse of legal persons being effectively tackled by Bahrain. Bahrain should develop a more thorough understanding of vulnerabilities and potential of abuse of legal persons for ML/TF. This should, for example, include multi-agency information sources, such as FID, CBB, PPO, other law enforcement agencies and MOICT, to identify any trends and patterns.

444. Trust activities in Bahrain are assessed in Bahrain's draft NRA to be of low risk due to high level of beneficiary transparency, small number of licensees, registration and regulatory framework, and relatively low levels of activities in Bahrain. This risk rating by authorities seems consistent with the nascence of trusts and with registration processes thereof in Bahrain.

445. NPO risks as legal entities and their mitigation are considered under IO.10.

### *Mitigating measures to prevent the misuse of legal persons and arrangements*

446. As a starting point, there are mitigating measures in place to ensure transparency of legal persons and arrangements in Bahrain. For example, it is mandatory to open a bank account with a Bahraini bank before completing company registration (which entails a separate CDD process by FIs where for instance, beneficial owners of the company are identified). Memorandum and Articles of Association are required to be notarised by applicants before registration. Further, a national standardised electronic identification system has been in place since 2005, as part of a move by the Government to provide more services online (eGovernment). The "Information and eGovernment Authority" established an identification system (SmartCard) for all citizens including, new borns, non-Bahraini residents, and visitors. This SmartCard (for all directors and authorised signatories) is required to register companies in the Sijilat system, and facilitates gathering information from a trustworthy source.

447. All legal persons operating in Bahrain (including Bahraini companies, foreign companies and individual establishments) require Sijilat registration. Applicants are subject to several requirements, including a letter from the MOJ (that no criminal matters are pending or no criminal convictions), and screening against the security checks of MOI. The MOICT has a built in blacklist in the Sijilat system, where all individuals and organisations listed in the United Nations are included, in addition to any local individual or organisation which is subject to domestic listing. Those who are listed will not be able to register or own or transfer ownership of any kind and can only access the public search function in the system.

448. The MOICT also reviews and assesses the legal persons' financial statements to properly identify the nature and size of the business for which it determines a set of indicators. Subsequent abnormal and/or significant results are deemed suspicious and are therefore subject to further assessment. The assessment mechanism includes reviewing each sector's income specifically cash income, and the assets. This is compared to the industry average, to identify trends and patterns. Cases were presented to the assessment team where companies were misused and the inspections conducted by the MOICT and the FID, were helpful in identifying criminal activity (See for instance, Box 1 in IO.7 and Box 13 under IO.2).

449. As noted above, Bahrain's draft NRA noted concerns with regard to the use of companies, and in particular, consultancy firms, for laundering criminal proceeds.

450. The assessment team received information on actions being taken by Bahrain to prevent the misuse of shelf companies. Funds related to a company which is considered active but with no specific license (from other Ministries or CBB) or activity, cannot be deposited in its corresponding corporate bank account, until a business license has been granted, for which the MOICT could and has in the past enquired on the source of funds, where the business history of the individual and economic capability do not seem to match (See Box 9 below).

**Box 9. MOICT diligence with regard to company activity in Bahrain**
(November 2017-Ongoing)

The MOICT AML/CFT Compliance Department provides monthly reports to its senior management and escalates any unusual situations. As part of its monthly reports, an increase in capital was noticed which did not seem to match the business history and profile of the investor of the company. It was also consistent with the industry's average share capital.

The department conducted enquiries and noted that one of the partners in the company had invested a significant amount of money in the company with no-business history which could justify the assets. Enquiries also found that a second partner with a significant investment was the CEO of another company whose liabilities far exceeded its assets. MOICT enquiries also noted that the initial capital proposed for the company was not commensurate with the proposed activity (no license had been requested at the time).

Actions taken by MOICT following its enquiries: i) The MOICT placed the company under monitoring and noted that whenever it applies for a license, the shareholders will be asked for source of funds (The MOICT noted there could have been a mistake in typing the amounts in the Sijilat system, when applying to increase capital, thereby resulting in a misleading amount); ii) The MOICT notified the FID of the attempt in increasing capital, although the licensing process was not completed; iii) Any final results will be escalated for further actions.

451. The Sijilat system is a live system, which is also capable of detecting any variations in the information submitted by companies (i.e. increase in shares,

transfers of ownership) and to also compare results, against the industry average. In case of any variations, an alert is triggered and is subsequently sent to the concerned department for further investigation. Where the primary finding does not justify the business purpose of the behaviour that generated the alert, in-depth investigation is conducted to determine whether such behaviour is associated with ML/TF risks (See Box 9 above).

452. For trusts, as mentioned earlier all trust services providers are licensed and supervised by the CBB. Further there were a limited number of trusts in existence in Bahrain at the time of the evaluation. Authorities stated that no violations took place with regards to trust service providers.

453. Waqfs would be supervised by the Waqf Council (MOJ) or a nather (person appointed by the waqif for supervising the waqf), to identify any misuse of this legal arrangement. Supervision tasks would mostly relate to ensuring that the terms (purpose) of the waqf are fulfilled, rather than protecting it from ML/TF misuse. However, authorities noted and the assessment team agrees that the possibility of a waqf being misused for ML purposes is largely mitigated by the fact that once established, the waqf cannot be cancelled, and it would not be an efficient method for disguising illegal origins of a given property. In terms of context, there are currently 1 681 waqfs in Bahrain. While the sector does not seem to pose significant ML/TF risk and no cases of their abuse have emerged, further vigilance should be in place to curb any potential misuse in ML/TF.

454. As explained above, there are a number of measures in place to prevent the misuse of legal persons and arrangements in Bahrain from a supervisory and enforcement point of view. Moreover, even though there is no explicit bar against nominee directors or shareholders, authorities insist that the use of nominees and bearer shares are not allowed in Bahrain as there are no explicit provisions that would enable their existence. Bahrain is active in international co-operation, and has exchanged useful information in this area, which also mitigates the risks to some extent.

455. However, resourcing of the MOICT, which holds both a registrar and a supervisory function (See Chapter 1 and IO.3), is a cause of concern. The MOICT currently has four staff members (in its Compliance Department), but given the volume of companies and MOICT's dual role, the resources don't seem adequate. MOICT's resources need to be enhanced to enable it to effectively perform its dual role.

### *Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons*

456. Basic ownership information of all legal persons is publicly available on Sijilat. Any changes to ownership is available real-time, as all amendments made are required to be reported to the MOICT through the Sijilat system and reflected immediately.

457. Furthermore, accurate ownership information is obtained by the Registry, through Smartcards and is verified with information available from the Labour and Migration Regulatory Authority information website and other ministries. Given the interrelatedness of the information available and the procedures implemented by

government entities, natural persons engaging in any commercial activity are required to submit their identity card ("ID"). Subsequently, relevant authorities and other institutions access the information of the ID holder through inserting it in the smartcard reader.

458. Changes in ownership are tracked and automatically updated in Sijilat. The total number of legal ownership transfers amounted to 143 between 2015 and 31st July 2017 (all in Bahraini owned companies). Information maintained in Sijilat is considered accurate and up to date as any change in ownership must be authorised by MOICT, and will not take effect without endorsement along with the approval of licensing authority (CBB or other Ministries involved) if any.

459. Beneficial ownership information of Bahraini owned companies can be easily traced following the chains of ownership in the Sijilat system and enquiries done by MOICT on the ownership makes sense from a business profile and resources point of view (See Box 9). In addition, Ministerial Order 19 of 2017 (Bahrain's Corporate Governance Code) mandates all companies (Bahraini or foreign) to disclose break down of their ownership details to the MOICT. These include ownership structure broken down by nationalities of the owners, names of all shareholders who own 5% and above in company shares as well as names of ultimate natural person who is the beneficial owner of the shares. Prior to the 2017 amendment, the MOICT was using its powers under the Commercial Registrar Law of 2015 and the 2010 Corporate Governance Code to obtain this information from companies, which is available to the MOICT through privileged access in the Sijilat system. However it only covers those who own shares, and lacks reference to those who may control a legal person through means other than ownership.

460. The assessment team could not clearly establish whether authorities have effective measures to ensure that BO information is available for foreign owned Bahraini company. MOICT stated that it can identify the structure and the individual behind that company, via analysis of financial statements and constitutive documents as well as these requirements to disclose names of beneficial owners. The MOICT would normally also communicate with foreign authorities, in such cases but it seems this is only carried out when needed and not on a routine basis.

461. Law enforcement authorities noted that information available through Sijilat has been useful in their investigations and also noted they have a good relationship with the MOICT, which is able to submit what is already available through Sijilat in a formal document, to be used in Courts (See Box 1 under IO.7 and Box 11 and 12 in IO.2). For example, the FID noted it managed to spot the creation of shell companies with an attempt to hide the proceeds of illegal work permits through information provided by MOICT (see Box 10 below).

462. Additionally, authorities also have access to beneficial ownership information through financial institutions and DNFBPs, which have an independent obligation to collect this information as part of customer on-boarding processes. In practice, law enforcement authorities access basic and beneficial ownership information through the Sijilat system and were positive about the output.

463. While Sijilat system has strong features, there are some concerns by the assessment team that Bahraini companies could still be misused by informal nominees or straw persons (where the legal owners or directors are not the actual

beneficial owners or controllers with a view to hide their identity). While the Sijilat system is capable of capturing ownership details, it would not amount to beneficial ownership information in such cases or where control is exercised through other means. A comprehensive ML/TF risk assessment of business structures in Bahrain would help the authorities to identify their vulnerabilities for such abuse.

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

464. Information related to waqfs is available through a court order in the Sharia Courts and waqfs councils, which supervise and manage waqfs to preserve their state. With regard to trusts, authorities have access, upon request, to all information relating to trust service providers, available in the CBB and general information has been shared with other authorities, including abroad. Authorities presented a request received from a foreign jurisdiction regarding a trust licenced by the CBB, which was seeking to acquire ownership rights in a licenced institution in that foreign jurisdiction and for which the CBB noted prior approval was required. No specific instances of abuse of trusts had come to the notice of authorities thus far.

**Box 10. Example of ML case where Sijilat was used to identify the ultimate ownership of a legal person** (2016-ongoing)

During 2016, information was received regarding the illegal trade of work permits by "Z", in violation of Bahraini human trafficking laws – a predicate offence of ML. An investigation was launched by the FID in collaboration with the competent LEA (Anti-human trafficking Directorate). Investigations revealed that the perpetrator had used his and other names to establish shell companies to sell the work permits of those shell companies to expats who purchased those "work visas" to enter Bahrain. The Sijilat system was used to identify all the companies associated with the perpetrator, connecting different data elements, among different company registration numbers. The Sijilat system further aided investigations to identify all companies related to the perpetrator, through details related to shareholders and associates. The funds generated from this act were seized and the case was forwarded to PPO for potential ML and human trafficking violations.

### *Effectiveness, proportionality and dissuasiveness of sanctions*

465. Sanctions are available for persons who fail to comply with the requirements of the Commercial Companies Law; imprisonment and a fine between BHD 5 000 and 10 000 (approximately EUR 11 000 to 22 000), for breaches such as providing false information in the memorandum of association (Art. 361 and 362 of the Commercial Companies Law) and a fine of 5 000 for other types of less serious breaches. This may not be sufficiently dissuasive for large companies.

466. The MOICT used its sanctioning power for not updating the required information in a timely manner, 1803 times during 2015-17. However, it noted that 60% of these sanctions were revoked due to the submission of the information required subsequently, before the renewal of company's registration. The failure to

submit the necessary information would also have resulted in the automatic suspension or the deletion of the CR on its maturity date.

467. At the initial application stage, the MOICT has rejected a number of applications due to variety of reasons (mostly non-AML related). In total, MOICT rejected 2244 applications regarding obtaining a license, adding an additional activity, and other requests, during the same sample period (2015-17). Rejections were due to multiple reasons, such as other licensing authority's rejection (i.e. if a restaurant, would need health license) and municipality rejection to the proposed location etc.

468. The MOICT stated that in case of material misstatements in the information submitted during the creation of the legal persons, the case will be sent to the PPO and this has been done in many instances, as noted in the table below. Reports below were made following a ML suspicion; upon the discovery of forged financial statements and for practicing a business without the specific license, among others. The assessment team was not notified of any sanctions applied in the trust and services providers sector. With regard to waqfs, six applications were made to the Sharia courts for mismanagement and four Nathers were replaced.

Table 35. **Number of cases referred to the PPO by MOICT**

| Year | Number |
|---|---|
| **2012** | 9 |
| **2013** | 3 |
| **2014** | 4 |
| **2015** | 3 |
| **2016** | 7 |
| **2017** | 21 |

## *Overall conclusions on IO.5*

469. **Bahrain 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

**Bahrain achieved a substantial level of effectiveness for IO.2.**

1. International co-operation is an important element for Bahrain, given its role as a financial and business centre. For example, Bahrain sends and responds to MLA requests for both ML and predicate offences and uses informal co-operation mechanisms for a variety of purposes. Formal bilateral agreements are signed at the request of counterparts, although no agreements or MOUs are required under Bahraini law to provide MLA or exchange information.
2. Bahrain takes a collaborative approach towards requests and it has not refused an international co-operation request because of a lack of reciprocity, but has worked with other authorities to find the most efficient means to provide co-operation.
3. The number of outgoing MLA requests is not fully in line with the ML/TF risk profile of Bahrain. However, the FID exchanges information related to ML/TF via the Egmont Secure Web, including beneficial ownership information with regard to Bahraini owned companies. The FID is very active on outgoing exchange of information requests particularly for ML cases. The CBB has the authority to, and has exchanged supervisory information with its international counterparts when relevant to AML/CFT.
4. Authorities have used MLA and Interpol channels in ML cases. For TF, Bahrain does not regularly utilise MLA to investigate TF. The lack of use of MLA for TF investigations is partly explained by a preference for other informal mechanisms, considering that intelligence and national security channels normally deal with terrorist and TF related threats and seek to cooperate informally.
5. With regard to extradition, authorities frequently use Interpol for facilitation. The average time for processing both MLA and extradition requests is variable, but requests have been generally addressed in a timely manner.
6. Bahrain lacked a system to ensure the timeliness of responses to MLA and extradition requests at the time of on-site visit, but developed one using existing data and systems, in April 2018. Statistics regarding assistance and co-operation provided were incomplete.

### Recommended Actions

Bahrain should:

1. Utilise the recently enhanced case management system which provides alerts and

reminders to speed-up responses and to adequately prioritise MLA requests.

2. Improve maintenance of MLA & international co-operation statistics, especially by including details on the type of assistance provided, time spent on a request, number of pending, refused or withdrawn requests.
3. Further use international co-operation, including MLA, for TF cases, as appropriate, in line with Bahrain's risk profile.

470. 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.

## *Immediate Outcome 2 (International Co-operation)*

### *Providing constructive and timely MLA and extradition*

### *Mutual Legal Assistance*

471. Bahrain has a sound legal basis to provide and seek the widest possible range of MLA in relation to ML, associated predicate offences and TF, and has provided constructive and timely MLA and extradition, to a large extent, for ML. For TF, quick and useful informal mechanisms have been used to a greater extent, considering that terrorist and TF matters are generally dealt with by security and intelligence agencies, including the FID.

472. Formal bilateral agreements are signed at the request of counterparts, although no agreements or MOUs are required under Bahraini law to provide MLA or exchange information. Furthermore, Bahrain's legislation contains grounds for the refusal of MLA requests, including the possibility to reject a request on the basis of it being "against public order", however the assessment team found it positive that in practice, no request has been rejected thus far.

473. Bahrain has put in place a structure to address MLA requests, where the High Criminal Court is the Central Authority and turns requests to the PPO for execution. A dedicated office is established within the PPO to address assistance requests. The office is headed by a chief prosecutor and is adequately supported and resourced. Authorities use a number of capabilities and investigative techniques and information technology tools (i.e. video conference to take a statement) available to domestic LEAs, to facilitate responses to requests.

474. Bahrain presented the details of five incoming requests related to ML, corruption, embezzlement and tax evasion which are included below. Although the number of cases is not high enough to reach a conclusion about consistency of responses and their timeliness, they indicate that a variety of types of assistance has been provided, involving a number of authorities and with good results. In terms of tracing, seizure and sharing of assets related to ML and its predicate offences, authorities also presented several cases where this has been done, even when not systematically recorded as part of the statistics kept by the country. For instance, several MLA requests were sent in one case, to identify bank accounts and recover

company information for seizure, as presented below. No MLA requests were received by Bahrain related to TF.

**Box 11. Corruption MLA Case (2016)**

**Case Description:** MLA request concerning money laundering through bank deposits and corruption. Bahrain was requested to identify and seize properties due to corruption charges in Country K. Upon approval from Higher Criminal Court, further investigations by FID were conducted regarding deposit of large amounts of funds in local banks in Bahrain.

**Procedures undertaken by PPO:** Investigation (Independent from the MLA request based on ML suspicions), seizure of funds and freezing of bank accounts belonging to suspect, suspect's wife and minor children. Based on MLA request, the following amounts were seized:

1- 17,512 USD (Suspect 1 Investment account.)

2- 592,388 USD (Suspect 1's son's Account)

3- 7,718,731 USD (Suspect 1's son's Account).

4- 5,308.560 BHD (Suspect's Account)

5- 118,929.920 Fr (Suspect's Account)

6- 68,744.417 BHD (Suspect's Account)

7- 54,476.790 Euro (Suspect's Account)

8- 19,898.410 BHD (Suspect's wife's Account)

**Case status:** Under Investigation – Waiting for result of corruption case in Country K to avoid duplicity in procedures against suspect.

**Request Status:** Fulfilled in 4 months.

**Box 12. Embezzlement of Funds Case (2015)**

**Request Description:** MLA request from Country X regarding employees of Company S in Country X, which were wanted for embezzlement of funds belonging to Company S and for laundering them from 2007 to 2009. Investigations in Country X discovered funds were being sent to Companies abroad located in multiple countries including Bahrain without those foreign companies providing any services in return.

**Accusations:** ML - Embezzlement.

**Actions taken by PPO:** Receive approval from High Criminal Court, Investigation with witnesses as per MLA request.

**Request status:** Fulfilled in 45 days.

**Box 13. Fraud Case (2014)**

**Request Description:** MLA request from Country P regarding fraud committed by suspects obtaining funds from individuals and companies in (Bahrain, Country U, Country S, Country W, Country T, Country H) by claiming influence over banks in order to provide victims with loans.

**Actions taken by PPO:** Receive approval from High Criminal Court, contact CBB and MOICT in order to fulfil MLA request, investigate and record witness's statements. The MOICT as the company registrar had a relevant role in this case, where it visited the company and obtained information such as bank statements (as part of its routine inspection process).

**Request status:** Fulfilled in 17 months.

**Box 14. Exporting Company Case (Multiple Requests) 2010- Ongoing**

***Request 1-*** A MLA request was received from country N regarding an ongoing investigation pertaining to company officials in country N, who were exporting goods without approval of their management, to country J. Investigations in country N discovered that the company had computers located in Bahrain which were remotely controlled and set up to show that exporting activities were being done in Bahrain. Bank accounts were opened in local banks in Bahrain to transfer the value of exported goods (to country J) into them.

**Accusation:** Money Laundering, Predicate Offences: Unknown, Accused: Employee 1, ML Techniques: Bank Transfers.

**Action taken by the PPO upon MLA request:** Investigation of concerned parties (as per MLA request), seizure of funds in bank accounts, search of company headquarters in Bahrain and addresses of some officials listed, seizure of shipments belonging to country N company, handing over of all documents relative to case to competent authorities in Country N.

***Request 2-*** In September 2014, the PPO received a MLA request from another country (Country Z) concerning the same matter. Further requests were received from competent authorities in Country N on: a) total amount of funds in company's account in local bank; b) assets seized by Bahraini authorities related to MLA request; c) possibility of restarting the investigation with certain persons located in Bahrain (as first attempt failed due to technological difficulties from the Country N' authorities); and d) inquiries regarding transfer of frozen funds belonging to company at local banks.

**Action taken by the PPO:** the PPO responded on each of the above areas and confirmed that the accounts and other assets were still frozen based on an earlier request. The PPO also confirmed its willingness to coordinate with the requesting authorities to reinvestigate if further details on the relevant persons were available, as the earlier address was found untraceable. The requesting country was also advised about the procedures to be followed in order to initiate transfer of funds to bank accounts in Country N.

**Countries Involved:** Bahrain and three other countries.

**Request status:** Fulfilled (one month in average per each request) and negotiations are currently ongoing regarding the funds seized (i.e. frozen accounts).

**Box 15. Tax Evasion Case (2013)**

MLA request from competent authorities in Country A, regarding tax evasion and fraud according to Country A's law, done by certain companies upon purchase and selling of global warming gas permits. MLA request was for transaction and associated details of specific accounts in local bank M, a discovery of any accounts/safe deposits in the bank regarding persons authorised to manage accounts, account opening documents, details of any financial dealings through accounts from EUR 1 000 and above, as also for seizure of financial assets owned by company C at the same bank.

**Predicate Offence:** Tax Evasion, fraud according to Tax Law of country A.

**Actions taken by the PPO:** Request approval from High Criminal Court regarding MLA request, request information from CBB regarding specific accounts at Bank M belonging to company C and the person authorised to manage account, account opening documents and account statements for the relevant period (2009-2015), details of funds sent/received by account during that period, and destination of funds and their source, receiver's details including their bank account number, determine if account holder had any other accounts/deposits/safes at the same bank, request FID investigations regarding persons who opened account or dealt in it, determine nature of activity and relation to the case.

**Request status:** request fulfilled in 29 months.

*Extradition*

475. In terms of extradition, the table below shows the number of persons located and returned to Bahrain through Interpol and MOJ channels, as well as those persons extradited from Bahrain. Bahrain was unable to provide a breakdown for extradition in ML and TF cases, but provided a total number of cases with a breakdown according to financial offences and terrorist act offences. This is a significant number in light of Bahrain's size and context. However, information regarding any requests which may be pending, suspended or withdrawn other than those where persons were located through Interpol warrants (which are normally executed in a shorter timeline, following Interpol's simplified procedures), or the details of the requested countries, would have been useful in further demonstrating effectiveness. It must however be recognised, that statistics for international co-operation, extradition and MLA have been improving in Bahrain, as the previous MER referred to a complete lack of statistics for MLA and extradition.

Table 36. **Returned nationals/extradition decisions for financial offences, incl. ML**

| Years | *Outgoing requests for the return of nationals (Interpol)* | *Extradition Decisions on incoming requests (Interpol)* | *Outgoing requests for the return of nationals (MOJ)* | *Extradition Decisions on incoming requests (MOJ)* |
|---|---|---|---|---|
| **2012** | 1 | 4 | 8 | -* |
| **2013** | 1 | 4 | 4 | - |
| **2014** | 1 | 5 | 6 | - |
| **2015** | 5 | 5 | 5 | 2 |
| **2016** | 4 | 4 | 5 | 2 |
| 2017 | 2 | 2 | 6 | - |
| Total | **14** | **24** | **34** | **4** |

*Note*: * Extradition of Iraqi National refused because of ongoing court matter in Bahrain.

**Table 37. Returned nationals/extradition decisions for terrorist acts**

| *Years* | *Return of nationals (Interpol)* | *Extradition Decisions (Interpol)* | *Return of nationals (MOJ)* | *Extradition Decisions (MOJ)* |
|---|---|---|---|---|
| **2012** | - | - | - | - |
| **2013** | 1 | - | - | - |
| **2014** | 2 | - | - | - |
| **2015** | - | - | 1 | - |
| **2016** | 1 | 1 | 1 | - |
| **2017** | 2 | - | - | - |
| *Total* | **6** | **1** | **2** | **0** |

476. Notwithstanding limitation in statistics noted above, it was possible for the assessment team to conclude that extraditions by Bahrain are provided in a relatively timely manner, given that: i) no complaints with regard to extradition noted by counterparts; and ii) the fact that by law, the average time to process extraditions cannot exceed 30 days (which could be extended to a maximum of 60 days), unless a reason is given by the requesting state. In urgent cases, direct transmission of extradition requests from the other country's judicial authority, to the High Criminal Court (rather than through diplomatic channels) is allowed. Interpol facilitation channels have also been used.

477. Further 21 delegations provided comments about their MLA experience with Bahrain and feedback was generally positive. In some instances, exchange between countries and Bahrain had not been sufficient for a judgement to be provided but this is not necessarily a negative reflection on Bahrain or particular to Bahrain. Bahraini authorities showed willingness to address any remaining concerns.

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

478. Outgoing MLA requests were limited. Bahrain only sent three requests in the last five years regarding the ML offence: to the United States; the United Arab Emirates; and Saudi Arabia. Given the significant use of cash within Bahrain, the cross-border risks present and the total number of non-disclosed carriage of cash into Bahrain, there are concerns that ongoing MLA requests are not fully in line with Bahrain's risk profile.

479. No MLA requests were sent by Bahraini authorities with regard to TF for terrorist organisations such as ISIL and Al-Qaeda, or FTFs, despite the geographical proximity of conflict zones. Authorities provided one example of a case with multiple MLA requests sent abroad for a number of terrorist groups active in Bahrain which enquired on the administrators/users of some social media accounts and persons who funded local terrorists.

480. The assessment team considered that the lack of regular use of MLA for TF investigations was partly explained by a preference for other informal mechanisms, following discussions with authorities in Bahrain, where it is the intelligence and national security agencies who normally deal with terrorist and TF related threats and seek to co-operate informally. The assessment team also considered that the use of informal mechanisms is not unexpected, as intelligence and national security agencies prefer this type of channels when a quick response is needed, and also when information is highly sensitive.

481. Lastly, the assessment team took note of the fact that the lack of formal MLA is also explained because as noted by Bahrain's authorities and confirmed by some domestic terrorism cases, the main terror threat comes from a country with which they do not have a diplomatic relation, and this makes exchanging information difficult.

482. Bahrain indicated that 26 of its citizens have joined ISIL, and there are other terrorist organisations active in the region such as Hezbollah and Al-Qaeda. In this context, Bahrain should use MLA to further understand any international linkages these groups have with Bahrain, even though Bahrain's authorities provided the example of several actions taken with regard to FTF, which did not require MLA, and included international co-ordination to invalidate their passports, revoke their citizenship, and disseminate their names to the international community. This is further noted under section 8.1.3 below.

483. One of the cases included in IO.7 contains a mix of incoming and outgoing requests, and showed several actions can be taken related to a single MLA request. It also showed that requests were made not only to seek assistance for obtaining an ML conviction, but for asset tracing purposes as well.

**Box 16. Terrorism and TF Case- Outgoing Request (2014)**

Bahrain made a MLA request in connection to the use of social media involving several individuals who were under investigation for having supported and perpetrated domestic terrorist acts in Bahrain. Response by the requested country is pending after Bahrain provided further clarifications on information needed.

### *Seeking and providing other forms of international co-operation for AML/CFT purposes*

484. Bahrain has to some extent, used other forms of international co-operation to pursue domestic ML and associated predicates with transnational elements, as well as TF as explained above, even though most of Bahrain's TF cases have related to domestic terrorism and information that is already available to Bahraini authorities.

485. The FID, the Interpol Directorate and other LEAs all have the ability to seek other forms of international co-operation for ML, associated predicate offences and TF in line with Art. 9 of the Decree Law No. 4 (2001) and Art. 6 of the Ministry of Interior Decision No. 18. Although there is no specific provision in the CBB law for seeking co-operation (only providing), supervisory authorities such as the CBB can and have sought co-operation pursuant to a broad interpretation of Art. 122 of the CBB law, as it was established in the TC annex.

486. As a member of Egmont Group since 2003, the FID sends its requests mostly via the Egmont Secure Web channel. The FID also uses MoUs and secure fax and e-mail systems for sending requests. The FID is party to 15 MoU for exchange of information, although these are not required to cooperate.

487. The FID can and has provided information upon request and spontaneously. The FID is proactive when requesting information from its counterparts via ESW channel and exchanged information with a total number of 77 countries since 2012 (See tables 37 and 38 below).The number of requests sent is almost 2.5 times higher than the number of requests received. The highest number of requests is with Saudi Arabia with 81 requests since 2012. In general, it seems that Bahrain has frequently asked and provided information to Gulf region countries and this is expected, considering geographical proximity. Land-borders and concerns about cash expressed in Bahrain's NRA also provide context to these requests.

488. Authorities did not provide a certain timeframe to obtain granted requests, since it depends on the complexity of the case and the request, but for Egmont requests, according to Egmont Group principles, which authorities follow, it should not exceed one month.

489. In addition, high risk requests are prioritised in accordance with the FID's internal document titled, "Policies on Information Exchange". Requests received from a MoU partner, conflict zones or in respect of sanctioned jurisdictions, suspects who have criminal backgrounds and all TF related requests, are given the highest priority.

490. The breakdown of both Egmont and Interpol requests per offence (See also tables 37-39 below), indicate that international co-operation requests both sent and received for TF are fewer in comparison with requests for ML. Only four requests have been made by Bahrain's authorities in relation to TF via Egmont, and this shows that the Egmont Secure Web (ESW) channel is not used for TF co-operation, although numbers are not so distant from requests received (nine for the period). There is also no indication on pending, withdrawn, abandoned requests, if any, which would allow a better assessment of Bahrain's performance. However, information regarding terrorists and TF has been shared through national security agencies. International communications while not done through formal mechanisms were key in obtaining information to identify FTFs and to pursue the rehabilitation of previously radicalised individuals and to monitor counterparties of monitored individuals, in different jurisdictions. Overall, the scenario in terms of international co-operation in this respect is positive.

Table 38. **Number of Requests Sent via Egmont Secure Web (ESW) Per Year***

| | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | TOTAL |
|---|---|---|---|---|---|---|---|
| ML | 35 | 97 | 58 | 42 | 32 | 21 | 285 |
| TF | 0 | 2 | 1 | 0 | 1 | 0 | 4 |
| | 35 | 99 | 59 | 42 | 33 | 21 | 289 |

*Note*: (*) Numbers show the current status of cases as per the date of onsite visit.

Table 39. **Number of Requests Received via ESW Channel per Year (*)**

| | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | TOTAL |
|---|---|---|---|---|---|---|---|
| ML | 17 | 40 | 13 | 14 | 11 | 11 | 106 |
| TF | 0 | 2 | 3 | 2 | 0 | 2 | 9 |
| | 17 | 42 | 16 | 16 | 11 | 13 | 115 |

*Note*: (*) Numbers show the current status of cases as per the date of onsite visit.

Table 40. **Number of Requests Sent/Received via Interpol Channel**

| YEAR | Interpol assistance requests sent | | Interpol assistance requests received | |
|---|---|---|---|---|
| | ML | TF | ML | TF |
| **2012** | - | 1 | - | - |
| **2013** | 1 | - | - | - |
| **2014** | 2 | - | - | - |
| **2015** | 11 | - | - | 1 |
| **2016** | 5 | - | - | - |
| Total | **19** | **1** | **0** | **1** |

491. The CBB has also sought assistance from competent authorities of other countries. The CBB provided statistics, letters and examples in this regard, which demonstrated that they have exchanged prudential supervision information including that related to AML/CFT supervision. In addition, the standard MoU

template of CBB includes provisions for exchange of supervision information between home and host authorities for the operations of cross-border establishments. CBB has signed 27 MoUs, apart from being a signatory to the IOSCO multilateral MoU. The CBB response time has ranged between two days to one month, depending on the nature of the request.

492. Bahrain's Customs authority also cooperates with its counterparts, particularly in the Gulf region. Bahrain and Saudi Arabia have an integrated customs system which has led to the detection of illegal cross-border cash smuggling. The FID shares a similar integrated system with Saudi Arabia. Jordanian Customs also has continuous co-operation with the Bahraini Customs authorities regarding intelligence information and smuggling trends. Bahrain's Customs Authority is also an active member of the World Customs Organisation. This is relevant both for seeking and providing co-operation.

493. The Interpol Directorate in Bahrain is authorised to provide assistance to its foreign counterparts given its Interpol membership. LEAs in Bahrain are required to obtain a warrant from prosecution authorities upon a request in order to conduct an inquiry or obtain evidence. Bahrain states that it can obtain such order within hours. Direct communication also exists between authorities in Bahrain and this is an advantage.

494. Authorities indicated that LEAs can conduct joint investigations based on international conventions even when no specific bilateral or multilateral agreement exists for establishing joint investigative teams.

495. With regard to tax evasion and fiscal fraud as a ML predicate, no requests have been made by Bahrain but this is explained by Bahrain's fiscal regime context (See explanation in IO.8). Incoming requests for co-operation however have been addressed, mostly channelled through the FID, although the PPO and the CBB also have the ability to exchange information and that has occurred. Information, including beneficial ownership information (for fiscal purposes) has been shared with bilateral partners and in the context of international protocols which Bahrain is signatory to. The case in Box 15 above shows a good example of how international co-operation has been used in the context of combatting tax evasion as a predicate for ML.

496. Feedback received from delegations regarding other types of international co-operation and particularly the FID was positive.

497. International exchange of basic and beneficial ownership information of legal persons and arrangements

498. As outlined in R.24 and IO.5, legal and beneficial ownership information, particularly with regard to Bahraini owned companies, is publicly available through a website held by the MOICT ("Sijilat"), so a request by international counterparts or formal exchange with the authorities is seldom necessary. Any person can access Sijilat from any jurisdiction. The website is available both in English and Arabic and is considered user-friendly and clear. Company shareholder information can be obtained immediately through this portal since the MOICT monitors the transfer of ownership and updates the database accordingly. For foreign companies, the MOICT has the authority to demand financial reports from companies registered, in order to

trace any changes in ownership. This helps ensure the availability of beneficial ownership information.

499. The MOICT receives an average of 550 phone calls on a daily basis for different purposes, out of which 27% are queries related to owners/authorised/activities/ address of a business. In addition, since ownership information (including beneficial ownership details in many cases) is captured in the Sijilat system, those interested can access such information directly through the system. MOICT provided information on the usage of Sijilat system and confirm it has been consulted from a number of countries. As a reference, only in 2017, Sijilat calculated 646 306 entries in its website related to ownership and beneficial ownership information.

500. As it was noted in several instances in this report, Bahrain is a major financial and business centre in the Gulf region. Incentives for business development, which require company formation, are provided by the government. At the same time, there has been a strategy to facilitate, yet strengthen company formation regulation and oversight. The existence of the Sijilat registrar system is meant to achieve that objective. Another important factor is that the MOICT is also an AML/CFT compliance regulator for DNFBPs and in that role, as well as in its role as registrar, it routinely visits companies and ensures that the companies formed are being used for the purpose they were created. Notwithstanding the above described direct and public access to information that international counterparts have, the MOICT has the authority to exchange basic and beneficial ownership information either domestically or internationally and based on what was also explained above, this information is reliable. The relevant role MOICT played in several case examples involving companies has been noted throughout the report. The FID is also authorised to exchange information on beneficial ownership for AML/CFT purposes (which would normally be obtained through the MOICT), this was done nineteen times during the assessment period, mainly to cover requests made in the context of tax treaties.

### *Overall conclusions on IO.2*

501. **Bahrain is rated as having a substantial level of effectiveness for IO.2.**

# TECHNICAL COMPLIANCE ANNEX

This annex provides detailed analysis of the level of compliance with the FATF 40 Recommendations in their numerical order. It does not include descriptive text on the country situation or risks, and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report.

Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the previous Mutual Evaluation in 2006. This report is available from http://menafatf.org/information-center/menafatf-publications/mutual-evaluation-report-kingdom-bahrain-anti-money

## Recommendation 1 – Assessing risks and applying a risk-based approach

There was no requirement for a national risk assessment (NRA) or other risk-related requirements which are now set out in R.1.

***Criterion 1.1*** - Art. 2 of MO No. 14 of 2017 states that the committee must determine a mechanism to coordinate the procedures to assess ML/TF risks on the national level by providing all relevant competent authorities and self-regulatory bodies (SRBs), FIs and DNFBPs, with appropriate information on the results of the risk assessment.

The assessment team received:

- a draft national risk assessment, which the Bahrain authorities hope to finalise in the near future.
- a document called "Anti-money laundering/terrorist financing and self-defence for real estate agents and professionals", containing indicators and FAQs;
- a document entitled "Anti-Money Laundering Defence Mechanism for Jewellers", containing indicators and FAQs;
- a document called "Analysis of Sector's Risk: Audit Firms". This document summarises contextual matters, including registration requirements and sector size, and market share analysis but in practice does not provide an analysis to allow for identification and assessment of ML/TF risks.
- a document called DNFBPs – A Specialised Sector Analysis (for audit firms, gold and jewellery and cars). This includes statistical analysis of STRs reported by these sector; and does not lead to a comprehensive understanding of ML/TF risks.

There is a mechanism in place to identify and assess risks (See the other criteria of this Recommendation immediately below) but, overall, the ML/TF risks have been identified and assessed only to some extent.

***Criterion 1.2*** - The Minister of Finance and National Economy, in co-ordination with the relevant entities, must appoint a policy committee for the prevention and prohibition of ML [Decree Law No.4 (2001)]. The committee (the National Policy Committee- NPC) has responsibilities under the law such as the establishment of general policies with regard to the prevention and prohibition of ML/TF and the study of regional and international ML/TF developments for the purposes of recommending updates to guidelines and changes to the law when necessary. Art. 12.1 of Decree Law No.4 (2001) states that the Minister of Finance and National Economy in co-ordination with the relevant entities may issue regulations or resolutions in relation to the functioning of the committee. In addition, Art. 2 of MO 14 of 2017 states that the committee shall draw up of general policies to identify and assess the ML/TF risks for the country on a national level.

***Criterion 1.3*** - The draft NRA, when completed, will be Bahrain's first NRA. Art. 2 of MO 14 (2017) states that the risk assessment process at the national level must be kept updated on a regular basis. Authorities indicated that the draft NRA would be completed and circulated by the end of May 2018.

***Criterion 1.4*** - Art. 2 of MO 14 (2017) states that the committee must determine a mechanism to coordinate the procedures to assess ML/TF risks on the national level by providing all relevant competent authorities and SRBs, FIs and DNFBPs, with appropriate information on the results of the risk assessment.

***Criterion 1.5*** - Art. 2 of MO 14 (2017) states that the committee should apply a risk-based approach methodology to ensure that measures to prevent or mitigate ML/TF are commensurate with the risks identified. The NRA results will provide the risk-based mechanism to ensure that the measures in place are commensurate with the identified risks in the assessment. The MO goes on to state that this approach is essential to the efficient allocation of resources according to the degree of risk and drawing up of general policies and implementing the necessary measures to prevent or mitigate ML/TF risks.

***Criterion 1.6*** - *(Not applicable)* All FIs and DNFBPs in Bahrain are subject to the full implementation of the FATF Recommendations.

***Criterion 1.7*** - FIs: The CBB Rulebook specifies the requirements for ECDD for conventional banks (FC-1.3.1 onwards of volume 1). These include situations where the conventional bank has assessed the customer as having a higher risk profile; non-face to face business; PEPs; charities, clubs and other societies; pooled funds and correspondent banking. Equivalent provisions are included in FC-1.3.1 onwards of volume 2; FC-1.3.1 onwards of volume 3 (there are no provisions in relation to charities, clubs and other societies or in relation to correspondent relationships or pooled funds).

These provisions cover generic risks and do not appear to extend to higher risks identified by Bahrain in any risk identification and analysis undertaken by Bahrain. The CBB Rulebook specifies that ECDD must be performed on those customers identified as having a higher risk profile, and additional enquiries made or information obtained in respect of those customers. It is intended that the results of

the NRA and action plans will be communicated to all licensees. The results of the NRA will provide the guidance for higher risks identified at a country level.

DNFBPs: DNFBPs supervised by the MOICT must carry out EDD when procedures identify a higher risk, when the client is not physically present, when entering a relationship with a PEP or in any other situation where a higher ML/TF risk might exist (Art.5 (D) of MO 173 of 2017). These are generic and there is no specific provision requiring entities automatically to take account of the NRA.

There is no provision requiring FIs or DNFBPs to ensure that higher risks identified by Bahrain are incorporated in risk assessments. To an extent, this is mitigated by FC-4.3.1 of volume 1 of the CBB Rulebook which requires that conventional bank licensees must take appropriate steps to identify and assess their ML/TF risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels). They must document those assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to the CBB. The nature and extent of any assessment of ML/TF risks must be appropriate to the nature and size of the business (equivalent provisions exist in FC-4.3.1 of volume 2, FC-3.3.1 of volume 3, FC-3.3.1 of volume 4, and AML-3.3.1 of volume 6). The intention is that higher risks identified by Bahrain in the NRA, once it has been completed, will be required to be incorporated in risk assessments.

***Criterion 1.8*** - There are provisions in each of the volumes of the CBB Rulebook on types of customer in relation to which simplified due diligence may be applied. It is not clear whether simplified measures are permitted for DNFBPs subject to the oversight of the MOICT. See criteria 1.12, 10.18 and 22.1. Bahrain has not prepared a written assessment of the basis of the cases subject to simplified measures but they nevertheless appear to be consistent with the country's risks.

***Criterion 1.9*** - The CBB has been appointed as the supervisor of FIs and professional trustees, while the MOICT has responsibility for the oversight of accountants, auditors and DPMS. During the onsite visit, monitoring authorities were established for legal professionals and notaries, while RERA/SLRB had been appointed for real estate agents in September 2017 with an operational date of early 2018. Prior to September 2017, real estate agents structured as legal persons were supervised by MOICT.

Both the CBB and the MOICT undertake onsite and offsite supervision. The CBB has put in place a framework for and some strong elements of a risk based approach to supervision, though it is not comprehensive. The MOICT has put in place a framework for and has a largely risk based approach to supervision. DNFBPs not subject to oversight by the MOICT have not been subject to any supervision to ensure that they meet their obligations. FIs are required to carry out a risk-based approach under the CBB Rulebook. DNFBPs subject to the MOICT's supervision are required to take a risk based approach for DNFBPs under MO 173 of 2017. See criteria 1.10 to 1.12. See R.26 and R.28.

***Criterion 1.10*** - FC-4.3.1 of the CBB Rulebook requires conventional banks to take appropriate steps to identify and assess their ML/TF risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels). This appears to constitute a risk assessment for the business as a whole. The nature and

extent of any assessment must be appropriate to the nature and size of the business. Under FC-4.3.1A, conventional banks should understand their ML/TF risks (although it is not clear how banks should use that understanding). While there appears to be no specific requirement to profile the risk of customer relationships at the outset of the business relationship or prior to the occasional transaction, there are implicit requirements. For example, under FC-1.3.1 of volume 1, ECDD must be performed on those customers identified as having a higher risk profile, and additional inquiries made or information obtained in respect of those customers. In addition, FC-1.1.2B stipulates that there must be ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of, inter alia, their risk profile. The guidance advises that the CBB may determine that individual documented risk assessments are not required if the specific risk inherent to the sector are clearly identified and understood. No such determination has been made by the CBB. The same provisions are contained in the other volumes except volume 5. FC-4.3.1 of volume 1 and equivalent provisions for the other volumes except volume 5 contain a requirement to document the risk assessment.

a) The FC Module requirements stipulate that the nature and extent of any assessment of ML/TF risks must be appropriate to the nature and size of the business although this is a different test to that of all the relevant factors required by the criterion (and in any case the test does not extend to individual relationships). There is no explicit requirement that the level and type of mitigation must be appropriate to the assessment, although it can be regarded as implicit.

b) FC-4.3.1 of volume 1 and equivalent provisions for the other volumes except volume 5 include a requirement to keep the risk assessments up to date.

c) FC-4.3.1 of volume 1 and equivalent provisions for the other volumes except volume 5 include a requirement for licensees to have appropriate mechanisms to provide risk assessment information to the CBB (but not other competent authorities).

Art.2 of MO 173 (2017) provides for a risk-based approach by MOICT supervised DNFBPs. Art. 5 also provides for enhanced due diligence requirements in case of higher risks. There are, however, no specific provisions which meet the requirements set out in this criterion.

***Criterion 1.11*** - Conventional banks must implement AML/CFT programmes which establish and maintain appropriate systems and controls for compliance with the financial crime module of the Rulebook and which limit their vulnerability to financial crime (FC-2.1.1 of the CBB Rulebook). These systems and controls must be documented and approved and reviewed annually by the Board of the licensee. Equivalent provisions are found in FC-2.1.1 of volume 2; FC-2.1.1 of volume 3 (albeit guidance indicates that for unincorporated entities annual reviews should be undertaken by the most senior person); FC-2.1.1 of volume 4; FC-2.1.1 of volume 5 and AML-2.1.1 of volume 6). The language of the Rulebook implicitly encompasses the criterion's requirement to enable banks to manage and mitigate the risks identified in light of the Rulebook's requirements to take appropriate steps to identify and assess their ML/TF risks and the implicit requirement to risk profile customers but the language could usefully be made clearer. There is no reference to policies. Concerning MOICT supervised DNFBPs, each registered person must

develop regulations and procedures to ensure the commitment of staff to implementing the MO (Art.7 (b) of MO No. 173 of 2017. The language of the MO does not cover policies, approval by the senior management, or the management and mitigation of risks (although there is a requirement on registered persons to adopt a risk based approach).

a) A conventional bank must review the effectiveness of its AML/CFT procedures, systems and controls at least once a year (FC-4.3.IB of volume 1). Equivalent provisions are there in FC-4.3.IB of volume 2, FC-3.3.IB of volume 3, FC-3.3.IB of volume 4, FC-4.3.1 of volume 5 and AML-3.3.1B of volume 6. There is no specific requirement to enhancing controls if necessary. With regard to MOICT supervised DNFBPs, the responsibilities of the compliance officer include ascertaining the suitability of the applicable internal controls, regulations and procedures, which could implicitly cover their enhancement as appropriate (Art.7 of MO No. 173 of 2017).

b) FC-1.3.1 of volume 1 (and FC-1.3.1 of volume 2, FC-1.3.1 of volume 3, FC-1.3.1 of volume 4, FC-1.3.1 of volume 5 and AML-1.3.1 of volume 6) requires enhanced CDD to be performed in relation to customers with a higher risk profile (with FC-2.2.1 in volume 1 and equivalent provisions in other volumes requiring risk based monitoring systems) but this could be different to requiring banks to manage and mitigate higher risks. DNFBPs, subject to the supervision of the MOICT are required to adopt enhanced due diligence measures where higher ML/TF risks exist.

***Criterion 1.12*** - FC-1.11.1 of volume 1 of the CBB Rulebook provides for six types of customer in relation to which simplified due diligence may be applied. Similar provisions (but with differences) are contained in 1.11.1 of volume 2, FC-1.6.1 of volume 3, 1.10.1 of volume 4, FC-1.10.1 of volume 5 and AML-1.10.1 of volume 6 (See c.10.18). See criterion 10.18. Under FC-1.11.7 simplified due diligence measures must not be applied where a conventional bank knows, suspects, or has reason to suspect, that the applicant is engaged in ML/TF or that the transaction is carried out on behalf of another person engaged in ML/TF. Identical provisions are found in FC-1.11-7 of volume 2; FC-1.6.8 of volume 3; FC-1.10.8 of volume 4; FC-1.10.7 of volume 5 and AML-1.10.8 of volume 6. No written assessment of the rationale for the types of customer potentially subject to simplified measures has been carried out but they appear to be consistent with Bahrain's risks. There is a provision for simplified due diligence for DNFBPs under the oversight of the MOICT where customers are well known to the registered person; it is not clear that in all such cases the simplified measures would be commensurate with lower risk (See the analysis of c.10.18 in c.22.1).

### *Weighting and Conclusion*

ML/TF risks have been identified and assessed only to some extent. Bahrain is yet to finalise its first NRA, and fully implement a risk-based approach to allocating resources and implementing mitigating measures. There are currently no requirements for FIs and DNFBPs to ensure that higher risks identified by Bahrain are incorporated in risk assessments. There are no specific provisions requiring DNFBPs to document their risk assessment or to consider all relevant risk factors while determining the overall level of risk and apply mitigating measures. Some

elements of risk management are missing (See criterion 1.11). Simplified measures are not risk based (See criterion 1.12).

**Recommendation 1 is rated Partially Compliant.**

## *Recommendation 2 - National Co-operation and Co-ordination*

Bahrain was rated partially compliant with former R.31 as no gateways existed between law enforcement and supervisory authorities for mutual assistance, and improvements were needed for co-ordination and co-operation between ministries. R.2 is now more specific about the need for countries to have national AML/CTF policies that encompass identified risks and for co-ordination to be more formalised.

***Criterion 2.1*** - Bahrain has put in place a structure and mechanism to identify national ML/TF risks and to draw national policies to address them. However, national policies are yet to be developed as the NRA is still being finalised. There appears to be no legislative requirement or procedure to regularly review policies. MO no.14 (2017) requires the country to regularly review and update its NRA.

The committee appointed by the Minister of Finance and National Economy is responsible for establishing general policies with regard to the prevention and prohibition of ML/TF [Art. 4 Decree Law No.4 (2001)]. The committee is entrusted with drawing up policies with respect to the prohibition and combatting of ML/TF [Art.1 MO no.14 (2017)]. The 13 members of the committee are senior representatives of the CBB (Chair); the MOI, MoFA, PPO; MOICT, SLRB; Ministry of Finance; MOJ and Islamic Affairs; MLSD; NSA; Ministry of Youth and Sports Affairs; Legislation and Legal Opinion Commission and Bahraini Customs [Art.1 MO no.14 (2017)].

Art. 2 of MO 14 of 2017 states that the NPC is entrusted with drawing up of general policies with respect to AML/CFT and, particularly, to identify and assess the ML/TF risks for the country at a national level by:

a) determining a mechanism to coordinate the procedures to assess ML/TF risks at the national level by providing all relevant competent authorities and SRBs, FIs and DNFBPs, with appropriate information on the results of the risk assessment;

b) applying a risk-based approach methodology to ensure that measures to prevent or mitigate ML/TF are commensurate with the risks identified. This approach is essential to the efficient allocation of resources according to the degree of risk and drawing up of general policies and implementing the necessary measures to prevent or mitigate ML/TF risks;

c) keeping the risk assessment process on the national level updated on regular basis.

The committee is also tasked with establishing mechanisms to enable policy makers, the financial intelligence unit, law enforcement authorities, regulatory bodies and other relevant competent authorities to cooperate and coordinate domestically with each other regarding the development and implementation of policies and activities to combat ML/TF. Such mechanisms should apply at the policymaking and operational levels.

***Criterion 2.2*** - See criterion 2.1 above.

***Criterion 2.3*** - Art. 2 of MO 14 of 2017 provides for the NPC to establish mechanisms to enable policy makers, FIU, law enforcement authorities, regulatory bodies and other relevant competent authorities to cooperate and coordinate domestically with each other regarding the development and implementation of policies and operational activities to combat ML/TF.

***Criterion 2.4*** - Bahrain has established the UN National Committee, which coordinates policy and operational activity on PF. The UN National Committee has a broad membership, including MoFA, NSA, Bahrain Defence Force, CBB, FID, MOI, MOJ, and Bahraini Customs, amongst others. At the bilateral level there has been positive co-operation and information exchange between the CBB and the FID in relation to a breach of PF requirements.

### *Weighting and Conclusion*

Bahrain has put in place a mechanism to create national policies and to ensure co-ordination among authorities, however national risk based policies have yet to be developed.

**Recommendation 2 is rated Largely Compliant.**

## *Recommendation 3 - Money laundering offence*

Bahrain was rated partially compliant with former R.1 as the scope of the ML offence was not fully consistent with Vienna and Palermo Conventions, and excluded TF as a predicate offence to ML. In 2006, Bahrain passed amendments to establish a TF offence.

***Criterion 3.1*** - Bahrain's offence covers the conduct set forth in the Vienna and Palermo Conventions. ML is criminalised in Art. 2 of the Decree No.4 (2001). The offence states that any person (natural or legal) who commits certain listed actions for the purpose of "showing that the source of the property is lawful shall have committed the offence of money laundering". The listed actions include, knowingly: conducting a transaction (i.e. using, conversion); concealing or disguising; acquiring, receiving or transferring; retaining or possessing proceeds of crime knowing or believing, or having reason to know or believe, that they were derived from criminal activity, or from an act of participation in criminal activity.

***Criterion 3.2*** - The ML offence outlined in c.3.1 applies to "the proceeds of crime from one of the crimes provided for in paragraph 2.1 of Decree no.25 (2013)". Paragraph 2.1 references many of the 21 predicate offences to ML. It also includes a provision that states that a predicate offence to ML also includes "any other crime set forth in the Penal Code or any other laws and crimes indicated in international conventions and protocols attached thereto which Bahrain is a party if they are punishable by Bahraini law". A number of predicate offences are established in the Penal Code, specifically: extortion (Art. 390), counterfeiting currency (Art. 262), murder (Art. 333), grievous bodily injury (Art. 337), and participation in an organised criminal group (Art. 152-153). Bahrain does not explicitly criminalise racketeering, but relies upon the United Nations Convention against Transnational Organised Crime to capture the offence of racketeering, without its transposition into national law. In terms of sentencing, Bahrain states that it would identify an existing offence that is similar in activity and apply that sanction. In 2006, Bahrain

established a TF offence, which is included as a predicate offence to ML. However, the deficiencies identified in R.5 regarding the exemption for liberation groups limits the scope of the TF predicate offence. Bahrain has ratified all of the nine anti-terrorism conventions included in the annex to the TF Convention and criminalised the offences therein.

**Criterion 3.3** - (Not applicable) No threshold is applied.

***Criterion 3.4*** - The term "proceeds of crime" relates to property which is derived directly or indirectly, in whole or in part, from any criminal activity. "Property" is further defined as property of every kind, nature and description, whether movable or immovable, tangible or intangible. A list of non-exhaustive examples are included in this definition of property, including "anything or object used in money laundering". This broad definition of property covers corporeal or incorporeal assets and legal documents or instruments in any form, evidencing title to, or interest, in such assets [Decree No.4 (2001)].

***Criterion 3.5*** - A person can be punished for ML even when not convicted of the underlying predicate offence [Art. 2.3 of Decree No.4 (2001)].

***Criterion 3.6*** - Art. 2.1 of Decree No.25 (2013), which sets out the predicate offences to ML (See c.3.2), states that the listed criminal activity is a predicate to ML regardless of whether or not the criminal activity occurred inside or outside of Bahrain.

***Criterion 3.7*** - Self-laundering is criminalised as a person may be charged/convicted separately of both the predicate offence generating the proceeds of crime, as well as the laundering of those proceeds [Art. 2.4 of the Decree No.4 (2001)].

***Criterion 3.8*** - Bahrain provided case law establishing that the intentional element of its ML offence may be inferred from objective factual circumstances.

***Criterion 3.9*** - The criminal penalty for ML is a fine not exceeding BHD 1 million (EUR 2 million) and a maximum imprisonment of seven years. The offence also includes mandatory minimum sentences of five years' imprisonment and a fine no less than BHD 100 000 (EUR 215 588) in certain circumstances, such as when ML was committed: through an organised criminal gang; by using power or influence through an institution; and, for the purpose disguising the source of the proceeds which are derived from criminal activity to appear as of a lawful source [Art. 3.1 Decree No.4 (2001)].

The sanctions available for ML are dissuasive and proportionate to other financially motivated crimes in Bahrain (e.g. embezzlement resulted in a five year sentence; prostitution resulted in a five year sentence; counterfeiting can result in a maximum five year sentence; and bribery can result in a maximum ten year sentence).

***Criterion 3.10*** - In Bahrain, a corporate body, including every person who, at the time of the commission of the offence, acted in an official capacity for or on behalf of such body, may be criminally liable for ML, if the offence was committed by intentional conduct or gross negligence [Art. 2.5 Decree No.4 (2001)]. In cases where ML is committed by a corporate body and notwithstanding the liability of any natural person, the corporate body shall be liable to the punishment of a fine (not exceeding BHD 1 million (EUR 2 million)) in addition to confiscation of the property which is the subject matter of the offence (Art. 3.3).

***Criterion 3.11*** - Art. 2.2 (a)-(d) of Decree No.4 (2001) captures the participation in conducting transactions related to ML, and concealing, disposing, acquiring, receiving, retaining, and transporting proceeds of crime. Acts set out in Decree No.4 to explain "participation" do not capture aiding and abetting, facilitating, and counselling the commission of such activities. The ancillary offences in the Decree Law No.4 (2001) are not applicable to legal persons. Art. 36-42 of the Penal Code establish an offence for attempting a criminal offence, which is also applicable to the ML offence. Art. 43 establishes the offences of participation in, association with, and conspiracy to commit a criminal activity. Art. 44 establishes the offences of aiding and abetting, and broadly covers facilitating and counselling the commission of a crime. The penalties for the ancillary offences are the same as for the primary offence; however, the Penal Code does not provide for corporate criminal liability and therefore the ancillary offences in the Penal Code also do not extend to legal persons.

### *Weighting and Conclusion*

The deficiencies identified in R.5 regarding the inclusion of an exemption to the TF offence limits the scope of the TF predicate offence for ML. Further, while ancillary offences are available to natural persons, they are not available to legal persons. This latter deficiency is assessed as minor. All other criteria are met.

**Recommendation 3 is rated Largely Compliant.**

## *Recommendation 4 - Confiscation and provisional measures*

Bahrain was rated partially compliant with former R.3 as confiscation was unavailable in TF cases (due to a lack of criminalisation) and effectiveness was considered insufficient.

***Criterion 4.1*** - The Penal Code outlines the general confiscation powers related to all criminal offences (Art. 64). While delivering a judgment for an offence, a judge is also empowered to confiscate the items seized in connection with an offence or items used or in the process of being used for the commission of the offence (instrumentalities). The confiscation of income or other benefits derived from criminal proceeds is also permitted. A confiscation order can be issued even if such items do not belong to the accused, or if no conviction verdict has been passed in respect of the case, when the manufacture, possession, ownership or use of such items, or dealing therein constitutes an offence. The Penal Code does not provide for corporate criminal liability; instead, this is explicitly included in the ML offence in Decree No.4 (2001). Upon conviction of ML, the legal person is liable to the confiscation of the "property which is the subject matter of the offence" (Art. 3.3).

While the Penal Code sets out the general powers related to confiscation, Decree No.4 (2001) establishes confiscation powers upon conviction of ML. Specifically, the Decree states, "without prejudicing the rights of bona fide third parties, a person convicted of ML is liable to confiscation of property which is the subject matter of the offence, or any other property owned by him equivalent in value to the property which is subject matter of the offence" [Art. 3.2–3.3 Decree No.4 (2001)]. Property is defined in Decree No.4 (2001) as "property of every kind, nature and description, whether movable or immovable, tangible or intangible".

Confiscation is possible when the suspect dies during the judicial investigation (led by the PPO) before the conviction, except if the heirs prove the legal origin of that property (Art. 3.2, and Art. 17 CPC). If the suspect absconds, criminal proceedings are possible in absentia.

Decree No.54 (2006) and Decree No.58 (2006) criminalises TF by amending Decree No.4 (2001) and establishes sanctions available for those convicted of TF, including confiscation pursuant to Art. 3.3 described in 4.1 above, as that Art. also applies to TF convictions (Art. 5 bis 5 of Decree No. 54 (2006).

***Criterion 4.2*** - All items in R. 4.2 (a) – (e) are met. In regard to ML investigations, Art. 6.1 of the Decree No.4 (2001) provides for the identification, seizing, freezing, and prohibition of the transfer of any property subject to confiscation in accordance with the provisions of the Decree. These measures are available upon receipt of an order from the PPO, and may be conducted without prior notice. Further, according to Art. 10.2 of the said Decree No.4 (2001) and its amendments, without prejudice to the rights of bona fide third parties, a contract shall be considered illegal and void if either party thereto knew or should have known that as a result of the contract the State of Bahrain would be prejudiced in its ability to recover financial claims pursuant to that Decree.

MO No.18 (2002) permits the FID to temporarily seize money during investigation until ascertaining the legitimacy of its source, this may also be done without prior notice. Further, in cases of fear of disposal of money, the FID may issue an order to preserve such money provided that the matter shall be presented to the PPO within three days upon the issuance of an order (Art. 3).

Art. 98 of the CPC states that the PPO is also empowered, in the case of necessity or urgency, to temporarily order that the accused, his/her spouse or minor children be forbidden from disposing or managing their properties. The PPO is required to refer the prohibition order to the High Criminal Court within seven days from its issuance.

In regard to TF investigations, Art. 24 of Decree No.58 (2006) includes reference to seizure powers of the High Criminal Court, upon judgement, of the properties, weapons, tools, machinery and documents apprehended that have been used or intended for use in the offences included in the Decree (including TF). Further, Art. 29 permits the Attorney General or whoever acting for him to order the seizure of mail of all kinds, publications, parcels and telegrams where it is "useful for uncovering the truth in crimes" contained in the Decree. In all cases, the seizure order is available for a period not exceeding sixty days. An extension is available upon approval of the High Court. Art. 30 also permits the PPO, upon prior approval from the High Court Judge, "to order the access or receipt of any data or information related to the accounts, deposits, trusts or safe deposit boxes with banks or other financial institutions or the transactions related thereto if necessary for revealing the truth in any of the crimes provided for in this Law".

***Criterion 4.3*** - Bona fide third parties can claim their rights, before, during, and after the court proceedings (CPC Art. 104-113). In addition, confiscation decisions are made without prejudice to the rights of bona fide third parties, in line with Art. 64 of the Penal Code.

***Criterion 4.4*** - The CPC permits the returning of seized assets, unless they are subject to confiscation (Art. 104-113). Bahrain has mechanisms for managing or

disposing of seized property [Art. 98, 99 of the CPC (which refer to the need to appoint someone for the management and the need for an adequate management of property) and Resolution No.66 (2017) further details the process]. Confiscated properties are devolved to the Treasury and concerned units such as MOJ, SLRB, and Traffic Department take a role in this process. Real estate transferred to the Treasury is dealt with in the same way as state property, and movables are sold through auction.

### *Weighting and Conclusion*

**Recommendation 4 is rated Compliant.**

## *Recommendation 5 - Terrorist financing offence*

Bahrain was rated non-compliant with former SR.II as TF was not criminalised. In 2006, Bahrain passed legislative amendments through Law No.54 (2006), introducing a TF offence.

***Criterion 5.1*** - Bahrain's TF offence states that it is an offence for anyone to raise, give or appropriate property, funds, or revenues to a society, group, organisation, association or gang that engages in terrorist activity based inside or outside of the country, or to one of its members for its benefit, or provide support or finance by any means knowing that it will be used for terrorist activities [Art. 3.1 Decree No.54 (2006), an amending act to Decree No.4 (2001)].

This definition includes a requisite mental element (*mens rea*) of the offence, and broadly covers both the provision ("give") and collection ("raise") of funds or other assets. Further, the term "property" is broadly defined in Bahraini law to cover funds or other assets (See c.5.3), and covers the provision of funds in full and in part.

Decree Law No.36 of 2017 criminalises the indirect provision and collection of funds, and this type of activity is also captured through Bahrain's ancillary offences in its Penal Code (See c.5.8).

Decree No.54 (2006) and Decree no.58 (2006) establish Bahrain's terrorism offence; however, the definitions of terrorism contained in the two decrees are inconsistent. Notably, one of the definitions (in Decree No.54) contains an exemption for "peoples struggle, including armed struggle against foreign occupation, aggression, colonialism, and hegemony, aimed at liberation and self-determination in accordance with the principles of international law" [Art. 1(b)]. This exemption is based on the same exemption in the Convention of the Organisation of the Islamic Conference on Combating International Terrorism. The Decree also states that the definition of terrorism is "without prejudice to the definition…which appears in the Treaty of the Islamic Conference Organisation for Combating International Terrorism", meaning that Bahrain both supports the exemption explicitly in law and through reference. Through the inclusion of this exemption, the TF offence is narrow in scope and inconsistent with the TF Convention.

Art. 6 of the TF Convention specifically prohibits exemptions from the scope of the TF offence. It states that each party shall adopt such measures as may be necessary, including, where appropriate, domestic legislation, to ensure that criminal acts within the scope of this Convention are under no circumstances justifiable by

considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature.

***Criterion 5.2*** - Bahrain's TF offence nominally extends to "everyone" who commits the offence of TF as articulated in Art. 3 of Decree No.54 (2006). Decree Law No.36 (2017) criminalises the financing, for any purpose, of an individual terrorist that engages or attempts to engage in terrorist activity. However, the exemption in Decree No. 54 in the definition of terrorism (See 5.1) potentially limits the scope of the TF offense significantly.

***Criterion 5.2bis*** - Decree Laws No.54 and No.36 criminalises the financing of an individual, group, or member of a group "that engages in terrorist activity, whether its headquarters is located inside or outside the country, or to any member of such a group, or anyone carrying out any operation on its behalf or providing it with support or funding by any means, with the knowledge that it engages in terrorist activity..." This broadly covers the travel of an individual, groups or group members as financing travel would be captured through the term "support or funding". However, the exemption in Decree no. 54 in the definition of terrorism (See 5.1) potentially limits the scope of the TF offense significantly.

***Criterion 5.3*** - Art. 3 of Decree No.54 criminalises raising, giving or appropriating "properties, funds or their revenues" to terrorists. "Property" is defined in Decree No.4 (2001) as property of every kind, nature and description, whether movable or immovable, tangible or intangible. A non-exhaustive list of examples is included in this definition, such as corporeal or incorporeal, and legal documents or instruments evidencing title to, or interest in such assets.

Art. 1 Decree no.58 also includes a definition of property, which mirrors the definition contained in Decree No.4 (2001).

***Criterion 5.4*** - Art. 3 of Decree No.54 criminalises the financing of a group or member of a group "that engages in terrorist activity, which is based inside or outside the country, or to one of its members or carries out for its benefit any operation or provides support or finance by any means and where he is aware that it engages in terrorist activity." This does not require that the funds have actually been used or linked to a specific terrorist act. Decree Law No.36 (2017) criminalises the financing, for any purpose, of an individual terrorist that engages or attempts to engage in terrorist activity.

***Criterion 5.5*** - Bahraini law provides that the TF offence must be committed intentionally to be punishable. Bahrain provided case law establishing that the intentional element of the offence may be inferred from objective factual circumstances.

***Criterion 5.6*** - The penalties available for TF are proportionate and dissuasive, as TF is punishable by a term of imprisonment not less than ten years and up to life imprisonment. In addition to a term of imprisonment, fines no less that BHD 100 000 (EUR 215 588) are available.

***Criterion 5.7*** - Art. 3 of Decree No.54 criminalises terrorist financing for "everyone" but does not specify whether this includes natural or legal persons. The term "everyone" is not defined in the Decree, but Bahrain has clarified that it does cover legal persons. Decree Law No.36 (2017) criminalises the financing of terrorism by

"anyone." While also undefined, Bahrain has verbally confirmed that this includes natural and legal persons. In other parts of Bahraini law, penalties are explicitly included for legal persons [See the criminal liability of corporate bodies for ML in Art. 2.5 of Decree Law No.4 (2001)].

Decree Law No.36 of 2017 provides penalties for legal persons for the financing of terrorism – in the order of "a fine of not less than BHD 100 000 and not exceeding BHD 500 000".

***Criterion 5.8*** - Art. 3 of Decree No.54 states that attempting to commit TF shall be punishable by the same penalty prescribed for the primary offence (Decree No.54). Art. 3 also criminalises the receipt of "properties or funds of any kind" from terrorist organisations "with the view of preserving them or exploiting them for their benefit".

As noted in c.3.11 above, Art. 36-42 of the Penal Code (1976) establish an offence for attempting a criminal offence. Art. 43 establishes the offences of participation in, association with, and conspiracy to commit a criminal activity. Art. 44 establishes the offences of aiding and abetting, and broadly covers facilitating and counselling the commission of a crime. It is unclear whether penalties for the ancillary offences are the same as for the primary offence, and whether the ancillary offences in the Penal Code may be applied to the TF offence, which is contained in a Decree.

***Criterion 5.9*** - The ML offence outlined in c.3.1 applies to "the proceeds of crime from one of the crimes provided for in paragraph 2.1 of Decree No.25 (2013)". Paragraph 2.1 explicitly references "terrorism crimes and its finance".

***Criterion 5.10*** - Decree No.54 criminalises the financing of terrorist activities that occur "inside or outside the country" (Art. 3.1).

### *Weighting and Conclusion*

Bahrain's TF offence is not in line with TF Convention. Specifically, its definition of terrorism includes an exemption for "peoples struggle, including armed struggle against foreign occupation, aggression, colonialism, and hegemony, aimed at liberation and self-determination in accordance with the principles of international law".

**Recommendation 5 is rated Partially Compliant.**

## *Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing*

Bahrain was rated partially compliant with former SR.III as TF was not criminalised and no legal or operational framework for TFS designations. In 2012, Bahrain appointed the AML/CFT Committee as the central authority for TFS.

***Criterion 6.1*** -

*Sub-criterion 6.1a* - Cabinet Decision No.2153-05 (2012) established a National Committee for the implementation of all UNSCRs. This Committee is led by the MOFA, with members from the MOI, the Bahrain Defence Force, the NSA, MLSD, CBB, MOJ, Islamic Affairs and Endowments, Customs Affairs, Civil Aviation Affairs, and the

General Organisation of Sea Ports. This Committee is empowered to propose persons or entities to the UN for designation to the 1267/1988 lists.

*Sub-criterion 6.1b* - The aforementioned National Committee, based on input by competent authorities, is the mechanism to identify and consider targets for designation to the relevant UN Committee (MO No.2153-05).

*Sub-criterion 6.1c* - The Committee's instructions state that the Committee must be satisfied by "reasonable grounds" prior to making a designation proposal to the relevant UN Committee (Section 3, Title 3).

*Sub-criterion 6.1d* - The National Committee's instructions include written procedures for proposing persons or entities to the "United Nations list related to Al-Qaeda and Da'esh (Section 3, Title 2). However, no similar guidance exists regarding proposals to the 1988 UN Committee. Bahrain has not yet submitted names to any UN committee.

*Sub-criterion 6.1e* - The authorities stated the National Committee would provide as much relevant information to support a proposal for designation as possible, including identifying information and a statement of case. The Committee's instructions state that the National Committee would submit the listing to the United Nations "through the guidelines provided" by the United Nations (Section 3, Title 2).

***Criterion 6.2*** -

*Sub-criterion 6.2a* - The National Committee is empowered to make domestic designations in relation to UNSCR 1373, and is composed of the relevant members to implement a domestic designation (Section 3, Title 3).

*Sub-criterion 6.2b* - The National Committee is empowered to identify targets for domestic designation pursuant to UNSCR 1373, and the instructions list criteria for designation (Section 3, Title 4). The Committee "provides the administrative court with the names of the designation, as the domestic list issued by the Cabinet is an administrative decision" (Section 3, Title 1).

*Sub-criterion 6.2c* - The National Committee's instructions state that the Committee has the authority to make a prompt determination to implement designations from other countries (Section 3, Title 5).

*Sub-criterion 6.2d* - The National Committee considers "integrating the names of individuals and entities on the domestic list from other states if the Committee is satisfied by the reasonable grounds as to why the individual or entity has been designated" (Section 3, Title 3). The instructions also state that Bahrain does not make designation conditional on a criminal proceeding (Section 3, Title 5).

*Sub-criterion 6.2e* - Bahrain has not submitted any names to other countries for designation. Bahrain notes that it would use diplomatic channels to relay its requests and would provide specific information to support such a designation.

***Criterion 6.3*** -

*Sub-criterion 6.3a* - Bahrain has the ability to collect or solicit information to identify persons and entities for designation through its National Committee, whose members include the MOI and the PPO, both of which have investigatory powers (Cabinet Decision no.2153-05).

*Sub-criterion 6.3b* - The National Committee's is authorised to operate *ex parte* against a person or entity who has been identified and to propose the person's designation to the administrative court (Section 3, Title 1).

***Criterion 6.4*** - The CBB requires financial institutions to freeze, without delay, the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the UN Security Council under Chapter VII of the Charter of the UN (FC Modules). No transposition or additional action is required for financial institutions to implement TFS obligations pursuant to UN Chapter VII decisions, according to the FC Module. Nevertheless, this obligation is supplemented by directives issued by the CBB in relation to changes to the UN lists, which are also legally enforceable. A similar, legally enforceable, provision exists in relation to the screening and freezing obligations for MOICT registered entities [real estate agents which are structured as companies (until September 2017 at which point, real estate sector was transferred to a separate authority, RERA under SLRB), DPMS, accountants and auditors] (MOICT 2014 TFS Guidance; Art.2 of MO 173). No such legally enforceable provision exists for lawyers, notaries, and real-estate agents/brokers (since September 2017 when they became supervised by RERA). DNFBPs supervised by the MOICT receive a notification from the MOICT via an RSS feed, alerting them to changes to the UN lists and have a legal obligation, similar to that of financial institutions, to implement without delay, upon notification.

***Criterion 6.5*** -

*Sub-criterion 6.5a* - Bahrain does not require all natural and legal persons in Bahrain to freeze, without delay and without prior notice, the funds or other assets of designated persons or entities. However, financial institutions have TFS obligations under the FC Module and CBB Directives to implement without delay. Real estate agents which are structured as companies (until September 2017 at which point, real estate sector was transferred to a separate authority, RERA under SLRB), DPMS and accountants and auditors are covered by MOICT 2014 TFS Guidance; Art.2 of MO 173. No such requirement exists for lawyers, notaries, and real-estate agents/brokers (since September 2017).

S*ub-criterion 6.5b* - In regard to financial institutions, Bahrain's freezing requirement extends to the "funds or other assets" of designated persons or entities (FC Module). No funds or other assets are to be made available, directly or indirectly, to or for the benefit of, any designated person or entity designated (FC Module). Registered entities of the MOICT have legal obligations regarding searching and freezing assets belonging to a designated individual or entity (MOICT 2014 TFS Guidance; Art.2 of MO 173). Lawyers, notaries, and real-estate agents/brokers do not have legal requirements in relation to screening/freezing/reporting of designated persons or entities' funds or assets.

S*ub-criterion 6.5c* - Bahrain prohibits financial institutions and real estate agents which are structured as companies (until September 2017 at which point, real estate sector was transferred to a separate authority, RERA under SLRB), DPMS, accountants and auditors from making any funds or other assets or other related services, available in any way for the benefit of designated persons and entities (FC Module; CBB Directives; MOICT 2014 TFS Guidance; Art.2 of MO 173). However, Bahrain does not have legally enforceable measures that apply to all natural and legal persons in Bahrain.

S*ub-criterion 6.5d* - Bahrain has a mechanism in place to communicate designations to financial institutions and to some DNFBPs immediately upon changes to the relevant lists. For financial institutions, the CBB issues directives upon changes to the UN lists (i.e. listings and delistings). Similarly, the MOICT provides email notifications to its registered entities. The MOICT also provides automatic updates to its registered entities who subscribe to its RSS feeds. The MOJ does not provide such notification to lawyers and notaries, nor does the RERA to real estate agents/brokers. The CBB provides limited guidance to financial institutions in its FC Module. Limited guidance is available to DNFBPs.

S*ub-criterion 6.5e* - The CBB requires financial institutions to verify that they have no dealings with designated persons and entities, and report their findings to the CBB (FC Module). Further, the CBB directives state that "licensees are required to report all balances and details of any assets that were frozen based on the instructions stated above. Licensees who have no such funds or claims must also notify the CBB of such information. All reports and notifications from Licensees are required to be filed with the CBB within two weeks of receiving this Directive". The MOICT does not require its reporting entities to respond to its email notifications.

S*ub-criterion 6.5f* - Bahrain has established that the rights of bona fide third parties are protected (as established through case studies).

***Criterion 6.6*** -

S*ub-criterion 6.6a* - Bahrain's National Committee oversees delistings. The process for considering and submitting delistings is included in the Committee's instructions, and made available on the website of MOFA. The delisting procedures contained in the Committee's instruction are extracts of those of the relevant UN Committees.

S*ub-criterion 6.6b-c* - The National Committee's instructions includes procedures for delistings pursuant to UNSCR 1373 (Title 1, Section 4). The National Committee has a form petitioners are to use to request to have a freezing order removed. The form is available on the website of MOFA.

S*ub-criterion 6.6d-e* - The central point for making a delisting request is the MOFA. Information is available to the public on its website regarding the procedure on submitting an application for delisting.

S*ub-criterion 6.6f* - In its directives to financial institutions, the CBB instructs all recipients to respond regarding frozen accounts, or lack thereof, as well as provides communication details to seek assistance in assessing false positives. In its email notifications, the MOICT does not require its entities to respond regarding frozen accounts, or lack thereof, but it does provide communication details for the assistance in the case of false positives.

S*ub-criterion 6.6g* - Upon delistings of persons or entities designated by the UN, the CBB and MOICT communicate these changes to their registered entities. Such information is not communicated to lawyers, notaries, and real-estate agents/brokers.

***Criterion 6.7*** - The CBB permits bank licensees to disburse or use frozen funds, upon permission in writing from the CBB (FC Module). Bahrain provided a case study where an individual was able to access frozen funds for basic living

exemptions (individual's assets were frozen pursuant to a court order). The MOICT does not have a similar procedure.

### *Weighting and Conclusion*

Bahrain has a legal framework for financial institutions and most DNFBPs to implement UNSCR 1267 and 1988 (and successor resolutions) without delay. However, this framework does not extend to all natural and legal persons in Bahrain, nor to lawyers, notaries, and real estate agents/brokers, which has an impact in several criteria in this Recommendation. There is no guidance regarding proposals to the 1988 UN Committee (See criterion 6.1 d). Limited guidance is available to DNFBPs. Additionally, the MOICT does not require its reporting entities to respond to its email notifications.

The MOICT does not have a procedure to allow access to funds (See criterion 6.7). Bahrain has the authority to designate entities domestically and to consider third party designations.

**Recommendation 6 is rated Partially Compliant.**

## *Recommendation 7 – Targeted financial sanctions related to proliferation*

This Recommendation was added to the Standard in 2012. Bahrain has, therefore, not previously been assessed against this Recommendation.

***Criterion 7.1*** - Financial institutions and registered entities of MOICT (jewellers and precious metals dealers, auditors, accountants, and real estate agents which are structured as companies) are required to implements TFS related to PF without delay. The CBB requires financial institutions to freeze, without delay, the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the UN Security Council under Chapter VII of the Charter of the UN (FC Modules). No transposition or additional order action is required for financial institutions to implement TFS obligations pursuant to UN Chapter VII decisions, according to the FC Module. Nevertheless, this obligation is supplemented by directives issued by the CBB in relation to changes to the UN lists, which are also legally enforceable. A similar, legally enforceable, provision exists in relation to the screening and freezing obligations for real estate agents which are structured as companies (until September 2017 at which point, real estate sector was transferred to a separate authority, RERA under SLRB), DPMS, accountants and auditors (MOICT 2014 TFS Guidance; Art.2 of MO 173).

***Criterion 7.2*** -

*Sub-criterion 7.2a* - Bahrain does not require all natural and legal persons to freeze funds without delay and without prior notice, the funds or other assets of designated persons or entities. However, financial institutions have PF TFS obligations under the FC Module and CBB Directives to implement without delay. The following DNFBPs are covered by MOICT 2014 TFS Guidance; Art.2 of MO 173: real estate agents which are structured as companies (until September 2017 at which point, real estate sector was transferred to a separate authority, RERA under SLRB), DPMS,

accountants and auditors. No such requirement exists for lawyers, notaries, and real estate agents/brokers.

*Sub-criterion 7.2b* - In regard to financial institutions, Bahrain's freezing requirement extends to the "funds or other assets" of designated persons or entities. It also states that no funds or other assets are to be made available, directly or indirectly, to or for the benefit of, any designated person or entity designated (FC Module). Registered entities of the MOICT have legal requirements in relation to searching and freezing designated persons or entities' funds or assets (MOICT 2014 TFS Guidance; Art.2 of MO 173). No such requirement exists for lawyers, notaries, and real-estate agents/brokers.

*Sub-criterion 7.2c* - Bahrain prohibits financial institutions and registered entities of MOICT from making any funds or other assets or other related services available in any way for the benefit of designated persons and entities (See c6.5b). However, Bahrain does not require this of all natural and legal persons in Bahrain.

*Sub-criterion 7.2d* - Bahrain has a mechanism in place to communicate designations to financial institutions and registered entities of MOICT upon changes to the relevant lists. For financial institutions, the CBB issues directives upon changes to the UN lists (i.e. listings and delistings). Similarly, the MOICT provides email notifications to its registered entities. The MOJ does not provide such notification to lawyers and notaries, nor does the RERA to real estate agents/brokers. The CBB and MOICT provide limited guidance to their respective entities.

*Sub-criterion 7.2e* - The CBB requires financial institutions to verify that they have no dealings with designated persons and entities, and report their findings to the CBB (FC Module). Further, the directives state that "Licensees are required to report all balances and details of any assets that were frozen based on the instructions stated above. Licensees who have no such funds or claims must also notify the CBB of such information. All reports and notifications from Licensees are required to be filed with the CBB within two weeks of receiving this Directive". The MOICT does not require its reporting entities to respond to its email notifications.

*Sub-criterion 7.2f* - Bahrain has established (through case studies) that the rights of bona fide third parties are protected.

***Criterion 7.3*** - Bahrain has measures and procedures in place for ensuring compliance with UN sanctions by financial institutions. The FC module allows the CBB to impose a penalty of up to BHD 100 000 (EUR 431 077) on a licensee for failing to comply with the FC Module, without the need of a court order and at the CBB's discretion. These penalties can be multiplied by the number of violations. In addition to monetary penalties, the CBB has the power to impose conditions, including appointing an observer member on the board of directors or placing the licensee under administration (see c.27.4). The MOICT also has the power to issue administrative penalties for violation with MO 173 (see c.28.4), which includes the rejection or suspension of compliance officers, and penalties set out in Decree Law No.4 (2001). Lawyers, notaries, and real estate agents/brokers are not monitored for compliance with TFS.

***Criterion 7.4*** -

*Sub-criterion 7.4a* - The National Committee oversees delisting requests to the relevant UN Committee. The process for considering and submitting petitions for delistings is included in the Committee's instructions. Information on delisting applications to the relevant UN Committee is also publically available on the website of MOFA.

*Sub-criterion 7.4b* - In its directives to financial institutions, the CBB instructs all recipients to respond regarding frozen accounts, or lack thereof, as well as provides communication details to seek assistance in assessing false positives. In its email notifications, the MOICT does not require its entities to respond regarding frozen accounts, or lack thereof, but it does provide communication details for the assistance in the case of false positives.

*Sub-criterion 7.4c* - The CBB permits bank licensees to disburse or use frozen funds, upon permission in writing from the CBB (FC Module). The MOICT does not have a similar procedure.

*Sub-criterion 7.4.d* - Upon delistings of persons or entities designated by the UN, the CBB communicates this information to its licensees. The MOICT also communicates these changes to its supervised entities, via email or automatically through RSS feeds. Such information is not communicated to lawyers, notaries, and real-estate agents

***Criterion 7.5*** *(a)-(b)* - The CBB permits bank licensees to permit the addition or disbursement to or from frozen accounts of interest or other earnings due on those accounts or payments due under contracts, agreements or obligations, upon permission in writing from the CBB (FC Module). The MOICT does not have a similar procedure.

### *Weighting and Conclusion*

Bahrain has a legal framework for financial institutions and most DNFBPs to implement UNSCRs related to Iran and the DPRK, without delay. However, there are no explicit legal obligations that apply to all natural and legal persons in Bahrain from making funds or other assets available to designated persons or entities, which has an impact in several criteria in this Recommendation. Moreover, no obligations exist for lawyers, notaries, and real estate brokers. The CBB and MOICT have provided limited guidance to its reporting entities. The MOICT does not require reporting entities to respond to email notifications and does not have a procedure to allow access to funds [See criterion 7.4 c and 7.5 (a) – (b)].

**Recommendation 7 is rated Partially Compliant.**

## *Recommendation 8 – Non-profit organisations*

Bahrain was rated partially compliant with former SR.III as it did not have an effective framework for assessing compliance with NPO's regulatory requirements. There was a need for increased resources and the development of a risk-based approach to focus on higher risks. Since then, Recommendation 8 was revised to follow a more risk-based approach and focus on those NPOs that not only meet

FATF definition, but are at most risk for TF. For context a brief description of the NPO regime in Bahrain is included in Chapter 1.

***Criterion 8.1*** -

a) Bahrain conducted a review of its NPO sector in 2016. 417 out of 618 NPOs were identified as low risk, 106 identified as moderate risk and 95 NPOs were identified as high risk. Out of those high risk NPOs, 55 were identified as being at TF risk. One of the aspects taken into consideration by the MLSD to determine NPOs with high risk for TF included having a reserve amount of over BHD 200 000 (EUR 431 077) and overseas financial transactions, which were considered as potential links to TF. The MLSD also took into account that although not related to TF, three NPOs were found involved in illegal fundraising and mismanagements (i.e. using funds for own benefit).

While these indicators have helped Bahrain identify those NPOs at TF risk, Bahrain's NPO risk assessment needs to be further refined to focus specifically on TF risks. Authorities have engaged with an external expert facilitated through technical assistance since 2015, to address the matter of risk management of NPOs, and particularly to adapt to the new requirements of R.8. Authorities will continue to work in refining their risk assessment and consequent risk-based approach supervision.

b) Bahrain identified one main method which can be used to abuse NPOs, according to its draft NRA: the misuse of religious tax and contributions or donations, which are in many instances collected in Bahrain. Results of Bahrain's NPO risk assessment was shared with the FID for comment on risk categories, to ensure they adequately reflected the understanding of TF risk in the NPO sector.

c) Bahrain undertook an initial review of the adequacy of laws and measures regarding subset of NPOs that may be abused for TF support, with the assistance of a consultancy firm. However, currently all NPOs are subject to the same licensing and pre-approval of transfers requirements described in Chapter 1. This could be nuanced to also follow a risk-based approach.

d) The MLSD instituted a programme to annually review all NPOs since the first quarter of 2017, based on Administrative Instructions by the NPO Support Directorate, to identify any residual TF risk, update and further refine their understanding of risk. Updates would also be made immediately after financial reports or other information received by the MLSD indicates changes in the risk profile assigned to a given NPO.

***Criterion 8.2*** -

a) Bahrain has several measures to promote accountability, integrity and public confidence in the administration and management of NPOs which include advice on administrative, financial and accounting issues. Bahrain has measures regarding the supervision of associations and sanctions for failure to comply with the provisions of Decree Law no.21 (1989) (Art. 22, 89-92), which refer to associations being supervised by the MLSD and the possibility of sanctions for including, the public collection of funds without due authorisation or permit. The MLSD collects and publishes information on the NPO's governance and activities in their website, and investigates any maladministration or complaint by the public. This could be

deemed to provide the public with some confidence about NPOs operating in Bahrain. Bahrain's authorities also indicated that they use dedicated resources in the MLSD website and a National NPO support centre for the gulf countries, which was established to further develop the capabilities of NPOs.

b) Bahrain has not encouraged or conducted outreach and educational programmes particularly related to TF, however one roundtable with 20 out of the 54 NPOs at TF risk was held in September 2017, to discuss TF risks. Other support training has been provided to NPOs, regarding NPOs general management, since 2006. Bahraini authorities indicated that following this initial consultation, an outreach programme for NPOs at risk is under development. Bahrain's authorities also indicated that they use dedicated resources in its website [www.mlsd.gov.bh/en/ngos] to offer advice and support to NPOs (although not specific for TF).

c) Bahrain is in the process of developing best practices to address terrorist financing risk and vulnerabilities, in order to protect NPOs from terrorist financing abuse. A meeting was held with NPOs in September 2017, as noted in b) above, which also contributed to this.

d) Bahrain encourages NPOs to conduct transactions via regulated financial channels. Every NPO is required to have a bank account and this bank is monitored by the MLSD in co-ordination with the CBB. For instance, associations need to deposit cash using their registration name, at one of the banks operating in Bahrain and licensed by CBB, and to notify the authorities of the bank's name and of any subsequent changes to bank details, within one week from the change [Art. 17 of Decree Law No.21 (1989)]. All NPOs and actually any individual involved in fundraising requires authorisation from the MLSD pursuant to Decree no.21 (2013), particularly Art. 2, as also noted in Chapter 1 of the MER. In addition, private institutions are explicitly not allowed to receive donations or grants unless pre-authorized by the MLSD (Art. 83 of Decree Law (21) 1989).

***Criterion 8.3*** - The MLSD implemented a number of measures towards NPOs considered at TF risk, which included: i) assigning a specific MLSD email address for direct communication and ease of enquiries, ii) setting up office consultation hours through their Non-Governmental Organisations (NGO) support centre, iii) holding periodic workshops during the year to develop the efficiency and financial management of the organisation by local and international experts, iv) field visits to the NPO headquarters to assess and audit the organisation's financial performance, v) meeting with the board of directors of the organisation and/or founders to provide assistance, vi) evaluation of institutional performance, and follow-up and review of CBB's statements for overseas transactions. In addition, Bahrain has measures to identify and supervise associations in general. For instance, all NPOs need to be registered with the MLSD and need to provide information on their activities and officials (Art. 1 and 2 of Decree Law No.21 (1989). NPOs have to provide detailed financial statements every year and those with yearly revenues or expenses over BHD 10 000 (EUR 21 550), should have their financial report reviewed by an external auditor. The MLSD reviews all financial reports.

***Criterion 8.4*** -

a) Bahrain, to a certain extent, identified the NPO sub-sector at TF risk and indicated onsite or field visits are to be performed which apply this focus; however NPOs have

been monitored since 2005. The MLSD monitors all NPOs, including those at TF risk, through for instance, the review of annual reports received and financial statements.

b) NPOs or persons acting on behalf of NPOs can be sanctioned for failing to comply with the provisions of Decree Law No.21 (1989), according to Art. 89 of that law. Registration can also be refused if certain criteria are not met. In case of illegal fundraising or any suspected TF abuse, the MLSD would refer and has referred the case to the police or FID.

***Criterion 8.5*** -

*a)* The MLSD coordinates with the CBB and with the FID, with regard to NPOs transfers overseas and separately, with the MOFA for the registration of foreign NPOs in Bahrain and to investigate any NPO request to be a member in a foreign organisation. The MLSD can also verify the source of funds for NPOs seeking to acquire real estate or the suitability of founding members of an NPO or boards of directors, through FID and the CID. The MLSD is also part of the National Policy Committee and cooperates with other Ministries such as the MOJ, to monitor NPOs fundraising activities.

*b)* The FID and the PPO have had cases of funding without due license (related to fraud or ML), which have been investigated and prosecuted and which show their capabilities and expertise to examine NPOs suspected of either being exploited for, or actively supporting terrorist activity or organisations.

*c)* The MLSD routinely receives and has received detailed financial and programmatic information from NPOs. In addition, Art. 15, 16, 32 and 33 of Decree Law No.21 (1989) give MLSD the right to examine records at any time; the need for each society to have a budget; among other elements of governance for associations.

*d)* The MLSD has direct communication with the FID and other relevant authorities and this enables it to promptly share information on any suspicion or reasonable grounds to suspect that a particular NPO may be involved in terrorist financing abuse.

***Criterion 8.6*** - Authorities indicated that requests for information regarding NPOs can be addressed through Egmont secure channels with the FIU being the main point of contact for requests for information. The FID works very closely with the MLSD in its role of authorising fundraising activities and incoming and outgoing transfer of funds. This facilitates communications and the possibility of routing any request for international co-operation through the FID, should it be necessary. Authorities indicated that the need has not arisen thus far. Requests could also be routed through the MOFA, especially with regard to foreign NPOs or overseas transactions.

### *Weighting and Conclusion*

Bahrain has a regulatory framework for NPOs and has identified NPOs at TF risk, but is still in the process of following a more risk-based approach, which addresses those risks. This has an impact in compliance with several criteria within this Recommendation (See criterion 8.1(a) and (c) and 8.2 and 8.4). Bahrain's NPO risk assessment needs to be further refined to focus specifically on TF risks. Bahrain has

not encouraged or conducted outreach and educational programmes particularly related to TF.

**Recommendation 8 is rated Largely Compliant.**

## *Recommendation 9 – Financial institution secrecy laws*

Bahrain was rated largely compliant with former R.4 as no onsite inspections had been conducted for the insurance and capital market licensees.

***Criterion 9.1*** - Secrecy of accounts held by FIs does not impede the implementation of the FATF Recommendations. No institution can plead before the PPO or the competent Court, secrecy or confidentiality in respect of accounts, identification of customers or record keeping provided under the provisions of any Law (Art.7 of Decree Law No.4 (2001)). Further, confidential information must not be disclosed by a licensee unless such disclosure is done in compliance with the provisions of the law or any international agreements to which Bahrain is a signatory, in the process of executing an order issued by a competent Court, or for the purpose of implementing an instruction given by the Central Bank among which are the AML/CFT requirements (Art. 117 of the CBB law).

**Sharing of information between competent authorities domestically and internationally:** The FID and the relevant entities in Bahrain can exchange information of a general nature regarding the ML offence with competent authorities in foreign States (Art.9 of the Decree Law No.4 (2001). The FID shall in response to a reasonable request from a competent authority in a foreign State provide to that competent authority specific information relating to suspicious transactions or persons and corporations involved in those transactions or the investigation or prosecution of a ML offence.

**Sharing of information between Financial Institutions:** FIs may share information with other FIs for the purpose of implementing a clear instruction given by the CBB in accordance with Art. 116 and 117 of the CBB Law.

### *Weighting and Conclusion*

**Recommendation 9 is rated Compliant.**

## *Recommendation 10 – Customer due diligence*

Bahrain was rated partially compliant with former R.5 as CDD improvements were required for the licensees in the capital markets and licensed inurance companies.

***Criterion 10.1*** - Art. 5 (h) of Decree Law No.4 (2001) states that institutions shall not open or keep any secret, fictitious, or anonymous accounts.

The CBB is the sole regulatory authority of the FIs; banks, insurance companies, companies dealing in securities, portfolios and investment funds, financing companies, money exchange companies, money brokers and mediators, insurance brokers, mediators of the securities market, consultancy firms dealing in the financial service industry, credit rating firms, Bahrain securities market, capital markets, and precious metals and strategic commodities markets, financial sector

support institutions, including institutions licensed to provide financial services according to Islamic Sharia principles.

No person shall carry out financial services provided by financial institutions in the Bahrain unless licensed by the Central Bank. The CBB supervises and controls the regulated services provided by FIs Institutions (Art. 39, 40, 44 and 45 of the CBB Law).

Rulebooks (Vol.1- 6 all under sub-paragraphs in FC-1.1) issued by the CBB for FIs under its supervision regulates the maintenance of accounts in this regard by requiring FIs not to establish or keep anonymous accounts or accounts in fictitious names. Where insurance licensees maintain a nominee account, which is controlled by or held for the benefit of another person, the identity of that person must be disclosed to the insurance licensee and verified.

***Criterion 10.2*** - The CBB Rulebook (Vol. 1-6 FC-1.1) requires FIs to implement the CDD measures when:

a) establishing business relations with a new or existing customer;

b) carrying-out one-off or occasional transactions above BHD 6 000 (EUR 13 000), or where several smaller transactions that appear to be linked fall above this threshold;

c) carrying out wire transfers irrespective of amount;

d) there is a suspicion of ML or TF;

e) having doubts about the veracity or adequacy of previously obtained customer due diligence information;

***Criterion 10.3*** - Based on the CBB Rulebook, (Vol. 1-6 FC-1.1 on CDD), FIs must establish effective systematic internal procedures for establishing and verifying the identity of their customers and the source of their funds and implement the CDD measures in specific cases. FIs are also required to understand, and as appropriate, obtain information on the purpose and intended nature of the business relationship, and obtain and record the following information before providing financial services of any kind: (a) Full legal name and any other names used; (b) Full permanent address (i.e. the residential address of the customer; a post office box is insufficient); (c) Date and place of birth; (d) Nationality; (e) Passport number (if the customer is a passport holder); (f) CPR or Iqama number (for residents of Bahrain or GCC states); (g) Telephone/fax number and email address (where applicable); (h) Occupation or public position held (where applicable); (i) Employer's name and address (if self-employed, the nature of the self-employment); (j) Type of account, and nature and volume of anticipated business dealings with the financial institution; (k) Signature of the customer(s); and (l) Source of funds. FIs are required to verify the above mentioned information by the specific methods.

***Criterion 10.4*** - The CBB Rulebook, (Vol. 1-6 FC-1.1 on CDD) requires FIs to obtain a signed statement from all new customers confirming whether or not the customer is acting on their own behalf. This undertaking must be obtained prior to conducting any transactions with the customer concerned and that where a customer is acting on behalf of a third party, the FIs must also obtain a signed statement from the third party, confirming they have given authority to the customer to act on their behalf. Where the third party is a legal person, the FIs must have sight of the original Board

resolution (or other applicable document) authorising the customer to act on the third party's behalf, and retain a certified copy. Also FIs must establish and verify the identity of the customer and (where applicable) the party/parties on whose behalf the customer is acting, including the beneficial owner of the funds, and where financial services are provided to a minor, the FIs must additionally verify the identity of the parent(s) or legal guardian(s). Where a third party on behalf of a person lacking full legal capacity wishes to open an account, the FIs must establish the identity of that third party as well as the intended account holder.

***Criterion 10.5*** - The CBB Rulebook (Vol. 1-6 FC-1.1 on CDD) requires FIs to enquire as to the structure of the legal entity or trust sufficient to determine and verify the identity of the ultimate beneficial owner of the funds, the ultimate provider of funds (if different), and the ultimate controller of the funds (if different), ascertain whether the legal entity has been or is in the process of being wound up, dissolved, struck off or terminated, obtain the names, country of residence and nationality of directors or partners (only necessary for private or unlisted companies), require, through new customer documentation or other transparent means, updates on significant changes to corporate ownership and/or legal structure, obtain and verify the identity of shareholders holding 20% or more of the issued capital, and in the case of trusts or similar arrangements, establish the identity of the settler(s), trustee(s), and beneficiaries.

For the purposes of identifying and verifying beneficial ownership, acceptable means of undertaking such due diligence might include taking bank references; visiting or contacting the company by telephone; undertaking a company search or other commercial enquiries; accessing public and private databases (such as stock exchange lists); making enquiries through a business information service or credit bureau; confirming a company's status with an appropriate legal or accounting firm; or undertaking other enquiries that are commercially reasonable. Bahrain defines beneficial owner as "the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement. This definition should also apply to "ultimate beneficial ownership"

***Criterion 10.6*** - The CBB Rulebook (FC-1.1.2A) requires FIs to understand, and as appropriate, obtain information on the purpose and intended nature of the business relationship.

***Criterion 10.7*** - The CBB Rulebook (FC-1.1.2B) requires FIs to:

(a) conduct ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds;

(b) implement the customer due diligence measures when a change to the signatory or beneficiary of an existing account or business relationship is made, take reasonable steps to ensure that they receive and maintain up-to-date copies of specific identification documents, require all customers to provide up-to-date identification documents in their standard terms and conditions of business, and review and update their customer due diligence information at least every three years. If, upon

performing such a review, copies of identification documents are more than 12 months out of date, the licensees must take steps to obtain updated copies as soon as possible.

***Criterion 10.8*** - The CBB Rulebook (FC-1.1.2A) requires FIs to understand, and as appropriate, obtain information on the purpose and intended nature of the business relationship. If the customer is a legal entity or a legal arrangement such as a trust, FIs must (FC-1.2.7) obtain and record specific information from original identification documents, databases or websites, in hard copy or electronic form, to verify the customer's legal existence and structure (FC-1.2.11). FIs must also obtain and document information on the structure of the legal entity or trust sufficient to determine and verify the identity of the ultimate beneficial owner of the funds, the ultimate provider of funds (if different), and the ultimate controller of the funds (if different), obtain the names, country of residence and nationality of directors or partners (only necessary for private or unlisted companies), and require, through new customer documentation or other transparent means, updates on significant changes to corporate ownership and/or legal structure, and obtain and verify the identity of shareholders holding 20% or more of the issued capital (where applicable).

According to the FC-1.2.11/f of the CBB Rulebook, FIs must, in the case of trusts or similar arrangements, establish the identity of the settler(s), trustee(s), and beneficiaries (including making such reasonable enquiries as to ascertain the identity of any other potential beneficiary, in addition to the named beneficiaries of the trust).

***Criterion 10.9*** - If the customer is a legal entity or a legal arrangement such as a trust, the FIs must (Vol. 1-6 FC-1.2): (a) obtain and record specific information from original identification documents, databases or websites, in hard copy or electronic form, to verify the customer's legal existence and structure, and (FC-1.2) must also (b) obtain and document information on the structure of the legal entity or trust sufficient to determine and verify the identity of the ultimate beneficial owner of the funds, the ultimate provider of funds (if different), and the ultimate controller of the funds (if different), obtain the names, country of residence and nationality of directors or partners (only necessary for private or unlisted companies), and require, through new customer documentation or other transparent means, updates on significant changes to corporate ownership and/or legal structure, and obtain and verify the identity of shareholders holding 20% or more of the issued capital (where applicable). They should also (c) verify the customer's legal existence and structure through specific information including registered address and trading address (where applicable).

***Criterion 10.10*** - If the customer is a legal entity or a legal arrangement such as a trust, FIs must obtain and record specific information from original identification documents, databases or websites, in hard copy or electronic form, to verify the customer's legal existence and structure, and (FC-1.2.11) must also obtain and document information on the structure of the legal entity or trust sufficient to determine and verify (a) the identity of the ultimate beneficial owner of the funds, the ultimate provider of funds (if different), obtain and verify the identity of shareholders holding 20% or more of the issued capital (where applicable). They should also verify the customer's legal existence and structure, and the ultimate

controller of the funds (if different), obtain the names, country of residence and nationality of directors or partners (only necessary for private or unlisted companies), and require, through new customer documentation or other transparent means, updates on significant changes to corporate ownership and/or legal structure.

***Criterion 10.11*** - If the customer is a legal entity or a legal arrangement (structure) such as a trust or a waqf, FIs are required to obtain and record specific information and verify the customer's legal existence and structure including the entity's names, registration number, legal form, type of business activity, and source of funds, and in the case of trusts or similar arrangements, establish the identity of the settler(s), trustee(s), and beneficiaries (including making such reasonable enquiries as to ascertain the identity of any other potential beneficiary, in addition to the named beneficiaries of the trust (Vol 1- 6 FC-1.2).

***Criterion 10.12*** - Insurance licensees are required (a) to implement due diligence requirements that must be incorporated in the licensee's new business procedures. In the case of trusts or similar arrangements, establish the identity of the settlor(s), trustee(s), and beneficiaries (including making such reasonable enquiries as to ascertain the identity of any other potential beneficiary, in addition to the named beneficiaries of the trust) (FC-1.2.11/f); (b) to establish and verify the identity of the customer and (where applicable) the party/parties on whose behalf the customer is acting. In the case of insurance policies, the identity of the beneficiaries must also be separately identified and verified, and the relationship between the insured party and the beneficiaries must be ascertained (FC-1.1.8). Verification must take place in accordance with specific requirements. If claims, commissions, and other monies are to be paid to persons (including partnerships, companies, etc.) other than the policyholder, then the identity of the proposed recipient of these monies must also be verified in accordance with the requirements specified in Chapter 1 of Volume 3. Consequently, the identity of the beneficiary must be verified whenever a change was made to the policyholder, including at the time of pay-out.

***Criteria 10.13*** - Insurers are required to apply enhanced customer due diligence on customers identified as having a higher risk profile (FC-1.3.1). There is no specific requirement for FIs to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable.

***Criterion 10.14*** - FIs must not commence a business relationship or undertake a transaction with a customer before completion of the relevant customer due diligence measures, subject to certain limited exceptions as analysed in criteria 10.15 below (Vol 1- 6 FC-1.1.2).

***Criterion 10.15*** - FIs must not commence a business relationship or undertake a transaction with a customer before completion of the relevant CDD measures specified in the Rulebook (FC 1.1.10 of the CBB Rulebook). However, verification may be completed after receipt of funds in the case of non-face-to-face business, or the subsequent submission of CDD documents by the customer after initial face-to face contact, providing that no disbursement of funds takes place until after the CDD requirements have been fully met.

***Criterion 10.16*** - FIs must take reasonable steps to ensure that they receive and maintain up-to-date copies of the identification documents. Financial institutions

must require all customers to provide up-to-date identification documents in their standard terms and conditions of business. They must also review and update their customer due diligence information at least every three years. If, upon performing such a review, copies of identification documents are more than 12 months out of date, they must take steps to obtain updated copies as soon as possible (Vol. 1-6 of the FC-2.2.10 and 11).

***Criterion 10.17*** - FIs are required to perform enhanced CDD on those customers identified as having a higher risk profile, and additional inquiries are required to be made or information obtained in respect of those customers (Vol. 1-6 CBB Rulebook FC-1.3).

***Criterion 10.18*** - FIs may apply simplified CDD measures, in certain cases including if the customer is the Central Bank of Bahrain, the Bahrain Bourse, a licensee of the CBB, a Ministry of the GCC or FATF member state government, a company in which a GCC or FATF government is a majority shareholder, or a company established by decree in the GCC, a company listed on a GCC or FATF member state stock exchange, a FI whose entire operations are subject to AML/CFT requirements consistent with the FATF Recommendations and it is supervised by a financial services supervisor in a FATF or GCC member state for compliance with those requirements, or if the transaction is a one-off or occasional transaction not exceeding BHD 6 000 (or equivalent in other currencies), or one of a number of transactions which are related and, when taken together, do not exceed BHD 6 000 per year (or equivalent in other currencies), yet record retention requirements apply in this case (FC-1 of the CBB Rulebook). However, FIs are required not to apply simplified CDD measures where they know, suspect, or have reason to suspect, that a customer is engaged in ML or TF or that the transaction is carried out on behalf of another person engaged in ML or TF.

***Criterion 10.19*** - If FIs are unable to comply with the CDD requirements, they must consider whether: they should freeze any funds received and file a suspicious transaction report; or to terminate the relationship; or not proceed with the transaction; or to return the funds to the counterparty in the same method as received (FC-1.1.11/ FC-1.1.12/ FC-1.1.13 of the CBB Rulebook, Volumes 1-6).

***Criterion 10.20*** - There is a general rule in the CBB Rulebook FC-5.2 that FIs, their directors, officers and employees must not warn or tip off their customers, the beneficial owner or other subjects of the STR when information relating to them is being reported to the relevant authorities. However there is no specific provision to permit an FI to not to pursue the CDD process, and instead require it to file an STR in case it reasonably believes that performing the CDD process will tip-off the customer.

### *Weighting and Conclusion*

There are no specific requirements for FIs to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable. FIs are allowed to consider returning the funds to the counterparty, when unable to comply with CDD requirements.

No specific requirements for FIs not to pursue CDD if there is a risk of tipping off and instead file an STR. Application of requirements to structures other than trusts (e.g. waqfs) is not clear.

**Recommendation 10 is rated Largely Compliant.**

## *Recommendation 11 – Record-keeping*

Bahrain was rated largely compliant in R.11 (former R.10) because although the regulation was in place, capital markets licensees and insurance licensees had not been subject to inspection to determine implementation.

***Criterion 11.1*** - FIs are required to keep for a period of five years after the relationship has ended, a copy of the evidence of identity of each client as may be provided for in the regulations made pursuant to this Law and to keep a transaction record of any new or unrelated transaction for a period of five years after the termination of the transaction so recorded (Art. 5 of the AML Law). Also, Art.60 of the CBB Law states that accounting and other records shall be kept for at least ten years at the licensee's main office in Bahrain or at such other places as the Central Bank may approve. There are similar requirements set out in the CBB Rulebook (Vol 1 – 6 FC 7.1.1/ FC 6.1.1).

***Criterion 11.2*** - FIs are required to keep for a period of five years after the relationship has ended a copy of the evidence of identity of each client as may be provided for in the regulations made pursuant to this Law, keep a transaction record of any new or unrelated transaction for a period of five years after the termination of the transaction so recorded (Art. 5 of the AML Law). Also, the CBB Rulebook (FC-7.1**)** obliges FIs to retain adequate records in relation to evidence of identity and business relationship records (such as application forms, account files and business correspondence, including the results of any analysis undertaken, for at least five years after the customer relationship has ceased). Chapter OM-7 (Books and Records) of the Operational Risk Management Module of the CBB's Rulebook has similar requirements for FIs**.**

***Criterion 11.3*** - FIs are required to comply with the record-keeping requirements contained in the AML Law in relation to documents (including customer instructions in the form of letters, faxes or emails) enabling a reconstitution of the transaction concerned, for at least five years after the transaction was completed (FC-7, FC-6 of the CBB Rulebook, Vol 1-6).

***Criterion 11.4*** - Domestic competent authorities have the right to a prompt access to records based on FC-7, FC-6 of the CBB Rulebook stipulating prompt and swift access by the relevant authorities or other authorised persons.

### *Weighting and Conclusion*

**Recommendation 11 is rated Compliant.**

## *Recommendation 12 – Politically exposed persons*

Recommendation 6 (which formerly contained the requirements for PEPs), now R.12, was rated PC in its 3rd MER. The major deficiency noted was that apart from

banks and insurance companies, no other sector was covered under requirements. This was addressed according to Bahrain's 4th Follow-up report through the issuance of rule books by the CBB. The 2012 Recommendations have been extended to domestic PEPs and the definition now also includes persons who have been entrusted a prominent function in an international organisation.

***Criterion 12.1*** - FIs are required to (a) have appropriate risk management systems to determine whether a customer or beneficial owner is a Politically Exposed Person ('PEP'), both at the time of establishing business relations and thereafter on a periodic basis, (b) obtain senior management approval before a PEP is accepted as a customer and is also required to existing customers if they become PEPs, (c) apply CDD measures that includes obtaining written record in the customer file to establish that reasonable measures have been taken to establish both the source of wealth and the source of funds and analyse complex financial structures, including trusts, foundations or international business corporations, and (d) pursue on-going account monitoring of the PEP's account by senior management (such as the MLRO) (The CBB Rulebook- Enhanced CDD: PEPs, FC-1.5).

***Criterion 12.2*** - 'Politically Exposed Persons' is defined as individuals who are, or have been entrusted with prominent public functions in Bahrain or a foreign country, for example Heads of State or government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations or important political party officials or persons who are or have been entrusted with a prominent function by an international organisation. In this sense, requirements for the domestic PEPs, or persons who have been entrusted with a prominent function by an international organisation are covered pursuant to the CBB Rulebook Vol. 1-6 (FC- 1.5).

***Criterion 12.3*** - FIs are required to apply all types of PEP requirements to family or close associates of such PEPs, where "family" means spouse, father, mother, sons, daughters, sisters and brothers. 'Associates' are persons associated with a PEP whether such association is due to the person being an employee or partner of the PEP or of a firm represented or owned by the PEP, or family links or otherwise (The CBB Rulebook: FC-1.5).

***Criterion 12.4*** - Rulebook on insurance (FC-1.5) stipulates on general requirements for insurance licensees to have appropriate risk management systems to determine whether a customer or beneficial owner is a PEP, both at the time of establishing business relations and thereafter on a periodic basis and not specifically at the time of pay-out. Further CBB Rulebook defines 'policyholder' as a person who is the legal holder of the policy, including any person to whom, under the policy, a sum is due, a periodic payment is payable or any other benefit is to be provided or to whom such a sum, payment or benefit is contingently due, payable or to be provided. Therefore, policyholders include beneficiaries of insurance policy. FC-1.5.3 also states that where an existing customer is a PEP, or subsequently becomes a PEP, enhanced monitoring and customer due diligence measures must include:

(a) Analysis of complex financial structures, including trusts, foundations or international business corporations;

(b) A written record in the customer file to establish that reasonable measures have been taken to establish both the source of wealth and the source of funds;

(c) Development of a profile of anticipated customer activity, to be used in on-going monitoring;

(d) Approval of senior management for allowing the customer relationship to continue; and

(e) On-going account monitoring of the PEP's account by senior management (such as the MLRO).

There is no requirement to inform senior management before the pay-out of the policy proceeds, where higher risks are identified.

### *Weighting and Conclusion*

There is no specific requirement to inform senior management before the pay-out of the policy proceeds, where higher risks are identified.

**Recommendation 12 is rated Largely Compliant.**

## *Recommendation 13 – Correspondent banking*

Bahrain was rated largely compliant with former R.7. The deficiency noted was that requirements to assess CFT controls were not yet in place.

***Criterion 13.1*** - The CBB Rulebook requires banks to apply CDD measures in the normal way on the respondent bank (FC-1.8.1 and 1.8.3). FC 1.11.2 also requires that where the account is a correspondent banking relationship, EDD applies. However, FC-1.8.1 which provides for EDD in case of correspondent banking relationships, allows for simplified measures applicable for FATF/GCC banks. Banks that intend to act as correspondent banks must:

a. Gather sufficient information (e.g. through a questionnaire) about their respondent banks to understand the nature of the respondent's business. Factors to consider to provide assurance that satisfactory measures are in place at the respondent bank include information about the respondent bank's ownership structure and management, identifying whether the respondent bank has been subject to a ML or TF investigation, and identify the extent to which the respondent bank performs on-going due diligence on customers with direct access to the account, and the condition of bank regulation and supervision in the respondent's country (e.g. from published FATF reports).
b. Provide assurance that satisfactory measures are in place at the respondent bank through the respondent's AML/CFT controls.
c. Ensure that the correspondent banking relationship has the approval of senior management.
d. Complete a signed statement that outlines the respective responsibilities of each institution in relation to ML detection and monitoring responsibilities.

***Criterion 13.2*** - In the case of 'payable through' accounts, financial institutions are required (FC-1.8) to get a confirmation that (a) the respondent bank has verified the identity of any third party entities that will have direct access to the correspondent banking services without reference to the respondent bank, and (b) the respondent bank is able to provide relevant customer identification data on request to the correspondent bank

***Criterion 13.3*** - Based on the CBB Rulebook (FC-1.8/1.10), bank licensees must refuse to enter into or continue a correspondent banking relationship with a shell banks and are also required not to establish business relations with shell banks; they must not knowingly establish relations with banks that have relations with shell banks and must make a suspicious transaction report to the Anti-Money Laundering Unit and the Compliance Directorate if they are approached by a shell bank or an institution they suspect of being a shell bank.

### *Weighting and Conclusion*

The FC Module allows for simplified CDD measures for FATF/GCC banks in the context of correspondent banking relationships. All other criteria are met.

**Recommendation 13 is rated Largely Compliant.**

## *Recommendation 14 – Money or value transfer services*

Bahrain was rated compliant with former SR.VI.

***Criterion 14.1*** - Regulated Services shall mean the financial services provided by the FIs and that the CBB shall issue regulations specifying the Regulated Services and organising the provision of these services (Art.39 of the CBB Law). The CBB shall supervise and control any licensees providing such services. Also, Art. 40 of the same Law states that no person shall carry out a Regulated Service in Bahrain unless licensed by the Central Bank and that no FI shall be established without the approval of the Central Bank. CBB has issued a detailed Rulebook on the licensing requirements for providers of regulated conventional banking services. (LR-1.3.1 states that Regulated banking services include the activities, carried on by way of business, for (m) providing money exchange/remittance services; or (n) issuing/administering means of payment).

***Criterion 14.2*** - Persons breaching licensing requirements are considered in breach of Resolution No.16 (2012) (on prohibiting the marketing of financial services in Bahrain) and are subject to penalties under Art.129 of the CBB Law that imposes administrative fines against violators of the Law through imposing the licensee an administrative fine not exceeding twenty thousand (BHD 20 000), if the licensee breeches the provisions of this law or the regulations and resolutions issued in connection with implementing thereof. Art.161 of the CBB Law also more specifically imposes penalties against violators of licensing requirements in (Art. 40-41) stating that without prejudice to any greater penalty prescribed under the Penal Code or any other law, any person who contravenes the provisions of Art. 40, 41, and the Regulations issued according to Art. 42 of this law shall be liable to a fine not exceeding one million (BHD 1 000 000), and the Court shall confiscate the proceeds of the crime. Bahrain reported that no cases were identified where action was needed against unlicensed providers and monitoring of unlicensed activity is exercised through, among other means, the business registration process.

***Criterion 14.3*** - The Central Bank shall supervise and control any licensees providing such services (Art.39 of the CBB Law). Licensees must be able to produce this information for inspection immediately upon request by the CBB (FC-3.2.2). Authorities provided that there is a mechanism for supervision conducting on-site

examinations, off-site supervision and follow-up visits. The CBB also conducts the analysis of STRs to aid its supervisory functions such as on-site/off-site supervision.

***Criterion 14.4*** - Regulated Services shall mean the financial services provided by the FIs and that the Central Bank shall issue regulations specifying the Regulated Services and organising the provision of these services (Art.39 of the CBB Law). This implies that any service that could be provided by an FI, including money or value transfer, would be a Regulated Service and according to Art.40 of the same Law, no person shall carry out a Regulated Service in Bahrain unless licensed by the Central Bank and no FI shall be established without the approval of the Central Bank. CBB also issued a detailed Rulebook on the licensing requirements for providers of regulated conventional banking services. In addition, when FC- Volumes 1 and 2 of the CBB Rulebook refer to Authorised MTVS, they clarify that this would be a bank or other licensee (such as a money changer) specifically authorised for money or value transfers.

***Criterion 14.5*** - FC Module 5 (4.3.1) requires licensees to review the effectiveness of its AML/CFT procedures at least once every year. The review must cover the licensee, its branches and subsidiaries and the outcomes for each segment of the licensee's business. However there is no explicit requirement that MVTS providers should include their agents in their AML/CFT programmes and monitor them for compliance.

### *Weighting and Conclusion*

There are no explicit requirements that MVTS providers should include their agents in their AML/CFT programmes and monitor them for compliance.

**Recommendation 14 is rated Largely Compliant.**

## *Recommendation 15 – New technologies*

This Recommendation (formerly R.8) was rated partially compliant because measures to deter ML/TF threats arising from new technologies needed to be put in place and regulations for insurance and capital markets licensees on non-face-to-face account opening needed to be developed. This was addressed according to its 4th FUR, as the Rulebooks issued by the Central Bank of Bahrain for various financial institutions require developing systems for protection against potential risks from exploiting modern technology in ML/TF.

***Criterion 15.1*** - FIs must establish specific procedures for verifying customer identity where no face-to-face contact takes place (FC-1.4.1 of the CBB Rulebooks Vol. 1-6). FIs must take additional measures in order to establish procedures to prevent the misuse of technological developments in ML/TF schemes (FC- 1.4.4). FIs must also ensure that they comply with any e-commerce laws and/or CBB Modules issued from time to time. FIs are also required to a) identify and assess the ML/TF risks that may arise in relation to the use of new or developing technologies for both new and pre-existing products. Risk assessment must take place prior to the launch of the new products, business practices or the use of new or developing technologies. Insurance licensees must take appropriate measures to manage and mitigate those risks b) mitigate the potentially higher risk associated with such business.

CBB, as the supervisory authority, identifies and assesses ML/TF risk associated with new technologies on case to case basis. Moreover, licensees are required to notify the CBB before the introduction of any new products or services or any changes in existing product/service. The CBB will respond to the concerned bank within one week of receipt of the notification if it has any observations on the new application (Business and Market Conduct Module, specifically BC-4.7.2 of the CBB Rulebook).

***Criterion 15.2*** - FIs must establish procedures to prevent the misuse of technological developments in ML/TF schemes and take additional measures in order to mitigate the potentially higher risk associated with certain customers such as non-face-to-face business (FC-1.4.4 of the CBB Rulebooks Vol. 1-6). FIs are also required to identify and assess the ML/TF risks that may arise in relation to the use of new or developing technologies for both new and pre-existing products. Risk assessment must take place prior to the launch of the new products, business practices or the use of new or developing technologies. Insurance licensees must take appropriate measures to manage and mitigate those risks.

### *Weighting and Conclusion*

**Recommendation 15 is rated Compliant.**

## *Recommendation 16 – Wire transfers*

Bahrain was rated Compliant with former SR.VII.

***Criterion 16.1*** - The CBB Rulebook requires FIs to accompany all wire transfers with information containing: a) (i) The name of the originator; (ii) The originator account number or IBAN where such an account is used to process the transaction (in the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction.); (iii) The originator's address, or national identity number, or customer identification number, or date and place of birth; and is also required to accompany wire transfers with b) (i) The name of the beneficiary; and (ii) The beneficiary account number where such an account is used to process the transaction. The originating banks are also required to ensure that wire transfers contain required and accurate originator information, and required beneficiary information (FC 3.1.11).

***Criterion 16.2*** - Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, FIs may be exempted from some of the requirements regarding originator information, provided that they include the originator's account number or unique transaction reference number, and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country (CBB Rulebook FC-3.1.7).

***Criterion 16.3*** - All transfers are subject to the same requirements referred to in 16.1 in accordance with FC-3.1.5 of the CBB Rulebook.

***Criterion 16.4*** - All transfers are subject to the same requirements referred to in 16.1 in accordance with FC-3.1.5 of the CBB Rulebook.

***Criterion 16.5*** - The CBB Rulebook requires FIs that information accompanying domestic wire transfers must also include originator information as indicated for cross-border wire transfers, unless this information can be made available to the beneficiary FI and the CBB by other means (FC-3.1.8). In this latter case, the originating FI need only include the account number or a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary.

***Criterion 16.6*** - The CBB Rulebook requires FIs that information accompanying domestic wire transfers must also include originator information as indicated for cross-border wire transfers, unless this information can be made available to the beneficiary FI and the CBB by other means (FC-3.1.8). In this latter case, the originating FI need only include the account number or a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary (FC-3.1.9). The information should be made available by the originating FI within three business days of receiving the request either from the beneficiary FI or from the CBB.

***Criterion 16.7*** - There is a general requirement for record-keeping stated in the CBB Rulebook (FC-7.1.1) requiring licensees to comply with the record-keeping requirements contained in the AML Law, and therefore retain adequate records, for the following minimum periods; (a) For customers, in relation to evidence of identity and business relationship records for at least five years after the customer relationship has ceased; and (b) For transactions, in relation to documents enabling a reconstitution of the transaction concerned, for at least five years after the transaction was completed.

***Criterion 16.8*** - The originating institution is required under FC-3.1.13 not to execute the wire transfer if it does not comply with the required and accurate originator information, and required beneficiary information, as well as maintaining all relative information.

***Criterion 16.9*** - Based on FC-3.1.14 of the CBB Rulebook, for cross-border wire transfers, banks processing an intermediary element of such chains of wire transfers must ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it. Corresponding provisions don't exist for MVTS providers.

***Criterion 16.10*** - Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record must be kept, for at least five years, by the receiving intermediary bank (FC-3.1.15 of the CBB Rulebook) of all the information received from the originating bank or another intermediary bank. Corresponding provisions don't exist for MVTS providers.

***Criterion 16.11*** - FC-3.1.16 of the CBB Rulebook requires intermediary banks to take reasonable measures to identify cross-border wire transfers that lack required originator information or required beneficiary information. Such measures are required to be consistent with straight-through processing. Corresponding provisions don't exist for MVTS providers.

***Criterion 16.12*** - An intermediary bank, as per (FC-3.1.17 of the CBB Rulebook), must have effective risk-based policies and procedures for determining (a) When to

execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) The appropriate follow-up action. Corresponding provisions don't exist for MVTS providers.

***Criterion 16.13*** - A beneficiary bank, as per (FC-3.1.18 of the CBB Rulebook), must take reasonable measures to identify cross-border wire transfers that lack required originator or required beneficiary information. Such measures may include post-event monitoring or real-time monitoring where feasible. Corresponding provisions don't exist for MVTS providers.

***Criterion 16.14*** - For wire transfers, a beneficiary bank must, according to (FC-3.1.19), verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information. Corresponding provisions don't exist for MVTS providers.

***Criterion 16.15*** - A beneficiary bank, as per (FC-3.1.20), must have effective risk-based policies and procedures for determining (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action. Corresponding provisions don't exist for MVTS providers.

***Criterion 16.16*** - Licensees are required under FC-3.2 of the CBB Rulebook, if they use the services of authorised MVTSs to effect the transfer of funds for a customer to a person or organisation in another country, that licensee must comply with requirements of the identity of its customers, the exact amount transferred for each such customer, and ability to produce this information for inspection immediately upon request by the CBB, CDD and record-keeping requirements (FC-1/FC-7), and filing an STR as appropriate. Administrative sanctions can be applied by the CBB on violators.

***Criterion 16.17*** - In the case of an authorised MVTS provider that controls both the ordering and the beneficiary side of a wire transfer, the authorised MVTS provider is required to (a) take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and (b) file an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Financial Intelligence Unit (FC-3.2.4 of the CBB Rulebook).

***Criterion 16.18*** - FIs are required to implement and comply with UNSCRs relating to the prevention and suppression of terrorism and TF (Insurance and investment business FC-7.2, FC 9.2 in Capital Market, and FC-8.2 for the rest of FIs). They must freeze, without delay, the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267(1999) and its successor resolutions as well as Resolution 2178(2014) or (ii) designated as pursuant to Resolution 1373(2001). Such institutions must also comply in full with any rules or regulations issued by the CBB in connection with the provisions of the UNSCR 1373. However, if an institution wishes, intends or has been requested to do anything that might contravene, in its reasonable opinion, the provisions of UNSCR 1373, must seek, in writing, the prior written opinion of the CBB on the matter (FC-8.2.2/ FC-7.2.2/ FC-

9.2.2). Authorities state that the CBB provided this clause to ensure the proper implementation by the licensees through guidance from the CBB; however it should be rephrased to reflect this meaning instead of being an exception.

### *Weighting and Conclusion*

There are no specific requirements for FIs other than banks for criteria 16.9-16.15. Potential exception for implementing UNSCRs in the Rulebook should be clarified.

**Recommendation 16 is rated Largely Compliant.**

## *Recommendation 17 – Reliance on third parties*

Recommendation 17 (formerly R. 9) was rated partially compliant in the 3rd round MER, because capital markets licensees, money changers, and money brokers were not covered under the requirements that were in place for banks and insurance companies. This was addressed according to Bahrain's 4th Follow-up report through the Rulebooks related to capital markets, stock brokers and specialised licensees (including foreign exchange offices) that included obligations consistent with requirements of former R.9.

***Criterion 17.1*** - The CBB Rulebook makes it mandatory that FIs accept customers introduced by other FIs or intermediaries, if they have satisfied themselves that the FI or intermediary concerned is subject to FATF-equivalent CDD measures (Vol 1/2 FC-1.9.1 / Vol 3/5 1.7.1 / Vol 4/6 1.8.2/ Vol 5 1.7.1). It is the responsibility of the institution delegating part of the CDD measures to another FI or intermediary to meet the requirements and not of the third party. FIs are also required to: (a) obtain all necessary information required pertaining to the customer's identity, the identity of the customer and beneficial owner of the funds, the purpose of the relationship and, where applicable, the party/parties on whose behalf the customer is acting, and also verify the CDD measures undertaken; and (b) get written confirmation from the introducer confirming that all customer due diligence measures required by the FATF Recommendations have been followed and the customer's identity established and verified. In addition, the confirmation must state that any identification documents or other CDD material can be accessed by the FI (though without specifically mentioning without delay) and that these documents will be kept for at least five years after the business relationship has ended, (c) perform periodic reviews ensuring that any introducer on which it relies is in compliance with the FATF Recommendations. However, there is a general rule ( FC-1.9.3) stating that the licensee must perform periodic reviews ensuring that any introducer on which it relies is in compliance with the FATF Recommendations. Where the introducer is resident in another jurisdiction, the FI must also perform periodic reviews to verify whether the jurisdiction is in compliance with the FATF Recommendations. This regulatory clause requires licensees to ensure that the introducer is present in a jurisdiction that applies the FATF's standards for regulation, supervision and monitoring.

***Criterion 17.2*** - The CBB Rulebook makes it mandatory that FIs must perform periodic reviews ensuring that any introducer on which it relies is in compliance with the FATF Recommendations (Vol 1/2 FC-1.9.3 / Vol 3/5 1.7.3 / Vol 4/6 1.8.3). Where the introducer is resident in another jurisdiction, the institution must also

perform periodic reviews to verify whether the jurisdiction is in compliance with the FATF Recommendations. The CBB also reserves the right to prohibit FIs from relying on third parties to conduct elements of the CDD process if they are located in jurisdictions that, in the opinion of the CBB, do not have adequate AML/CFT systems (FC-8.1.4)

***Criterion 17.3*** - *(Not applicable)* See criteria 17.1 and 17.2. There is no distinction made between reliance on third parties which are part of the financial group with those outside the group.

### *Weighting and Conclusion*

**Recommendation 17 is rated Compliant.**

## *Recommendation 18 – Internal controls and foreign branches and subsidiaries*

Recommendations 15 and 22, which previously contained the requirements of R.18, were rated partially compliant and largely compliant, respectively in the 3rd MER, because requirements for FT training and subsequent implementation for all financial institutions were considered necessary. High hiring standards had to be a requirement of the capital markets licensees and there was no implementation verification completed for insurance licensees. Deficiencies for former R.15 were largely addressed according to Bahrain's 4th follow up report.

***Criterion 18.1*** - Art. 5 of the AML Law (e and g) requires FIs to (a) comply with the instructions of the relevant entities (Ministries and Government entities which license, supervise and regulate institutions) regarding developing and applying internal policies, procedures and controls including the designation of compliance officers at management level to combat ML and develop audit functions to evaluate such policies, procedures and controls. In addition, the CBB Rulebooks (Vol 1/2/5 FC-6.1.6/ Vol 3/4/6 FC - 5.1.6 add that FIs (b) must develop adequate screening procedures to ensure high standards when hiring employees. These procedures must include controls to prevent criminals or their associates from being employed by FIs and (c) ensure that their AML/CFT training for relevant staff remains up-to-date. Art. 5 of the AML Law also requires FIs to (d) develop and apply a procedure to audit compliance with the provisions of that Art.

***Criterion 18.2*** - the CBB Rulebook requires financial groups to implement group-wide programs against ML and TF, including:

(a) Policies and procedures for sharing information within the group for AML/CFT purposes. This general requirement includes the appointment of an MLRO.

(b) FIs must also apply the requirements as set out in the Rulebook to all their branches and subsidiaries operating both in Bahrain and in foreign jurisdictions. MLRO has access to all transactional information relating to any financial services provided by the FIs to a customer, or any transaction conducted by the FI, and has access to all customer due diligence information obtained.

(c) There are no specific provisions to ensure adequate safeguards on the confidentiality and use of information exchanged.

***Criterion 18.3*** - FIs (Vol 1/2/4/5/6 FC-B.2 Vol.3 FC-B.3) (FC-B.2 & FC-B.3) must apply the requirements to all their branches and subsidiaries operating both in Bahrain and in foreign jurisdictions. Where local standards differ, the higher standard must be followed. Licensees must pay particular attention to procedures in branches or subsidiaries in countries that do not or insufficiently apply the FATF Recommendations and do not have adequate AML/CFT procedures, systems and controls, and where another jurisdiction's laws or regulations prevent a conventional bank licensee (or any of its foreign branches or subsidiaries) from applying the same standards contained in CBB Rulebook or higher, the licensee must immediately inform the CBB in writing. In such instances, the CBB will review alternatives with the conventional bank licensee. Should the CBB and the licensee be unable to reach agreement on the satisfactory implementation of requirements in a foreign subsidiary or branch, the financial institution may be required by CBB to cease the operations of the subsidiary or branch in the foreign jurisdiction in question.

### *Weighting and Conclusion*

There are no specific provisions to ensure adequate safeguards on the confidentiality and use of information exchanged.

**Recommendation 18 is rated Largely Compliant.**

## *Recommendation 19 – Higher-risk countries*

Bahrain was rated partially compliant with former R.21 as countermeasures were not established in regulation and the regulation only applied to FATF-identifed jurisdictions.

***Criterion 19.1*** - FC-8.1.3 of volume one of the CBB Rulebook requires that conventional banks must apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and FIs, from countries where such measures are called for by the FATF. The type of enhanced due diligence measures applied must be effective and proportionate to the risks. Identical provisions are contained in volume 2 (FC-8.1) for Islamic banks, volume 3 (FC-7.1) for insurance, volume 4 (FC-7.1) for investment business and volume 6 (AML-9.1) for capital market intermediaries. Volume 5 for specialised licensees does not include this language; it includes text (also included in the other volumes) that licensees should give special attention to any dealings they may have with countries or territories which are identified by the FATF as being non-cooperative; it is not certain that "special attention" would always lead to enhanced due diligence proportionate to the risks being undertaken even though FC-1.3.1 stipulates that enhanced CDD must be performed on those customers identified as having a higher risk profile, and additional inquiries made or information obtained in respect of those customers. Based on the language of the Rulebook, the authorities rely on FIs to ensure that they are aware of the jurisdictions in connection with which the FATF calls for enhanced due diligence; they do not issue separate notices.

***Criterion 19.2*** - FC-8.1.4 of volume one of the CBB Rulebook states that the CBB reserves the right to: refuse the establishment of subsidiaries or branches or representative offices of FIs from such jurisdictions, or from jurisdictions that, in the

opinion of the CBB, do not have adequate AML/CFT systems; limit business relationships or financial transactions with the identified jurisdiction or persons in that jurisdiction; prohibit FIs from relying on third parties located in such jurisdiction to conduct elements of the CDD process; require FIs to review and amend, or if necessary terminate, correspondent relationships with FIs in such jurisdiction; require increased supervisory examination and/or external audit requirements for branches and subsidiaries of FIs based in such jurisdiction; or require increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in such jurisdiction. The other volumes contain the same powers except for volume 5, which does not refer to any powers.

The CBB has advised that Art. 38 of the CBB Law can be used to issue binding directives to ensure that FIs apply countermeasures where there are weaknesses in countries in relation to which the FATF has called for enhanced due diligence and also in relation to other countries. It has pointed to the high risk provisions in the Rulebook and the requirements mentioned in criterion 19.1. However, it is unclear what legal basis could be used by the CBB to meet the test in Art. 38 that directives under it are "to ensure the implementation of this Law, any regulations issued in accordance to this Law and the achievement of the objectives of the Central Bank".

***Criterion 19.3*** - FC-8.1.3 of volume 1 of the FCC Rulebook states that conventional banks must give special attention to any dealings they may have with entities or persons domiciled in countries or territories which are identified by the FATF as being non-cooperative or notified to conventional banks by the CBB. The other volumes (except volume 5) contain identical provisions. However, there is no procedure to inform FIs of the concerns about weaknesses in the AML/CFT systems of other countries.

### *Weighting and Conclusion*

All FIs, save for specialised licensees, are required to apply enhanced due diligence measures when called for by the FATF. There are no specific procedures in place to ensure that FIs are advised of concerns about weakness in AML/CFT system of other countries.

**Recommendation 19 is rated Largely Compliant.**

## *Recommendation 20 – Reporting of suspicious transaction*

Bahrain was rated partially compliant with former R.13 and SR.IV as there was no obligation to report STRs related to TF for capital markets, money changers, and there was a lack of clarity about where capital market licensees were supposed to report STRs. Furthermore, there were concerns about the low level of reporting, particularily by capital markets and insurance licensees.

***Criterion 20.1*** - There is a legal requirement in Art. 4 and 5 (c) of Decree Law No. 4 (2001) to report suspicious transactions related to ML and related offences to the FID. Suspicious transactions relating to TF are covered following an amendment, through Decree Law No. (54) 2006, Art.5 bis (4) and (5), which added "terrorism finance" to the previous provisions. Further, FC-5 in the Rulebook (Vol. 1) details the practical guidelines for conventional banks on how to report to the FIU. Similar

provisions are included the Rulebook volumes (volumes 2-6, sections 5, 4, 4, 5 and 4 of the respective Rulebook).

There is no indication in the Law, that reporting should occur promptly; however, Rulebook volumes applicable to the different licensees require that reporting must be done promptly after being considered by the Money Laundering Reporting Officer (MLRO) or compliance officer.

***Criterion 20.2*** **- .** The reporting obligation included in Art. Art. 4 and 5 (c) of Decree Law No. 4 (2001) does not refer to the need to report attempted transactions. The Rulebook volumes that cover the different licensees as indicated above, however, do indicate the need to report attempted transactions. This should be clarified in the law.

### *Weighting and Conclusion*

The need to report suspicious transactions promptly and to report attempted transactions is not contained in law.

**Recommendation 20 is rated Largely Compliant.**

## *Recommendation 21 – Tipping-off and confidentiality*

Bahrain was rated largely compliant with former R.14 as the legal protection for reporting STRs did not require reporting being conducted in good faith.

***Criterion 21.1*** - Art.10 of Decree Law No.4 (2001) and its subsequent amendment by Decree Law No. (54) 2006 to add TF reporting, provides the legal protection required by the FATF standards. Similar provisions are included the CBB Rulebooks applicable to the different CBB licensees. In addition, Art. 7 of MO No.7 (2001) states that reporting to the FID or Public Prosecutor as required by the order is not a breach to any law. This largely meets the requirement except for the fact that it is not required that reporting is done "in good faith". Authorities noted that the CBB Rulebooks are being amended to capture this.

***Criterion 21.2*** - MO No. (7), 2001 indicates that institutions should not communicate with the concerned customer or any other person with respect to ML, except with the authorisation of the Anti –Money Laundering Unit. Art. 2.6 of Decree Law No.4 (2001) makes it an offence to reveal information or a suspicion acquired in the course of that person's, trade, business, profession, employment or otherwise regarding the issue of an investigation order or attachment order in a ML offence, where such disclosure is likely to prejudice the investigation. This provision was made applicable to TF through the amendment of Decree Law No. 4 (2001), which added a reference to "terrorism finance"everywhere but in Art. 4.4 and 4.5 of the said law, and is sufficiently broad to cover what is required by 21.2 even when there is no explicit reference to filing a report. Further, Rulebook (FC- 5.2.6) indicates that in accordance with the AML Law, licensees, their directors, officers and employees must not warn or inform ("tipping off") their customers, the beneficial owner or other subjects of the STR when information relating to them is being reported to the relevant authorities.

### *Weighting and Conclusion*

FIs, their directors and employees are protected from both criminal and civil liability, even though they are not required to report in "good faith". The provision to report TF suspicions should be further clarified (See criterion 21.2).

**Recommendation 21 is rated Largely Compliant.**

## *Recommendation 22 – DNFBPs: Customer due diligence*

Bahrain was rated partially compliant with former R.12 due to a number of deficiencies related to CDD and record-keeping. Further, there was no uniform understanding by lawyers that they need to identify and verify the identity of their clients and keep client identification for all clients for a minimum of five years after the termination of the client relationship.

Casinos are not permitted in Bahrain (See criterion 28.1).

Decree Law No.4 (2001) provides power for authorities responsible for supervision and licensing to issue orders to regulate the sectors that fall under their supervision with regards to AML/CFT. The MOICT has issued MO 173 (2017), covering the sale and trade of jewellery, audit and accountancy. Legal practice and advocacy are covered under Decree Law No. 4 of 2001 and subsequent Resolution 64 of 2017 for AML/CFT purposes. It applies to law practice and legal consultations by lawyers, foreign firms and law firms.

Notaries are governed by Law 14 (1971), which restricted notarisation to employees of the MOJ until at the time of the onsite. During that time, the concept of private notaries was introduced by Law 37 (2017). At the same time, duties for notaries were specified in the Resolution 76 of 2017, while the procedures and guidelines of the AML/CFT Law were applied to notaries by Resolution 77 of 2017; this Order applies the requirements of Decree Law No.4 (2001) to notaries. Notaries in Bahrain are civil servants and do not act on behalf of customers. Their functions are limited to confirming the identity of the parties appearing before them, ensuring they have legal capacity, understanding the content and effect of the documents being notarised and confirming that the documents do not contradict public order. Private notaries will have the same functions.

Professional trustees fall within the scope of the CBB Law and the CBB's supervision. Company services providers are not identified separately as these types of services are provided by lawyers (to which the provisions apply).

***Criterion 22.1 -***

10.1: MO 173 requires registered entities to identify and verify customers (See criterion 10.2). It is prohibited to deal with persons whose identity is not known (Art. 5). Resolution 64 of 2017 requires legal professionals to be provided with identity information on their customers (Art. 4).

*When CDD is required*

10.2: MO 173 requires the identity of clients to be verified before conducting any business relationship or separate process (occasional transaction) (Art. 5). Criterion 10.2(e) is not satisfied. In addition, while Art. 3 requires a registered person not to

establish a business relationship whose purpose is ML/TF, this test is different to the test of suspicion in criterion 10.2(d). Art. 4 of Resolution 64 of 2017 provides that legal professionals shall require customers in the process of seeking advice to provide identity information. Criteria 10.2(d) and (e) are not addressed.

*Required CDD measures for all customers*

10.3: Art. 5 of MO 173 specifies that individuals must be verified by *inter alia*, passport information and an ID card. For corporate entities, incorporation documents must be verified. The criterion is addressed to some extent (there is no explicit requirement to use reliable, independent source documents, data or information). The Bahrain authorities have advised that the government source data referred is reliable and independent and that the language of the Order gives registered entities flexibility to go beyond these requirements to use such information as it considers appropriate.

10.4: MO 173 requires that, for companies, the identity of the company's legal representative must be verified (Art. 5). Resolution 64 of 2017 mandates legal professionals to require customers which are legal persons to provide the name and ID information of the legal representative. In addition, Art. 4 contains a provision on the ID/passport and other information to be obtained by attorneys acting for clients. This criterion is met in part.

10.5: This criterion is met in part. MO 173 states that where the registered person adopts EDD, it must obtain further information to establish the client's ultimate beneficial owner and take special measures to identify the ultimate beneficial of legal structures (Art. 5). Resolution 64 (2017) states that lawyers must obtain information on the legal person's owner and the major shareholders of the legal person (Art. 4). It is not clear that legal arrangements are covered. In relation to lawyers, there is no requirement to verify the identity of beneficial owners in all circumstances and, for DNFBPs covered by the two Orders, it is not specified that relevant information or data from a reliable source should be used.

10.6: MO 173 of 2017 provides that the background and purposes of processes and deals should be inspected (Art. 3(d). Art. 5 of the 2017 Order adds that EDD includes finding out the purpose of the transaction. The criterion is met in part; there is no requirement to understand the purpose and intended nature of the relationship.

10.7: MO 173 states that client transactions must be continuously monitored (Art. 5), which partly meets criterion 10.7(a).

*Specific CDD measures required for legal persons and legal arrangements*

10.8: This criterion is addressed to some extent for MOICT registered entities by Art. 5 of MO 173 (2017), which states that, for corporate customers, information on the types of activity undertaken must be obtained.

10.9: MO 173 specifies that the identity information to be verified for legal persons is the name, legal form, number and place of registration, address of the head office and branches, names of the members of the board of directors, and the corporate's legal representative (Art. 5). This does not cover legal arrangements and sub criterion (a) is satisfied except for this. Names of the members of the board of directors must also be provided, which, taken with provision of the incorporation documents, means that sub criterion (b) is met in part as not all relevant names of

senior management have to be provided and it is not clear that there is coverage of legal arrangements. The address of the head office and any branches must also be provided to the registered person. Sub criterion (c) is not completely met as the language of the Orders does not cover the address of the principal place of business if that is different to the head office and it is not clear that legal arrangements are covered.

Resolution 64 of 2017 requires legal persons to provide their name, legal form, number and place of registration, address of the head office and the branch, names of the company's board of directors and the name and ID information of the legal representative (Art. 4). The Orders would appear to address the information requirements of sub criterion (a) for legal persons. With reference to sub criterion (b), not all relevant names of senior management are necessarily addressed. Sub criterion (c) is not completely addressed as the language of the Order does not cover the address of the principal place of business. Legal arrangements are not addressed for any of the sub criteria.

10.10 and 10.11: See analysis in criterion10.5 of this Recommendation above.

*CDD for Beneficiaries of Life Insurance Policies*

10.12 and 10.13: These criteria are not applicable.

*Timing of verification*

10.14 and 10.15: There are no provisions under MO 173 (2017) permitting delayed verification. There are also no such provisions in Resolution 64 of 2017.

*Existing customers*

10.16: This criterion is not addressed by the Orders except for the ongoing due diligence provisions mentioned at criterion 10.7 above.

*Risk-based approach*

10.17 and 10.18: MO 173 (Art. 5) states that registered entities must adopt EDD where there is a high possibility that the transaction would involve a ML/TF crime in accordance with a range of factors. This includes cases of higher risk, customers who are not physically present during the identification process, PEPs and any other situation where a higher risk of ML/TF might exist. Art. 5 also specifies what constitutes EDD. Simplified measures are permitted where the customer is a government, a semi-government or related to the government of Bahrain. It is also permitted for customers well known to the registered person. It is not clear that, in all such cases, the simplified measures would be commensurate with lower risk.

*Failure to satisfactorily complete CDD*

10.19: This criterion is not addressed explicitly but the effect of the provisions within MO 173 criteria (See criteria 10.1 and 10.2) is that criterion 10.19 is partially met as new customers must not be accepted unless CDD has been carried out.

*CDD and tipping off*

10.20: This criterion is not specifically addressed by the Orders. There are requirements to report suspicion and tipping off provisions (See criteria 23.1 and 23.2) but these do not extend to explicit permission not to pursue the CDD process.

***Criterion 22.2*** -

11.1: See criterion 11.1 for the application of Decree Law No.4 (2001). Paragraph (b) of Art.6 of MO 173 states that transaction records must be retained for a period of five years from the expiry of the transaction; paragraph (a) requires that all records relating to the details of transactions must be obtained and the retained. With regard to legal professionals, Resolution 64 of 2017 requires information and documents on the subject matter of the activity undertaken to be retained for five years from the conclusion of the activity.

11.2: See criterion 11.2 for the application of Decree Law No.4 (2001). Paragraphs (a) and (b) of Art.6 of MO 173 states that registered persons shall maintain information and documents related to the identity of clients, their representatives and the beneficiaries of the transaction, together with accounting records, for a period of five years after the transaction. Any changes made to the status of the clients shall be regularly included in these records. With regard to legal professionals, Resolution 64 (2017) requires information and documents on the identity of clients or persons seeking advice (and their representatives) to be maintained for five years from the date of the activity undertaken.

11.3: Paragraph (a) of Art.6 of MO 173 applies to records of the details of transactions although it is possible that the records held by registered persons might not be sufficient to permit reconstruction of all individual transactions so as to provide evidence for prosecution of criminal activity.

11.4: MO 173 requires that records and supporting documentation in relation to the results of suspicious and/or extraordinary deals, CDD information and the results of investigations must be easily retrievable (Art.6). This would not necessarily capture all information for the purposes of the criterion. In addition, these records must be made available to the competent authorities in accordance with the law.

***Criterion 22.3*** - There are no express provisions in MO 173 to address R.12 except that EDD must be carried out when entering into a business relationship with a PEP, and EDD includes finding out about the source of funds (Art. 5).

***Criterion 22.4*** - There are no provisions which address R. 15 except that Art.7 of MO 173 states that, where a registered person has a new product or technology, the same rules of client's identity would be applicable as outlined in Art. 5 of the Order.

***Criterion 22.5*** - *(Not applicable)* There are no provisions which permit reliance on third parties.

### *Weighting and Conclusion*

Main deficiencies relate to identification and verification of BO, timing of CDD, application to existing customers and requirements relating to PEPs.

**Recommendation 22 is rated Partially Compliant.**

## *Recommendation 23 – DNFBPs: Other measures*

Bahrain was rated partially compliant with former R.16 as the DNFBP sector, and especially lawyers, had little understanding regarding their STR obligations.

***Criterion 23.1*** -

(a) The provisions of Decree Law No.4 (2001) described at R.20 apply in relation to legal practice and advocacy, audit and accountancy, and notaries.

In addition, with regard to notaries, Art.2 of Resolution 77 (2017) requires notaries to notify the FID and the Follow-Up Unit within the MOJ, of activities which are suspected to involve directly or indirectly the ML/TF offences specified in Art. 2.1 of the Decree Law. The promptness of reporting by notaries is not specified. There are no provisions which cover attempted transactions for notaries. Art. 9 of MO No. 173 (2017) contains a similar provision. While the definition of client in Art. 1 of each Order includes persons wishing to deal with a registered person; the provisions do not refer to an obligation to report attempted transactions.

Resolution 64 (2017) details the obligation on lawyers that is prescribed in Art.29 of Law 26 (1980). This obliges lawyers to inform the authorities of any criminal activities even if discovered through a lawyer/client relationship. Art. (5)2 of Resolution (64) provides that suspicion or irregular activities (irregular activities are defined in Art. 1 of Resolution (64) as related to ML/TF as defined by Decree Law No.4 (2001) and amendments) must be reported to the Follow-Up Unit within MOJ, detected when carrying out transactions on behalf of clients, particularly, the purchase or sale of real estate; management of the principal's funds, securities or other assets; management of the principal's bank accounts of all categories; and establishment, management or dissolution of legal persons. The language in the Resolution does not include attempted transactions.

(b) DPMS have reporting obligations under Decree Law No.4 (2001) described in R.20. Art.9 of MO No.173 (2017) includes provisions on the reporting of suspicious or extraordinary deals. This must be done by the compliance officer within 24 hours from the time of becoming aware of such deals. Attempted transactions are not covered.

(c) Trust services providers need to be licensed by the CBB and the relevant FC volume applies as described in R.20, as well as Decree Law No.4 (2001). Similarly, only lawyers can provide company services provider activities and the provisions under (a) above apply.

***Criterion 23.2*** -

Criterion 18.1 is partly met by Art.7 of MO No.173 (2017) which requires the appointment of a compliance officer with independence and power (it refers to an appropriate person while not requiring that the person to be appointed is at a manager level), inter alia, to ascertain the suitability of internal controls, regulations and procedures, ascertain that employees have received appropriate training, control the level of compliance, and control the level of commitment to record keeping.

Criterion 18.2 is partly met by Art.3 of MO No.173 (2017) which requires persons registered by the MOICT to oblige foreign branches to adopt measures of preventing ML/TF in accordance with the FATF Recommendations and apply the provisions of the Order; also Art.2 applicable to registered persons and their branches and subsidiaries inside and outside Bahrain (See criterion below). There is no

requirement for the implementation of group-wide programmes and none of the sub criteria of the criterion is addressed.

Criterion 18.3 is partly met as Art.3 of MO No.173 (2017) requires registered persons to oblige their foreign branches (but not subsidiaries) to adopt measures to prevent ML/TF as detailed above regarding 18.2 as well as the provisions of the Order to the extent allowed by laws and regulations applicable where the branches operate, especially if the countries concerned do not or inadequately abide by the provisions of the Order. The registered person must inform competent bodies in cases where the laws of the countries hinder the application of the provisions of the Order. The Order does not cover all home country requirements [e.g. record keeping requirements are included in Decree Law No.4 (2001)]; majority owned subsidiaries are not covered; and the criterion's requirements on the application of appropriate additional measures are not included.

***Criterion 23.3*** - There are no provisions governing the application of R.19 except for the requirement in Art. 5 of MO No.173 (2017) to adopt enhanced due diligence where there are situations with a higher risk of ML/TF and a requirement in Art.5 of Resolution 64 (2017) for legal professionals to report to the Follow-Up Unit if the principal or person seeking advice is a person or entity of a high risk country classified in statements issued by the FATF, or if the activity of a power of attorney or request for consultation is set to take place in any such country.

***Criterion 23.4*** - The protections described at criterion 21.1 in relation to Decree Law No. 4 (2001) also apply to DNFBPs falling within the scope of the Schedule to the law. Art. 7 of MO No.7 (2001) also applies to DNFBPs falling within the scope of the reporting obligations. Criterion 21.1 is rated as Mostly met.

1.2, Art.9 (g) of MO No.173 (2017) provides that registered persons are prohibited from informing the client of the submission of a STR or any related information to the FIU. The provisions do not explicitly cover directors, officers and employees although Bahrain advises that the provisions extend to all staff. In addition, the provision only applies after an STR has been made; it does not seem to cover the period during the process of making the STR even though Bahrain has indicated that the law applies to everything related to the process of suspicion and raising an STR.

With reference to legal professionals, in addition to the foregoing, Art.5 of Resolution 64 (2017) specifies that legal professionals must comply with the requirements of Decree Law No.4 (2001) not to report or leak information on any action taken or to be taken in respect of AML/CFT. In addition, the Art.5 also requires legal professionals not to make their suspicions, particularly in relation to dubious transactions, known to their principals and persons seeking consultation or advice, and not to notify them of such suspicions.

### *Weighting and Conclusion*

Attempted transactions are not covered. Requirements on internal controls and high risk countries are not detailed to meet the FATF standards.

**Recommendation 23 is rated Partially Compliant.**

## *Recommendation 24 – Transparency and beneficial ownership of legal persons*

Bahrain was rated largely compliant with former R.33, as the capital market regulations did not include explicit requirements related to conducting CDD on legal persons or the identification of beneficial ownership.

***Criterion 24.1*** - Bahrain has companies and other types of legal persons which include non-profit organizations analysed separately under R.8. Decree Law No. (21) 2001 (the Commercial Companies Law, Art.2) lists the forms of companies that can exist in the country; the different forms and basic features, as well as the processes for the creation of these legal persons:

1. General Partnership Company
2. Limited Partnership Company
3. Association in participation
4. Joint Stock Company
5. Limited Partnership by Shares
6. Limited Liability Company
7. Single Person Company
8. Holding Company

The Commercial Companies Law also applies to foreign companies incorporated abroad and undertaking activities in Bahrain (by virtue of Art.346). The Commercial Companies Law and the Company Registry contains provisions regarding obtaining and recording basic information, which is kept in a Registry website held by the MOICT: (www.sijilat.bh/). Nor the Commercial Companies Law or the Company Registry have a specific requirement for obtaining and recording beneficial ownership information (only a requirement to record basic and shareholder information) although it is possible to identify the ultimate beneficial owner through the Sijilat system, particularly for Bahraini owned companies, which represent more than half of companies registered. In addition, Ministerial Order 19 of 2017 (Bahrain's Corporate Governance Code) mandates all companies (Bahraini or foreign) to disclose break down of their ownership details to the MOICT. These include ownership structure broken down by nationalities of the owners, names of all shareholders who own 5% and above in company shares as well as names of ultimate natural person who is the beneficial owner of the shares. Prior to the 2017 amendment, the MOICT was using its powers under the Commercial Registrar Law of 2015 and the 2010 Corporate Governance Code to obtain this information from companies, which is available to the MOICT through privileged access in the Sijilat system. However it only covers those who own shares, and lacks reference to those who may control a legal person through means other than ownership.

***Criterion 24.2*** - Bahrain has not assessed the ML/TF risks associated with all types of legal persons, though it has conducted a limited assessment of some of the DNFBPs, the legal forms associated with them and analysis of STRs from different DNFBPs in terms of nationality and areas where these were being generated. In addition, specific assessments ("Self-defence guide against ML/TF) were done regarding companies providing specific services such as audit firms, jewelleries, and

real estate agents or other professionals. Bahrain still needs to conduct a comprehensive risk assessment of different kinds of legal persons created in Bahrain, and their vulnerability to ML/TF abuse. This should, for example, include multi-agency information sources, such as FID, CBB, PPO, other law enforcement agencies and MOICT, to identify any trends and patterns.

***Criterion 24.3*** - Companies created under the Companies Law above, are required to be registered [Art.4 and 6 of Decree Law No.27 (2015)], and must have a memorandum of association or Art. of association before being able to operate. According to Art.30 of the Commercial Companies Law, these memorandums of association or Art., and any changes to them, should be presented to the Registry. The summary of the memorandums should contain at a minimum:

a) Company's name, objective, headquarters, branches, if any.

b) The directors/partners' names, domiciles, professions and nationalities.

c) The company's capital and sufficient definition of each partner's shares and their due date.

d) The names of the managers and the persons authorised to sign for the company.

e) The date of the company's incorporation and its term.

f) The beginning and the end of the company's financial year.

This information is publicly available through the Sijilat system.

***Criterion 24.4*** - Companies are required to maintain the information set out above and in addition, Art. 118 of the Commercial Companies Law indicates that all companies should maintain a record with shareholder names, nationalities & domiciles, the number and serial numbers of share certificates, and the dealings made thereof. It does not require clarifying voting rights however. A copy of this information should be forwarded to MOICT & the Bahrain Stock Exchange. This applies to foreign companies (Art.346 of the Commercial Companies Law). Art.171 also establishes similar requirements, specifically for Joint Stock Companies with the difference that for these companies, information is kept in the company headquarters.

***Criterion 24.5*** - Changes on the information provided (as detailed above), should be notified to the Registry within 30 days (Art.11 of Decree Law No.27 (2015)). The MOICT inspects companies and ensures information is kept up to date. The MOICT has also alert mechanisms to remind companies of obligations and registration numbers have been frozen for non-compliance.

***Criterion 24.6*** - Bahrain uses a combination of mechanisms in this respect. The Sijilat system allows searching for the ultimate shareholder and individual behind a chain of companies. This would lead to identifying BO in some cases, as long as these are residents of Bahrain, who are identifiable through a secure e-key. In addition, Ministerial Order 19 of 2017 (Bahrain's Corporate Governance Code) mandates all companies (Bahraini or foreign) to disclose break down of their ownership details to the MOICT. These include ownership structure broken down by nationalities of the owners, names of all shareholders who own 5% and above in company shares as well as names of ultimate natural person who is the beneficial owner of the shares. Prior to the 2017 amendment, the MOICT was using its powers under the

Commercial Registrar Law of 2015 and the 2010 Corporate Governance Code to obtain this information from companies, which is available to the MOICT through privileged access in the Sijilat system. However it only covers those who own shares, and lacks reference to those who may control a legal person through means other than ownership. Further, the concept of beneficial owner is not defined in legislation, which would help set expectations for companies. No mechanism seems to exist to ensure that shareholders are indeed beneficial owners and not straw men in all cases.

Changes on the information provided (as detailed above), should be notified to the Registry within 30 days, and changes are routinely updated in the Register and available online (Art.11 Decree Law No.27 (2015)). Finally, information regarding on beneficial ownership can also be obtained through FIs. CBB Rulebook (Vol. 1- 6), requires FIs to identify and verify the identity of the ultimate beneficial owner of the funds, the ultimate provider of funds (if different), and the ultimate controller of the funds (if different).

***Criterion 24.7*** - As noted above beneficial ownership seems to be obtained in some cases by the registry and by the FIs, which have an obligation to obtain such information and keep it accurate and up to date.

***Criterion 24.8*** - (a)-(b) are not applicable because Bahrain does not have measures requiring that one or more natural persons in the country, or that require that a DNFBP in the country, is authorised by a company and are accountable to competent authorities for providing basic and beneficial ownership information and providing assistance. (c) Bahrain has however taken comparable measures to ensure basic information is accessible. Art.359 of the Commercial Companies Law indicates that "any concerned party may apply to have access to the data kept at the MOICT, in respect of the companies subject to its supervision and control, and may have copies thereof (…)". Besides all basic information and in some cases beneficial ownership information is available in the company registry. Beneficial ownership information can also be obtained through FIs. CBB Rulebook (vol. 1- 6), requires FIs to identify and verify the identity of the ultimate beneficial owner of the funds, the ultimate provider of funds (if different), and the ultimate controller of the funds (if different).

***Criterion 24.9*** - Art. 344 of the Commercial Companies Law indicates that company books and records shall be kept 10 years from the day of striking off the company. Information kept by MOICT including that of the online register is kept indefinitely.

***Criterion 24.10*** - Art. 19 of Law No.27 (2015), the Commercial Register Law, indicates that authorities (MOICT) can request any document deemed to be necessary for their functions and authorise judicial officers (for the purposes of enforcing the law, as indicated in Art.26 of the same Law). Other law enforcement authorities also have powers to obtain this information pursuant to Art.359 of the Commercial Companies Law.

***Criterion 24.11*** - Bahrain stated that bearer shares does not exist in Bahrain, and therefore they cannot be misused for ML or TF, although a general provision that companies may issue bearer shares, subject to rules and requirements decreed by Minister of Commerce and Industry exists. This, however, has not occurred as Bahrain noted that Art. 118 and 171 of the Commercial Companies Law, as well as several CBB provisions related to the issuance of securities point out the

identification of shares and warrant holders. Thus notwithstanding the enabling provision in law, no such ministerial regulation has been issued, which in effect implies the absence of bearer shares in Bahrain. This criterion was therefore deemed as met.

***Criterion 24.12*** - Bahrain stated that nominee shares and nominee directors do not exist in Bahrain, and thus cannot be misused, for ML/TF; however there is no express bar against nominee shareholders or directors.

***Criterion 24.13*** - Sanctions are available for persons who fail to comply with the requirements of the Commercial Companies Law; imprisonment of one week to three years according to Penal Code Bahrain, and a fine between BHD 5 000 and BHD 10 000 (EUR 11 to 22 000), for breaches such as providing false information in the memorandum of association (Art. 361 and 362 of the Commercial Companies Law) and a fine of 5 000 for other types of less serious breaches. This may not be sufficiently dissuasive for large companies.

***Criterion 24.14*** - Basic and some beneficial ownership information is available in the Sijilat system. In addition, Art. 359 of the Commercial Companies Law indicates that "any concerned party may apply to have access to the data kept at the MOICT in respect of the companies subject to its supervision and control, and may have copies thereof (…)". This can be helpful for Bahrain to rapidly provide international co-operation, through its registry, which is directly accessible for foreign authorities and the general public. According to information described under IO.2 and IO.5, assistance has been provided with regard to basic and beneficial information where required.

***Criterion 24.15*** - There are no specific measures to monitor the quality of assistance received from other countries in response to requests for basic and beneficial ownership information.

### *Weighting and Conclusion*

Information on those who may control a legal person through means other than ownership of shares may not be available (See criterion 24.1 and 24.6). Bahrain is yet to fully assess ML/TF risks associated with all types of legal persons created in Bahrain. There is no express bar against nominee shareholders or directors. There are no mechanisms to ensure that shareholders are indeed beneficial owners and not strawmen in all cases and this has an impact on several criteria (particularly 24.6-24.8). There are no measures to monitor the quality of assistance received from other countries in response to requests for basic and beneficial ownership information. Sanctions may not be dissuasive for large companies.

**Recommendation 24 is rated Largely Compliant.**

## *Recommendation 25 – Transparency and beneficial ownership of legal arrangements*

Bahrain was rated not applicable in former R.33, which previously contained the requirements for transparency of legal arrangements. The MER noted at that time, that there was no trust law or instruments in Bahrain, which now exist and are analysed below.

Only CBB registered and supervised trust companies can act as trustees in Bahrain. Hence the CBB Rulebooks apply together with provisions contained in Decree Law No.23 (2016) or Trust Law. A figure similar to trusts exists, the "waqf" which is a Sharia legal arrangement by which property or money can be kept in favour of the public or a particular individual, for eternity.

***Criterion 25.1*** -

With regard to trusts:

a) There is an obligation to obtain and hold information on the settlor, trustee, beneficiary or class of beneficiaries (Art. 14 of the Trust Law) and according to FC 1.2.3., volume, the trust instrument may provide for the appointment of a Protector, who would then be identified following Art. 24 of the Trust Law or to any other natural person exercising ultimate effective control over the trusts. Art. 30 of the Trust Law refers to the duty of the trustee of keeping accurate account and records of its trusteeship. In addition, Rule FC-1.2.11 of the FC Module of CBB Rulebook Volume 5 requires the licensee to obtain DD documents on "ultimate controllers of the funds", below is the rule reference.

b) There are no measures to obtain and hold information regarding services providers to the trust.

c) Only licensed trustee services providers can act as professional trustees and have an obligation to keep records and information, for at least 5 years following the CBB Law and the Financial Crime Modules (FC) in particular, as detailed under R.11 (See 11.1).

There are no specific provisions as regards foreign trusts operating in Bahrain (unless they operate through trust services providers in which case CBB provisions would apply as they would have to be licensed). The Trust Law refers to foreign trusts but no identification requirements are included among the common provisions.

With regard to Waqfs:

a) There is an obligation to obtain and hold information on the different parties of the Waqf according to Sharia law, including the donator (Waqif), supervisor of the Waqf (Nather) beneficiary or class of beneficiaries (i.e. members of the family of the deceased) who will benefit from the Waqf.

b) There are no measures to obtain and hold information regarding services providers to the Waqf.

c) There are no record keeping provisions as regards to waqfs but Bahrain noted records of the Waqfs are kept in the MOJ and waqif councils (supervisors of waqfs).

***Criterion 25.2*** - There are measures to require that any information held pursuant to this Recommendation (i.e. CDD information) is kept accurate and as up to date as possible, and is updated on a timely basis. There are no provisions regarding foreign trusts, except if one of these were to be licensed by the CBB which are subject to record keeping requirements applicable to FIs (see R.11). There are also no specific requirements for Waqfs, although in principle, according to the definition and the purpose of the Waqf, there is no transfer of ownership during the duration of the Waqf.

***Criterion 25.3*** - Art. 32 of the Trust Law requires that trustees disclose their capacity as trustees in all contracts entered to, or transactions made for the benefit of the trust, particularly banking transactions, shipping documents, among others. There are no specific provisions as regards foreign trusts operating in Bahrain. The Trust Law refers to foreign trusts but no identification requirements are included among the common provisions. There are also no provisions applicable to Waqfs.

***Criterion 25.4*** - There are no inhibiting measures that impede access to information related to trusts and information on trusts is available in the trust registry maintained by the CBB. Access to information can be granted to authorities through a court order pursuant to Art. 25 of the Trust Law and Art. 111, 117 and 123 of the CBB Law. Also, trustees are not prevented under any law or enforceable means from providing competent authorities with any information relating to the trust, or from providing FIs and DNFBPs, upon request, with information on the beneficial ownership and the assets of the trust held or managed under the terms of the business relationship. Information regarding foreign trusts will be available once the trustee is an entity regulated by the CBB and information on waqfs will be available through MOJ.

***Criterion 25.5*** - Given that trustees are CBB licensees, the CBB can request the trustee to provide information regarding beneficial owners of trusts under their administration (Art. 69 of the Trust Law/ Part 7 of the CBB law.), subject to limitations for foreign trusts which are not CBB licensees. Law enforcement authorities have also broad powers to obtain information held by trustees and other FIs or DNFBPs as indicated under R.31.

***Criterion 25.6*** - (a) Bahrain facilitates access to information on trusts through its Central Bank based registry (Art. 25 of the Trust Law). (b) Bahrain can exchange domestically available information pursuant to Central Bank Law (Art. 111, 117 and 123) and Art. 42 of the Trust Law which refers to the ability of the beneficiary, protector and enforcer or a charity (in certain circumstances), to request the disclosure of information. (c) Art. 70 of the Trust Law explicitly indicates that the Central Bank must cooperate with foreign authorities in carrying out investigations related to any Trust and so does Art. 122 of the Central Bank Law. There are no equivalent measures for foreign trusts or Waqfs although authorities indicated that information could be provided on Waqfs, by the MOJ and Waqif councils.

***Criterion 25.7*** - (a) Art. 43 of the Trust Law indicates that trustees are liable for breaches of the trust. Also, Art. 47 of the Trust Law refers to several measures that can be taken to ensure the trustee complies with this duties including a court order to compel the Trustee to perform its duties, remove the Trustee, if there is a serious breach and order a replacement, among others (i.e. Art. 2, item 4 of Trust Law, where it is stated that a trustee can be sued in its capacity as a trustee). b) There also sanctions for specific obligations of a trustee, such as disclosing its capacity as a trustee to third parties (Art. 65 of Trust Law). Sanctions range from 10 days to three years of prison and/or a maximum of BHD 100 000 (EUR 215 588) fine. A fine of BHD 50 000 (EUR 107 441) can be applied together with 10 day-three years of prison for purporting to act as a trustee without being licensed. In addition, since trust services providers can only be licensed institutions, they are subject to Central Bank Law and Volume 5 of the CBB Rulebook and its sanctions. These are all considered proportionate and dissuasive. There are no equivalent measures for

foreign trusts or waqf (for AML/CFT purposes), although a CBB registered trustee providing services to foreign trust would be covered.

***Criterion 25.8*** - For trusts, the CBB would provide information to law enforcement authorities and in turn, if the licensee does not abide by CBB law requirements, then the CBB has the right to impose enforcement measures (Art. 125 to 132 of the CBB law and the Enforcement Module under CBB Rulebook Volume 5, applicable to specialised licensees such as trustees). No specific provisions applicable to foreign trusts, except if licensed by the CBB in which case, the above provisions apply. Information on waqfs would be provided by the Waqf Councils.

### *Weighting and Conclusion*

Information on the beneficial owner of a trust is not always timely available and the provisions for waqfs are limited; this has an impact on several criteria.

**Recommendation 25 is rated Largely Compliant.**

## *Recommendation 26 – Regulation and supervision of financial institutions*

Bahrain was rated partialy compliant with former R.23, which contained the previous requirements for R.26. The main deficiencies related to the lack of inspections for insurance and capital markets licensees.

***Criterion 26.1*** - The CBB must regulate, develop and license the regulated services specified in Art. 39 of the law, and exercise regulatory control over institutions that provide such services (Art.4 CBB Law). All aspects of the FATF's description of FIs are covered by the CBB's framework.

***Criterion 26.2*** - See criterion 26.1. No person shall carry out a regulated service unless licensed by the CBB (Art.40 of the CBB Law). All FIs are required to be licensed.

Banks are required to have a physical place for business and audited accounts (Art.45 and 59 onwards). The stautory framework for licensing (including under licnsing requirments modules), combined with high level control and general requirements modules, prevent shell banks from being established or operating.

***Criterion 26.3*** - The CBB may refuse to give approval to "a controlling interest" (i.e. control through ownership) if it will affect the legitimate interests of customers or if it is detrimental to the relevant sector or, if the CBB decides at its own discretion, that it would be inappropriate according to criteria set by the CBB (Art.55 of the CBB Law).

Art. 52(a) specifies that the CBB shall issue a regulation specifying the nature and limits of control and regulations for approving control over a licensee. Criteria have been set through CBB Regulation No.31 (2008), Resolutions No. 43 (2011) and No. 33 (2012) issued under Art. 38 and 52 of the Law. The language of these instruments is incorporated within general requirements modules (GRMs), with one module being issued for each business sector.

***The CBB Law:*** The CBB must, be notified if (i) effective control of a licensee takes place indirectly by way of inheritance or otherwise; (ii) directly as a result of any action leading to it; or (iii) the intention is to take any actions that would lead to

control of the licensee (Art.52(b) CBB Law). The controller/person intending to take control and the licensee itself (if it is aware) must request the CBB's approval for taking control and include such information and documents as the CBB may specify. Where provisions (i) and (ii) above apply the notification must be provided within 15 days of control being achieved. It would appear under provision (ii) that control can be deliberately achieved by a person without first obtaining the CBB's approval.

The CBB must make a decision within three months of receiving a notice. The CBB may require a person to transfer shares in a licensee or refrain from exercising voting rights or seek a court order to take appropriate precautionary measures or for a person to sell shares (Art. 56 of the CBB Law).

***General Requirements Modules (GRMs):*** Prior approval from the CBB is required for new controllers and existing controllers for increases of holdings above 10%, 20%, 30% and 40% (GR 5.1). The provisions apply both to applications for licences and to existing banks. The definition of controller includes shareholders, shareholders in parent undertakings and persons exercising significant influence over the management of the bank and/or its parent and extends to beneficial owners above the shareholders of the parent undertaking.

In considering whether or not to issue an approval the CBB must be satisfied that there are no undue risks to the licensee. The suitability criteria of the CBB are set out in GR-5.3. These include the propriety of a person's conduct, whether or not such conduct resulted in conviction for a criminal offence, the contravention of a law or regulation, or the institution of legal or disciplinary proceedings; a conviction or finding of guilt in respect of any offence other than a minor traffic offence; any adverse finding in a civil action by any court or competent jurisdiction relating to fraud, misfeasance, or other misconduct in connection with the formation or management of a corporation or partnership; whether the person has been the subject of any disciplinary proceeding by any government authority, regulatory agency or professional body or association; the contravention of any financial services legislation or regulation; whether the person has ever been refused a licence, authorisation or other authority; dismissal or a request to resign from any office or employment; disqualification by a court, regulator or other competent authority, as a director or as a manger of a corporation; and the extent to which the person has been truthful and open with regulator. A decision on suitability is issued within three months by the CBB.

GR-5.2 applies the concept of controller and the CBB's consideration to some (but not all) associates, namely close family members, undertakings of which the controller is a director and, if the controller is a legal person, directors of that legal person, its subsidiaries and directors of those subsidiaries.

Provisions with some differences are included in the GRMs for Islamic banks, insurance firms and investment businesses. The definition of controller for the latter two types of business does not extend to persons exercising significant influence over the FI other than by ownership.

***Management:*** The above provisions apply to ownership rather than control through management. Under licensing requirements modules, the CBB's prior written approval is required for any person wishing to undertake a controlled function in a licensee (See, e.g. LR-1A.1 for conventional banks). The approval from the CBB must

be obtained prior to appointment. Control functions are those functions occupied by board members and persons in executive positions and include: (a) Board Member; (b) Chief Executive or General Manager and their Deputies; (c) Chief Financial Officer and/or Financial Controller (d) Head of Risk Management; (e) Head of Internal Audit; (f) Head of Sharia Review; (g) Compliance Officer; (h) Money Laundering Reporting Officer; (i) Deputy Money Laundering Reporting Officer; and (j) Heads of other Functions. Approval is only granted by the CBB, if it is satisfied that the person is fit and proper to hold the particular position in the licensee concerned. The definition of 'fit and proper' and associated guidance is provided in the module. There is no fit and proper test for management as opposed to the senior management positions specified above.

***Criterion 26.4*** -

*a) For core principle financial institutions:* FC-B-2.4 of volume 1 of the CBB Rulebook requires financial groups to implement group-wide programmes against ML/TF, including policies and procedures for sharing information. There are equivalent provisions for Islamic banks, insurers, investment businesses, capital markets and insurance companies.

All core principle and other FIs are subject to AML/CFT supervision by the CBB. There is close liaison between the sectoral supervisory directorates and the compliance directorate, which is responsible for all onsite and offsite AML/CFT supervision. Core principle FIs are regulated and supervised largely in line with the core principles. The compliance directorate manual does not include reference to consolidated group supervision for AML/CFT purposes and could usefully be amended. However, the CBB appears to exercise consolidated group-wide AML/CFT supervision in practice and is enabled to do so through the language in the CBB Rulebook.

*b) For all other financial institutions:* The CBB is responsible for ensuring compliance with AML/CFT requirements for these institutions. Volume 5 of the CBB Rulebook does not contain the group-wide provision mentioned above for banks in volume 1. Most of the FIs subject to volume 5 are domestically incorporated and not part of groups; hence the gap is not significant.

***Criterion 26.5*** - The CBB has a compliance directorate manual which states that the annual onsite examination plan is based on offsite analysis that is primarily centred around risk based supervision (paragraph 5.2.1). Section 5.2 also indicates that qualitative and quantitative factors are mainly used to formulate an understanding of the institution's ML/TF risk and that information obtained to assess the level of the institution's ML/TF risk will subsequently assist in identifying the extent and type of onsite examination needed. While the particular factors in sub-criteria (a) to (c) of this criterion are not specifically included in the manual, as indicated in IO3, the CBB has put in place a framework for and strong elements of a risk based approach to supervision, although it is not fully comprehensive.

***Criterion 26.6*** - See criterion 26.5. The compliance directorate manual does not contain language on the review of the assessment of the ML/TF risk profile of FIs. In practice, FIs subject to onsite inspection have been risk graded and the rating is reviewed when an institution is next inspected.

### *Weighting and Conclusion*

There are some minor deficiencies with regard to measures to prevent criminals or their associates owning or controlling FIs (See c.26.3). The compliance directorate manual does not include a specific reference to consolidated group supervision for AML/CFT purposes or for review of assessment of the ML/TF risk profile of FIs.

**Recommendation 26 is rated Largely Compliant.**

## *Recommendation 27 – Powers of supervisors*

Bahrain was rated compliant with former R.29.

***Criterion 27.1*** - Art.4 of the CBB Law provides that the CBB must regulate, develop and license the regulated (financial) services specified in Art. 39 of the law and exercise regulatory control over institutions that provide such services. It has powers under to issue subsidiary directives, regulations (and Rulebooks) under Art. 38 and 52 of the law. Under Art.114 of the CBB Law, the Governor of the CBB may assign officials or other persons to inspect licensees (the power of inspection covering onsite and offite supervision). It also has the powers referred to in criteria 27.2 to 27.4 below.

***Criterion 27.2*** - The CBB has authority to inspect licensees' businesses pursuant to the principles and procedures stated in regulations issued by the CBB (Art.114). Inspectors are authorised to investigate whether licensees are complying with the provisions of the law and regulations and resolutions issued in connection with the implementation of the law. In order to achieve this, inspectors are authorised to enter the premises and offices of licensees; to have access to books, documents and correspondence and to question nay person deemed necessary. The CBB has developed a compliance directorate manual, which includes detail on the CBB's approach to inspections.

***Criterion 27.3*** - The CBB is authorised to demand and be provided with any information, documents, statistics, or yearly or other periodic reports that the CBB requires under the law (Art.111).

The CBB may request any licensee's partner to provide any reports that may be necessary under the law (Art. 113). The Bahraini authorities have advised that this is an enforceable requirement but it is not clear what legal provision creates the enforceability as there appear to be no penalties for breach of the request.

There is no provision for third parties, except for partners of licensees, to provide information relevant to AML/CFT compliance. "Partner" is defined as any body associated with the licensee (eg. subsidiries, third parties, etc.) and that partners refer to third parties (Art.13 CBB law).

FC-7.1.4 of volume one of the CBB Rulebook requires records to be available for swift and prompt access by relevant authorities. Equivalent provisions are contained in volumes 2 to 6.

***Criterion 27.4*** - The CBB may impose conditions for enforcement purposes on a licensee (Art.45 CBB Law). A licence may be amended or revoked if the licensee fails to satisfy any licence conditions or if the licensee violates the terms of the law or regulations or rules [Art.48(c)]. There are appeal provisions with at least 30 days'

notice to the licensee although a revocation can be immediate in exceptional cases that require no delay (the revocation is still subject to appeal).

Restrictions on a licence can be imposed to secure compliance with the law as well as regulations and resolutions issued for the purposes of implementing the law (Art.128 of the CBB Law). There must be significant evidence and indicators that violations have most likely occurred.

Administrative fines up to a maximum of BHD 100 000 (EUR 215 588) (CBB Law Amendment No. 34 of 2015) for each violation can be imposed for breaches of the Law or regulations and resolutions issued for the purposes of implementing the Law or for breaches of the terms and conditions of a licence (Art.129). Although this is a recent and considerable increase over the previous figure and applies to each violation, there may be some situations in which the maximum fine would not be proportionate or dissuasive. If fines prove to be futile, the CBB may appoint an observer member on the board of directors or place the licensee under administration (Art.130). Nevertheless, the maximum fining powers are partially proportionate and dissuasive. In addition, the power to issue fines does not apply to individuals.

The CBB may suspend a licence where a licensee contravenes any provisions of the Law, regulations or rules or bylaws issued in connection with implementation of the Law or where the licensee has breached the terms and conditions of the licence (Art.131).

The CBB may issue a public statement in relation to licensees or officials for the breaches referred to above (Art.132). Publication must be carried out in a manner proportionate to the nature and magnitude of the violation. Under EN-5.1.3 of the CBB's enforcement module, any director, manager or official responsible for the direction or management of a licensee, is to be considered removed from office should he be convicted by a court for a crime affecting his honesty; is declared bankrupt by a court; or if a court rules that his legal capacity is totally or partially impaired. The CBB can also remove any director, manager or official responsible for the direction or management of a licensee for violations, under its fit and proper framework.

### *Weighting and Conclusion*

There is no provision for third parties to provide information as required by criterion 27.3, except for partners of licensees. In addition, there is a narrow focussed concern about the maximum level of fining powers as detailed in criterion 27.4.

**Recommendation 27 is rated Largely Compliant.**

## *Recommendation 28 – Regulation and supervision of DNFBPs*

Bahrain was rated non-compliant with former R.24, which contained the previous requirements in this area, given that it had no measures in place for DNFBPs.

***Criterion 28.1 (N/A)*** Gambling is prohibited under Art. 308 of the Criminal Appeal Law 1976. Therefore, there are no casinos in Bahrain.

***Criterion 28.2*** -

Decree Law No.4 (2001) allows for Orders/Resolutions to be issued by supervisory authorities on reporting of suspicion, establishing the identity of customers and their beneficial owners, and internal reporting requirements (Art. 4.5).

The MOICT has been appointed under Art. 8 of MO 173 as responsible for the supervision and inspection of registered persons in all matters related to AML/CFT. These entities include DPMS, accountants and auditors. MO 173 makes the MOICT responsible for supervising and enforcing compliance by the DNFBPs subject to the Order in relation to all matters related to AML/CFT (Art. 8).

Legal professionals are governed under Resolution 64 of 2017. Art. 6 provides that the MOJ's Office of the Registry General is charged with receiving and auditing the digital data record of all legal services, consultation or advice required of legal professionals under Art. (5)14; it can also require any papers and documents to be provided to it verify the validity and integrity of such records. In addition, the Registrar General may assign members of the Follow Up Unit or external auditors to conduct field visits to the premises of legal professionals to audit, papers, records and documents related to AML/CFT to ascertain their compliance with the Resolution.

With regard to notaries, Art. 3 of Resolution 77 of 2017 empowers the MOJ's Notarization Department with with monitoring compliance by notaries with AML/CFT legislation. The Bahraini authorities have advised that the Notarization Law provides power for the Department to carry out onsite and offsite supervision and to require information and documents to be provided to it.

The Regulatory framework for real estate brokers and agents was recently transferred from the MOICT to RERA, which is now the licensing authority for them.

The CBB has supervisory responsibility for professional trustees. These fall within the specialised licensee regime of the CBB and are subject to the same provisions as those mentioned in R.27. CSPs are regulated by MOJ, as the provisions made for lawyers and legal professionals explained above apply.

***Criterion 28.3*** - See criterion 28.2 above. In addition, Art. 4 of MO 173 specifies that auditors must ensure that all clients have internal control systems on the reporting of suspicious or extraordinary transactions, the adequacy of internal controls on verification of customers and the nonexistence of suspicious or extraordinary transactions. In addition, for persons registered with the MOICT, auditors must verify that the registered person reports all suspicious or extraordinary transactions to the MOICT and not infringe any of the provisions of the Order. No systems for monitoring compliance with AML/CFT requirements exist for other categories of DNFBPs.

***Criterion 28.4*** -

*(a)* See criterion 28.2 above.

*(b)* MOICT registered entities (including their owners and directors) are subject to vetting by the MOI for background checks. Any ownership change is also subject to these vetting procedures. In addition, auditors are subject to the Auditors Law of 1996. Art. 2 specifies that auditors must be of good repute and not convicted of a breach of trust or crime affecting his honour or integrity or, a crime involving

professional ethics, unless he has been reinstated or three years have passed since the final judgment for the offence. Art. 16 of the law requires auditors to obtain a licence from the MOICT, which requires a check by the MOI.

Lawyers need to be of good conduct and reputation so as to be able to respect the duties of the profession. He/she shall not be convicted of misdemeanour or felonies that relates to honour, honesty and integrity (Art. 2 Decree No.26 (1980))

With regard to notaries, licensing provisions for private sector notaries were introduced by Resolution 78 of 2017. Notaries must be licensed; the term of each licence is three years. There are no licence criteria related to criminality in the resolution but the applicant must not have been stricken from the register (Art. 4) and licensed notaries must provide their services with accuracy, integrity and competence (Art. 12). The Bahraini authorities also advise that Law 37 of 2017 includes a provision which permits a criminal check on the good standing of all notaries although copies of the relevant provisions have not been provided to the evaluation team. Real estate brokers and agents are required to submit a clearance certificate from MOI covering all directors (though not beneficial owners). Professional trustees are subject to the standards specified in R.27. CSPs are regulated by MOJ, as the provisions made for lawyers and legal professionals explained above apply.

*(c)* Persons falling within the scope of Decree Law No. 4) of 2001 are subject to the penalties in that law for breaches of the law. MO 173 empowers the MOICT to reject the appointment of a person as a compliance officer or suspend his/her registration (Art. 10). Any person who breaches the order is subject to the penalties in Decree Law No.4 of 2001 (Art. 12). The requirement that each registered person should develop regulations and procedures to ensure the commitment of employees to implementing the Order means that the Art. 12 penalty applies to individuals. For legal persons Art. 10 of Resolution 64 of 2017 states that any person who violates the Resolution shall be subject to the penalties in Decree Law No. 4 of 2001. Art. 5 of Resolution 77 of 2017 specifies that notaries are subject to the penalties in the Decree Law. Professional trustees are subject to the standards specified in criterion 27.4 and R.35. As CSPs are regulated by lawyers, the provisions applicable to lawyers will apply.

***Criterion 28.5*** - The MOICT has a framework in practice which is a largely risk based approach to supervision. It has risk graded each DNFBP it supervises using a written template which include AML/CFT and a minority of elements, which the evaluation team is not persuaded have much or any AML/CFT value. Ratings are also considered annually and during onsite inspections. Offsite supervisory information informs the content of inspections. High risk entities are subject to more than one inspection a year and to longer inspections than other businesses, with more customer files being reviewed. The decision on which inspections to undertake is informed by diversity and type of business but the degree of discretion allowed under the risk based approach is not. There is a separate, basic written procedure on the MOICT's approach to onsite inspections. The document does not cover intensity of supervision, offsite supervision, the degree of discretion allowed to DNFBPs under the risk based approach or that risk ratings appear to be re-examined in practice during the inspection.

In relation to professional trustees, the approach of the CBB identified at criterion 26.5 applies (although no onsite inspections have been undertaken to professional trustees and they have not been risk rated).

Other supervisors have not undertaken supervision falling within the scope of criterion 28.5 and there are no written procedures or other documents on risk.

### *Weighting and Conclusion*

The gaps related to the regulatory and sanctions powers mentioned under c.28.3, c28.4, and to the limited application of risk-based AML/CFT supervision mentioned under c.28.5 have a moderate impact on the rating.

**Recommendation 28 is rated Largely Compliant.**

## *Recommendation 29 - Financial intelligence units*

Bahrain was rated largely compliant with former R.26 as there was a lack of guidance related to the filing of STRs. FATF standards have been significantly strengthened, imposing new requirements focused on the FIU's strategic and operational analysis functions, and powers to disseminate information upon request and request additional information from reporting entities.

***Criterion 29.1*** - The FID is Bahrain's FIU. It was established by the MOI to receive and analyse STRs related to ML, TF, and related offences [Art. 4.4 Decree Law No. (4) of 2001, MO (102) of 2001 which was amended by MO No.8 (2007), and MO No.9 (2007), which added TF to its mandate]. MO No.17 (2017) further clarified the role of the FID, clarifying among others, that it has a duty to conduct operational and strategic analysis. The Public Prosecution Office (PPO) is the competent authority to conduct ML, TF, and predicate offence investigations. The FID is authorised to disseminate its initial analysis to the PPO for further investigation and possible prosecution [Art.4 MO No.18 (2002)].

***Criterion 29.2*** -

*a)* The FID is the designated authority to receive STRs related to ML, TF, and related offences from reporting entities (Art. 1, Decision No.18, 2002). The CBB and MOICT are also required to receive these reports, which inform their supervisory activities.

*b)* The FID directly receives reports from the customs authorities as it relates to the disclosure system (See c.32.6).

***Criterion 29.3*** -

*a)* Institutions are required to provide the FID with further information or assistance upon request [Art. 5(d) Decree Law No.4 (2001)]. Further, upon court order, any person must submit any information (including documents) to the FID.

*b)* The FID is a law enforcement FIU and therefore has direct access to police databases (i.e. it is part of the Najem unified criminal database system), in addition to several investigative and intelligence related databases, including those of the traffic police, immigration, passports and residence affairs. The FID is also authorised to request information from other authorities, such as the SLRB, MOICT, Coastguard, the CBB, and the Notarisation Office in the MOJ.

***Criterion 29.4*** - Art. 2 of MO No.17 (2017) formally added the implementation of operational and strategic analysis to the competences of the FID, although this was already conducted by the FID and included in several clauses of the FID's Manual of internal procedures.

*a)* In addition, the FID gave some examples of operational analysis being conducted while pursuing ML cases where a variety of sources were used and flows were identified in money changers, companies, etc.

*b)* The FID also conducts strategic analysis. Examples were provided on trends distributed to custom officers and to the Anti-Narcotics Directorate.

The FID uses a vast amount of available and obtainable information, considering it has direct access to the MOI network (all law enforcement agencies), SLRB, MOICT and other authorities.

***Criterion 29.5*** - The FID can refer all files on ML, TF and related crimes to the PPO for investigation [Art. 4 MO No.18 (2002)] and can share information with other law enforcement authorities via encrypted message through the MOI network.

***Criterion 29.6*** -

*a)* The FID has rules in place governing the security and confidentiality of its information, including a specific policy for information technology with rules on incoming and outgoing web traffic and firewalls. In addition, FID employees are forbidden as officials, from disclosing any information or documents protected by Art.5 of Decree Law No.16 (2014), which is Bahrain's general law on the protection of state information and documents. The penalties for disclosing such information is up to seven years' imprisonment and a fine not less than BHD 1000 (EUR 2 147) and no more than BHD 3000 (EUR 6 441).

*b)* FID employees are subject to security clearance and are public servants called to conduct themselves with honesty and integrity and this is a factor that can contribute to the adequate handling of information. They are also subject to other restrictions in revealing information on investigations, as part of the public forces. Employment in the FID is completed upon the submission of a certificate of good conduct by the applicant. Furthermore, employment contracts place particular emphasis on staff members' commitment to maintain confidentiality and the consequent disciplinary measures incurred in case of relevant breaches. Periodic monitoring is conducted by the Preventive Security Department to identify any cases of staff integrity breaches. There have been no cases of breach of integrity by the FID staff and members.

*c)* Anyone who enters or attempts to illegally enter a restricted place or to access information systems with an intention to obtain information or documents protected under the provisions of the Decree Law No.16 (2014) shall be punished by imprisonment for a term not exceeding five years [Art. 6(d)].

***Criterion 29.7*** -

*a)* The FID has the authority to receive and analyse information and proceed on ML, TF and related offences investigations [Art. 4.4 Decree Law No.4 2001] and it does so under the umbrella of the MOI but with a separate budget and with the FID Director having the authority to make decisions within the FID, including to disseminate information to other LEAs.

*b)* According to the same Art. noted above, the FID has the power to implement relevant international co-operation procedures as provided in that law, which has enabled it to sign several MOUs.

*c)* The FID has direct report to the Minister of Interior and although within the MOI complex of buildings and wing, it has an independent structure to carry out its functions (with both human and administrative resources). The FID also has an independent server to the MOI.

*d)* The FID has its own budget approved by the Minister of Interior, where once approved; individual expenses do not need to be re-approved.

***Criterion 29.8*** - The FID has been an Egmont Member since July 2003.

### *Weighting and Conclusion*

**Recommendation 29 is rated Compliant.**

## *Recommendation 30 – Responsibilities of law enforcement and investigative authorities*

Bahrain was rated largely compliant with former R.27, as it had in place *de facto* investigatory powers for TF offences, but no formal regulation for postponing or waiving seizures. This has since been addressed through the criminalisation of TF.

***Criterion 30.1*** - The FID has the responsibility to conduct initial investigations and compile evidence related to ML/TF and related offences, as well as to execute decisions, orders, decrees issued by the competent courts in relation to ML/TF and related offences [s.6 Decree No.4 (2001)]. The PPO is responsible for judicial investigation and prosecution of ML/TF and predicate offenses.

***Criterion 30.2*** - The MOI (including the FID) and the PPO are authorised to investigate ML/TF offences during a parallel financial investigation regardless of where the predicate offence(s) occurred.

***Criterion 30.3*** - Upon receipt of an order issued by the PPO, the FID is authorised to search public or private premises and seize property subject to confiscation. The FID may also order the freezing of property for up to 72 hours prior to receiving a court order (Art. 6.2 Decree Law No.4 (2001)). PPO is also empowered (Art. 98 of the CPC), in the case of necessity or urgency, to temporarily issue a prohibition order forbidding disposal or management of property belonging to the accused, his/her spouse or minor children. The PPO is required to refer the prohibition order to the High Criminal Court within seven days from its issuance.

***Criterion 30.4*** - Bahrain Customs is responsible for implementing Bahrain's disclosure system. Disclosure information is required to be sent directly to the FID (Circular no.7 of 2008). Bahrain Customs has some law enforcement powers through Decree No.12 of 2017 to investigate smuggling offences, including search and seizure.

***Criterion 30.5*** - There are no specialised anti-corruption bodies in Bahrain; corruption is investigated by the MOI (General Directorate of Anti-corruption and Economic and Electronic Security) and prosecuted by the PPO. The FID receives reports internally from the Anti-Corruption Crime Directorate, and externally from

the PPO and can identify, trace, and initiate freezing and seizing of assets in such cases.

### *Weighting and Conclusion*

**Recommendation 30 is rated Compliant.**

## *Recommendation 31 - Powers of law enforcement and investigative authorities*

Bahrain was rated partially compliant with former R.28 as there was no autonomous or predicate TF offence as a legal basis for investigative/compulsory measures. This has since been addressed through the criminalisation of TF.

***Criterion 31.1*** - Law enforcement powers are set out in the Criminal Procedures Code (CPC), and may be used in ML/TF, and predicate offence investigations. Decree No.4 (2001) also outlines powers for LEAs related to investigating ML, and Decree No.58 (2006) includes some investigatory powers specific to TF investigations. Decrees No.4 and no.58 duplicate many of the investigatory powers contained in the CPC.

The CPC establishes powers relating to:

a) providing production orders: Art. 86 empowers the PPO to order "the person in possession of a thing which he decides to seize or inspect it to produce such thing."

b) searching of persons and premises (Art. 66-70, 90-92)

c) taking witness statements (Art. 114-121)

d) seizing and obtaining evidence (Art. 73)

According to Decree No.4 (2001), where the FID has evidence that a person has committed, attempted to, participated in ML, it may obtain an order from the PPO to:

- order the production of records held by FIs, DNFBPs, and other natural or legal persons [Art. 6.1(a)];
- enter into public or private premises to search for any documents, records, papers or objects which are required for the investigation [Art. 6.1(b)]
- seize any property subject to confiscation [Art. 6.1(c)]. Further the FID may seize property in order to prevent its disposal on their own authority, provided that they notify the PPO within three days of seizure (Art. 6.2).

Decree No.58 (2006) also includes powers related to terrorism investigations, including TF. For instance, Art. 30 states that the PPO, upon prior approval by the High Court, may order access or receipt of any data or information related to the accounts, deposits, trusts or safe deposit boxes with banks or other financial institutions or the transactions related thereto if this is deemed necessary for revealing the truth in any of the crimes provided for in this Law.

***Criterion 31.2*** -

***(a, c, d)***: LEAs have the authority to conduct undercover operations, access computer systems, or conduct controlled deliveries for ML, TF, and predicate offences (CPC; IT Crimes Act). This was confirmed through case studies as well.

***b)*** The interception of communications is provided for in Art. 93 CPC and is conducted under the supervision of the PPO after lower court authorisation. Further, in regard to TF investigations, Art. 29 of Decree No.58 (2006) permits the Attorney General or whoever acting on their behalf to order the surveillance of communications by all methods and recording of everything that takes place in public or private premises where this is useful for uncovering the truth in crimes to which the provisions of this Law applies (which includes TF).

***Criterion 31.3*** -

a) Art. 111 of the CBB Law permits the CBB to demand a licensee, by written notice, to provide any information, documents, statistics, yearly reports or any other periodical reports required by the CBB Law. Art. 117 allows licensees to disclose confidential information in the process of executing a court order or in compliance with the provisions of the law or for the purpose of implementing instructions given by the CBB. This information extends to whether a natural or legal person holds or controls an account.

b) The CBB can disclose confidential information to LEAs upon order by the court, without prior notification.

***Criterion 31.4*** - In addition to its core FIU responsibilities (See R.29), the FID is responsible for the initial investigation of ML/TF, and the PPO is responsible for further judicial investigations. The PPO can obtain any relevant information held by the FID to support its investigations.

### *Weighting and Conclusion*

**Recommendation 31 is rated Compliant.**

## *Recommendation 32 – Cash Couriers*

Bahrain was non-compliant with former SR.IX, as a declaration or disclosure system was not in force and effect. Bahrain has since amended Decree No.54 (2006) and introduced Decree No.12 (2017) to establish a disclosure system.

***Criterion 32.1*** - Decree no.12 2017 establishes a disclosure system for "funds" entering or exiting Bahrain by natural and legal persons. The term "funds" cross references the definition of property in Decree No.4 (2001), which captures currency and BNIs. This includes funds imported or exported through shipments or parcels transported by courier services by natural or legal persons or any other organisations.

***Criterion 32.2 (N/A)*** Bahrain does not implement a declaration system.

***Criterion 32.3*** - Upon suspicion, customs officials may demand persons (natural or legal) to provide a truthful disclosure about the funds in their possession [Art. 3 Decree No. 12 (2017)] and provide express answers in this respect. As noted above, the term "funds" captures currency and BNIs.

***Criterion 32.4*** - In case of false or non-disclosure, customs officials are empowered to demand additional information about the source of funds, their owners and other parties related thereto, and reasons of their entry or exit [Art. 3 Decree No.12 (2017)].

***Criterion 32.5*** - The Customs Orders (Art. 9) establishes the penalties for violations of the disclosure system, which cross-references the penalties of ML offence in Decree Law No.4 (2001). The penalty is a fine not exceeding BHD 1 million (EUR 2 million) and a maximum imprisonment of seven years. This penalty is proportionate and dissuasive.

***Criterion 32.6*** - Disclosure information is required to be sent directly to the FID (Circular No.7 of 2008).

***Criterion 32.7*** - Art. 4 of Decree No.4 (2001) establishes a domestic policy and operational co-ordination mechanism to prevent ML/TF. Specifically, this Art. establishes a policy Committee, as well as FID to *inter alia,* conduct investigations and compile evidence on ML/TF. Both the FID and customs authorities belong to this Committee. Further, Customs and FID are connected through integrated IT systems.

***Criterion 32.8*** - Competent authorities are able to restrain currency and BNIs where there is a suspicion on ML/TF, where a false disclosure was made, and when no disclosure is made [Art. 4 Decree No.12 (2017)]. This decree does not permit restraining cash or BNIs upon suspicion of predicate offence. However, Art. 2 of MO No.18 (2002) permits the FID and customs officials, upon receipt of a judicial order, to compel a person "to submit any information that may prove useful to the investigation" or to seize "any money during investigations and collection of information until ascertaining the legitimacy of its source." Bahrain stated that a judicial order can be obtained within 24 hours.

***Criterion 32.9*** - Art. 8 of Decree No.12 (2017) requires the FID to retain all disclosure information to facilitate international co-operation, including information on the value of currency and BNIs.

***Criterion 32.10*** - The information collected pursuant to the disclosure obligations are subject to confidentiality or other safeguard measures.

***Criterion 32.11*** - Persons who are carrying out a physical cross-border transportation of currency and BNIs related to ML/TF are subject to ML/TF offences (See R.3 and R.5). Powers exist to confiscate criminal proceeds or instrumentalities (See R.4). Further, Art. 4 of Decree No.12 (2017) permits Customs to seize funds upon suspicions of ML/ TF, and immediately notify the FID.

### *Weighting and Conclusion*

Bahrain cannot immediately restrain cash or BNIs upon suspicion of a predicate offence.

**Recommendation 32 is rated Largely Compliant.**

## *Recommendation 33 – Statistics*

Bahrain was rated PC for R.32 (the predecessor to R.33) in its 3rd MER given the limited availability of AML/CFT statistic information.

***Criterion 33.1*** - There is no legal requirement for Bahrain to maintain comprehensive statistics relevant to its AML/CFT regime, however some statistics are maintained as required by the Recommendation and internal PPO procedures mandate it to keep statistics.

*(a) and (b)* Bahrain maintains statistics on STRs received and disseminated and on ML/TF investigations, prosecutions and convictions.

*c)* Bahrain maintains statistics on property frozen; seized and confiscated although not in a consolidated manner; and

*d)* Bahrain maintains statistics on MLA or other international requests for co-operation made or received, which would be more comprehensive if they included details on the timeliness and the type of requests.

### *Weighting and Conclusion*

Bahrain maintains statistics on STRs, property frozen, seized and confiscated (although not consolidated), as well as on MLA or other international co-operation requests (both incoming and outgoing) Statistics on MLA and international co-operation requests need to be further improved by including details on the timeliness and types of requests.

**Recommendation 33 is rated as Largely Compliant.**

## *Recommendation 34 – Guidance and feedback*

Bahrain was rated largely compliant with former R.25 due to some regulatory and awareness weaknesees, particularly amongst capital markets licensees.

***Criterion 34.1*** -

***Guidance and feedback by supervisors***

FIs: Section 38 of the CBB Law specifies that the CBB can issue guidance. The CBB has issued seven volumes of the financial crime module of its Rulebook under section 38 of the CBB Law (which refers to the issue of directives and regulations); these volumes largely contain rules, with a few elements of guidance. Other types of outreach made and guidance issued by the CBB are included in IO.3. Overall, once the NRA has been published, the CBB should issue enhanced guidance (taking account of the NRA), including guidance on emerging trends, trade based ML and FinTech. The CBB also provides feedback in relation to poor quality STRs by asking for further information and/or holding bilateral meetings with individual reporting entities where necessary to enhance their reporting.

DNFBPs: Art. 2 of the MO 173 specifies that the MOICT can issue guidance. Criterion 1.1 and IO.3 specify the guidance which has been issued by the MOICT. Evidence was provided of contact with DNFBPs to understand better the content of individual STRs. Common reasons for reporting suspicion is provided by the MOICT to its reporting entities. The MOICT has begun to provide information to assist DNFBPs, particularly focussing on suspicion. It has made its risk assessments public (redacted in the case of auditors as it contains firm-specific information). It also issues circulars approximately each month on matters such as the filing of STRs, STR trends and the introduction of new standards. The MOICT contacts individual DNFBPs when more information is needed on an STR which has been made. Onsite inspections and emails are used to increase understanding of STRs. The Ministry's website also contains general information on AML/CFT. The MOICT should extend its existing outreach by issuing comprehensive guidance on the AML/CFT measures to be adopted by entities it supervises and, in light of the NRA and that guidance,

review its approach to outreach so as to ensure that it is AML/CFT risk based and effective.

Guidance and feedback is not issued in relation to DNFBPs other than those supervised by the MOICT; there are no legal provisions or procedures on the issue of guidance or feedback.

***Guidance and feedback by the FIU***

FID's most recent annual report specifies that its objectives include raising awareness on new methods and trends, indicators and improving reporting. FID has an AML/CFT awareness department (Research and Co-operation Section), which provides feedback to specific entities on STRs submitted. FIs and DNFBPs are generally satisfied with the feedback that they receive but are of the view that it could be further improved through the provision of information on the final decision on cases reported. FID provides general AML/CFT information through its website, including statistics on ML/TF reporting. It also has exchanges with MLROs directly as well working through the CBB and MOICT. The evaluation team noted that both FIs and DNFBPs met indicated difficulties in detecting suspicious transactions related to TF and would welcome additional guidance from authorities in this area. It would be useful if Bahrain issues further guidance to the reporting entities, specifically DNFBPs, including typologies and red flag indicators, including for TF.

### *Weighting and Conclusion*

There is a case for aligning guidance across sectors on a number of issues, including risks, typologies, trends and red flags.

**Recommendation 34 is rated Largely Compliant.**

## *Recommendation 35 – Sanctions*

Bahrain was rated largely compliant with former R.17 due to deficiencies related to the lack of co-ordination between criminal and administrative sanctioning and the lack of corporate liability.

***Criterion 35.1*** -

*a) Targeted Financial Sanctions (R.6):* The criminal penalties available in the AML/CFT Law for breaches under that law are applicable to breaches relevant to TFS. The administrative penalties of the CBB Law (See below) are similarly applicable in relation to FIs, as are the penalties mentioned below for DNFBPs.

*b) NPOs (R.8):* See criterion 8.4.

*c) Preventive Measures and Reporting (R.9-23):* Any contravention of regulations and orders issued under Decree Law No.4 (2001) can be punished by a maximum of three months' imprisonment and/or BHD 20 000 (approximately USD 53 000) fine (Art. 3.5). This applies to both natural and legal (corporate) persons. In addition, criminal sanctions (maximum of two years and/or BHD 50 000 fine (USD 133 000) would be imposed on anybody who is found guilty of any of the following "offences related to money laundering" [Art. 2.6 and 3.4 Decree Law No.4 (2001)]: non-disclosure of suspicious transactions; obstructing the execution of Law Enforcement Unit's or judicial orders; tipping-off on investigating or freezing orders.

FIs - See criterion 27.4. The CBB may impose conditions and directions on a licensee. It also has power to make public statements, appoint an observer member on the board of directors, place the licensee under administration and suspend and revoke licences. The administrative penalties may reach up to BHD 100 000 per violation and breach.

DNFBPs - As indicated in criterion 28.4(c), breach of the Orders/Resolutions issued in relation to DNFBPs subject to the supervision of the MOICT and legal professionals and notaries are also subject to the penalties in Decree Law No.4 (2001). In addition, MOICT has powers to issue Order to its registered entities to stop the breach and eliminate their reasons and effects. In case of a failure to abide by the Order, the MOICT may suspend registration of the licensee for a period not exceeding three months, impose an administrative fine not exceeding BHD 20 000, publish a statement of breach and also refer the case to PPO in case of a criminal offence (Art.20 of Decree No. 27 of 2015). MOICT may also order closure of business for non-fulfilment of registration conditions, and violation of its Order (Art.22 of Decree No. 27 of 2015). Also see criterion 28.4 for the other DNFBP supervisors.

***Criterion 35.2*** -

a) Targeted Financial Sanctions (R.6): See criterion 35.1 above.

*b) NPOs:* There are no specific sanctions for senior management or directors regarding NPOs although there are general sanctions applying to "every person" related to the NPO which incurs in a given misconduct [Art. 89, 90 and 91 of Decree Law No. 21 (1989) and Decree Law No. 21 (2013)].

c) Preventive measures and reporting

Criminal sanctions: The measures in Decree Law No.4 (2001) mentioned above [c35.1 (c)] apply to individuals.

The CBB can remove any director, manager or official responsible for the direction or management of a licensee for violations, under its fit and proper framework. The CBB can also issue public statements in this regard. In addition, under EN-5.1.3 of the CBB's enforcement module, a director, manager or responsible official is considered removed from office should he be convicted by a court for a crime affecting his honesty; is declared bankrupt by a court; or if a court rules that his legal capacity is totally or partially impaired.

Under Art. 11 of MO 173, the MOICT may reject the appointment of a person as a compliance officer or suspend his registration.

If a lawyer is convicted of misdemeanour or felonies that relates to honour and honesty, he would lose one of the conditions required for being a licensed lawyer and will be disqualified after following disciplinary procedures as outlined in the law (Art. 2 of 26 of 1980).

### *Weighting and Conclusion*

Administrative sanctions available to authorities other than the CBB are not fully dissuasive or proportionate.

**Recommendation 35 is rated Largely Compliant.**

## *Recommendation 36 – International instruments*

Bahrain was rated partially compliant with formerR.35 and SR.I, primarily due to a lack of full implementation of the International Convention for the Suppression of the Financing of Terrorism.

***Criterion 36.1*** - Bahrain ratified the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 through Law No.17 (1989). Bahrain also ratified the United Nations Convention against Transnational Organized Crime 2000, the Palermo Convention, as reflected in Decree Law No.4 (2001). Bahrain also ratified the United Nations Convention against Corruption (Merida Convention) as reflected in Decree Law No.7 (2010). Bahrain ratified the International Convention for the Suppression of the Financing of Terrorism according to Law No.8 (2004).

***Criterion 36.2*** - Some elements are outstanding as detailed in analysis of R.3 and 5, such as the criminalisation of legal persons for ancillary offences and the exemption to the terrorism offence.

### *Weighting and Conclusion*

Bahrain meets most of the requirements for R.36, except some elements stated in detail in analysis of R.3 and R.5, such as the exemption clause in the definition of terrorism, availability of ancillary offences to legal persons.

**Recommendation 36 is rated Largely Compliant.**

## *Recommendation 37 - Mutual legal assistance*

Bahrain was rated largely compliant with former R.36 and SR.V due to a lack of statistics on Mutual Legal Assistance (MLA).

***Criterion 37.1*** - Bahrain has a legal basis to rapidly provide the widest possible range of MLA in relation to the investigation, prosecution and related proceedings of ML, TF and other offences [Art.9 of Decree Law No.4 (2001)], which requires, among other things, timeliness in addressing requests. Art. 426 and 428 (chapter two-Judicial Delegation of Authority) of the Criminal Procedure Code (CPC) also provides a legal framework for MLA in respect of ML, associated predicate offences and TF, as well as extradition requests. Art. 426 allows direct communication between judicial authorities of the requesting and requested states. In addition, Bahrain is a member of Arab League and has been party of Riyadh Arab Convention for Judicial Co-operation (1983). Bahrain has bilateral agreements on judicial and legal co-operation with Syria, India and Egypt. International conventions referred in R.36 are also taken as a basis for MLA requests.

***Criterion 37.2*** - MLA requests are received by the MOJ and approval is accorded by the High Court (Art. 426-427 CPC). According to Art. 426 and 427 of the CPC, the High Criminal Court is the central authority for foreign (incoming) mutual legal assistance requests. The High Criminal Court and the MOJ are the central authorities for sending (outgoing) requests for mutual legal assistance, through diplomatic channels. The High Criminal Court after approval transmits the MLA requests to the competent judicial authority (usually PPO) unless they conflict with the public order.

The concept of "public order" is not defined in the Law but authorities noted that this is meant to be for example, the request made would violate defendants' rights regarding due process).

There is no specific rule on the timeliness of requests or on prioritization but Art. 426 of the Criminal Procedures Code contemplates urgent matters being addressed by direct communication between parties. Also, at the time of the onsite, the case management system in use did not allow for proactively monitoring progress as well as timeliness of response. In April 2018, the features were enhanced and the system now provides additional details and generates automatic pop-up alerts to enable a prompt response.

***Criterion 37.3*** - MLA is not prohibited or unduly restricted. According to Art. 427/1 of the CPC, the High Criminal Court directly transmits MLA requests to the competent judicial authority (Judge or PPO) unless they conflict with the public order (See 37.2 on what could constitute a reason of "public order").

***Criterion 37.4*** -

***a)*** There are no provisions restricting legal assistance within the framework for providing legal assistance [i.e. Art. 8 of Decree Law No. 4 (2001) and in practice, fiscal matters are not deemed or have been used as barriers for refusing a request for mutual legal assistance].

***b)*** Regarding secrecy and confidentiality rules, Art. 7 of Decree Law No.4 (2001) establishes that no institution can plead before the PPO or the competent Court, secrecy or confidentiality in respect of accounts, identification of customers or record keeping provided under the provisions of any Law. In addition, Art. 117 and 118 of the CBB law provide a framework for disclosing confidential information and accordingly, a licensee or CBB itself may disclose such information in accordance with the provisions of the law or any international agreements to which Bahrain is a signatory, in the process of executing an order issued by a competent Court. Thus, secrecy and confidentiality requirements cannot be put forward to refuse an MLA request.

***Criterion 37.5*** - There is no specific provision in Bahrain domestic law for maintaining the confidentiality of mutual legal assistance requests received. However, the confidentiality of investigation procedures set forth in Art. 83 of the CPC apply (as it would to domestic investigations) and anyone who violates confidentiality of an investigation shall be liable to a punishment of imprisonment not exceeding one year or a fine not exceeding BHD 100 (EUR 215) according to Art. 371 of Penal Code.

Furthermore, Art. 119 of CBB law (related to confidentiality of financial information kept by licensees and the CBB) imposes a specific restriction on disclosing confidential information which would apply to MLA requests. The conditions for disclosing confidential information are delineated in Art. 117 and 118 of the CBB Law, which prohibit disclosure of confidential information unless requested by competent courts in regard to MLA. In other circumstances, no person can disclose it, whether he/she receives it directly or indirectly.

***Criterion 37.6*** - Bahrain does not require dual criminality to execute MLA requests they receive pursuant to Decree Law No.4 (2001).

***Criterion 37.7*** - Bahrain does not require dual criminality (See above) for executing MLA requests and implementing coercive measures (Art. 427 CPC).

***Criterion 37.8*** - Art. 8 of Decree Law No.4 (2001) provides for the use of authorities specific powers when providing international co-operation, such as applying to a court for a search warrant, obtaining any document or object relevant to identifying, locating or quantifying any property which reveals the possession, control or transfer of a property, seizing, and managing or disposing such property. Authorities explained that in practice, requests from a foreign country are therefore handled in the same way as an investigation being carried out domestically. Bahraini authorities are able to exercise all the relevant powers and investigative techniques as set out in R.31 for mutual legal assistance requests.

### *Weighting and Conclusion*

Bahrain meets many of the requirements for R.37. Nevertheless, Bahrain did not have a case management system that enabled it to track progress of requests at the time of the onsite. This was put in place in April 2018 following the onsite visit. Minor deficiencies in R.5 noted in R.36 above, do not impact MLA requests given Bahrain's approach to find the most appropriate means to cooperate (See 37.7).

**Recommendation 37 is rated Largely Compliant.**

## *Recommendation 38 – Mutual legal assistance: freezing and confiscation*

Bahrain was rated largely compliant with former R.38, given the lack of a fund for assets which were confiscated.

***Criterion 38.1*** - Bahrain has the authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize or confiscate property, including laundered property, proceeds, instrumentalities and property of corresponding value as listed in (a)-(e) of this criterion, pursuant to Art. 426 - 427 of the CPC and Art. 8 of Decree Law No.4 (2001) and its amendments (See R.37 and R.4 (as same domestic powers are available for international requests)).In particular for confiscation, execution of foreign confiscation orders is possible in line with Art. 12 of the Penal Code which establishes the general principles for enforcement of decisions given by foreign courts.

***Criterion 38.2*** - Non-conviction based confiscation is possible in Bahrain within the context of criminal proceedings in cases when the suspect dies or absconds before conviction in accordance with the provisions of Art. 3.2 of Decree Law No.4 (2001), Art. 17 of the CPC and Art. 64 of the Penal Code. Criminal proceedings are possible in the absence of defendants in Bahrain and foreign MLA requests can be executed in line with the principles of domestic law.

Authorities also indicated that foreign confiscation orders within the context of civil law (in rem) can be executed in Bahrain in line with Civil Procedures Code, Art. 252 and 255 of Decree Law No. 12 (1971), Civil and Commercial Proceedings Code, pursuant to Art. 4 of the CPC which indicates that the provisions of the Civil and Commercial Proceedings Code apply unless there is a special provision in the CPC and to the extent it does not conflict with this provisions. Art. 252 and 255 refer to the execution of orders of judgements of a foreign country, following the laws and

procedures of that country, including when a perpetrator is unavailable or unknown.

***Criterion 38.3*** -

a) There are no mechanisms or arrangements for coordinating seizure and confiscation, in cross-border cases. However, authorities have used telecommunication tools to coordinate for urgent cases.

b) Art. 8.2 (c) of Decree Law No.4 (2001) allows Bahrain's Authorities to obtain an order from the court for managing and disposing of seized property. Art. 98, 99 of the CPC and Resolution No.66 (2017) as detailed in Recommendation 4 above, refer to the procedures to follow with seized property, including where necessary, the appointment of a public or private entity specialized in the management and/or investment of property. There is no asset management office or specific procedures to handle confiscated assets, which are returned to the treasury.

***Criterion 38.4*** - Art. 8.6 of Decree Law No.4 (2001) allows Bahrain to share assets with other countries. Bahrain has dealt with requests for asset sharing on the basis of reciprocity.

### *Weighting and Conclusion*

Bahrain meets many of the requirements for R.38, except for the lack of mechanisms for coordinating the seizure and confiscation measures with other countries and the lack of mechanisms for managing or disposing confiscated property (as discussed in its previous MER).

**Recommendation 38 is rated Largely Compliant.**

## *Recommendation 39 – Extradition*

Bahrain was rated largely compliant with former R.39 as statistics were unavailable on the time taken to complete the extradition process.

***Criterion 39.1*** -

*a)* Art. 11 of Decree Law No.4 (2001) and Art. 412-425 of the CPC allows Bahrain to extradite for ML and TF offences.

*b)* Bahrain did not have a case management system at the time of the onsite (See explanation in R.37), but does have clear processes and procedures for the timely execution of extradition requests[7] and implemented a case management system in April 2018:

[7] In addition, it is also relevant that Bahrain does not require extradition treaties with other countries to execute extradition requests. According to article 412 of the CPC, this can be done following the provisions of the CPC, and the rules of international law (and treaties). It uses them however, when requested by the other country. As a member of Arab League, Bahrain is party of Riyadh Arab Convention for Judicial Cooperation (1983) which also has provisions for cooperation on extradition requests. Bahrain is also a party of extradition treaties with Syria and India.

According to Art. 417 of the CPC requests are received by the MOJ through diplomatic channels; then the High Criminal Court examines extradition requests, for the fulfilment of the necessary conditions and procedures. It also has the authority to issue a warrant for searching premises should it be necessary.

Art. 421 of the CPC, allows for direct communication of judicial authorities in urgent cases. Execution of extradition requests should be completed within 30 days unless the requesting country provides a reason for the delay. In any case, the detention period for persons to be extradited cannot exceed 60 days.

*c)* Art. 415 of CPC lists the grounds for refusal and Bahrain does not place unreasonable or unduly restrictive conditions on the execution of requests. In addition, Bahrain's authorities have to inform counterparts of any reason for not executing the request forthwith or of any delay in execution of the request according to Art. 8.1 of Decree Law No.4 (2001).

***Criterion 39.2 -***

a) Art. 415 (a) of the CPC lists the grounds for refusal, Bahrain cannot extradite its own nationals.

b) In case of non-extradition, Bahrain noted that it can take over the prosecution of the suspect according to Art. 8 and 9 of the CPC, however these provisions are very generic and do not indicate a timeline for such execution nor the details of how this will be undertaken.

***Criterion 39.3*** - Extradition is subject to the dual criminality principle according to Art. 413 (b) of the CPC and the principle of reciprocity (for non-treaty countries), and in line with Art. 11 of the Decree Law No.4 (2001). However, there is no requirement for the category of the offence to be identical in both countries and authorities can use the description of criminal conduct in domestic law, which most resembles the crime being presented.

***Criterion 39.4*** - Bahrain has simplified extradition mechanisms such as the direct transmission of requests is possible in urgent cases, in line with Art. 421 of the CPC. Bahrain can and has also facilitated extradition through the Interpol channel as a member of Interpol.

### *Weighting and Conclusion*

Bahrain meets most of the requirements for R.39, except for the existence of a specific case management system which was put in place only after the onsite visit in April 2018, and the fact that with regard to the non-extradition of nationals, measures to deal with them domestically are not fully in line with what is required under 39.2. Given the explained in 39.3, the deficiencies with regard to the TF offence do not have an impact on this Recommendation.

**Recommendation 39 is rated Largely Compliant.**

## *Recommendation 40 – Other forms of international co-operation*

Bahrain was rated compliant with former R.40.

***Criterion 40.1*** - Bahrain's competent authorities (FID, Interpol Directorate and the CBB) can provide international co-operation for ML, associated predicate offences

and TF. The FID can provide assistance according to Art. 9(1) and 9(2) of the Decree Law No.4 (2001). These Articles allow the FID to exchange information spontaneously and upon request. Exchange of information via Interpol channel is based on Bahrain's Interpol membership. Art. 6 and 7 of Ministry of Interior Decision No.18 (2002) refer to international co-operation at a law enforcement level. Art. 122 of the CBB Law allows the CBB to provide assistance upon request. The CBB does not have the authority to spontaneously exchange information. There are no specific provisions that indicate that co-operation should be provided rapidly in all cases.

***Criterion 40.2*** -

a) Art. 8.2 of Decree Law No.4 (2001) and Art.7 of the MOI Decision No.18 (2002), provide an overall legal basis for international co-operation. Bahrain's law enforcement authorities, including the FID, can obtain orders from investigation magistrates, to search and obtain any kind of information or documentation and this would assist in providing co-operation. Art. 118(3) and 122 of the CBB Law also provide a legal basis for international co-operation with international organisations and overseas authorities (as regards financial institutions).There are no specific provisions for the MOICT to cooperate but information on DNFBPs is accessible via law enforcement authorities.

b) There are no impediments for Bahrain to use the most efficient means to co-operate. The above cited Art. 8.2 allows Bahrain's authorities to use the most effective means of co-operating, Art. 7 of the MoI Decision No.18 (2002) and Art. 111, 113 and 121 of the CBB Law provide authorities with a range of powers to avail themselves of different types of information and take a number of actions which would mean they can "use the most efficient means to co-operate".

c) Bahrain has clear and secure channels to facilitate the transmission and execution of requests, including Egmont Secure Web channel for information exchanges between FIUs; the Interpol channel for information regarding cross-border investigations. Additionally, the FID exchanges information via e-mail or secure and encrypted fax systems and the CBB exchanges information via written letters and e-mails.

d) Art. 8.1 of Decree Law No.4 (2001) indicates that authorities should inform of any delays in requests and the PPO indicated that they would normally consider urgent requests for prompt execution. As noted in R.29, there are also some measures to prioritize higher risk requests, for instance, those pertaining to TF. However, there were no specific prioritisation mechanisms to handle requests at the time of the onsite.

e) In terms of safeguarding information received, Bahrain noted that a general provision about the confidentiality of investigations (Art.83 CPC) applies to all MLAs. Also, as regards internal communications, the use of the Najem system provides a confidential channel to communicate. In addition, Art. 117 and 118 of the CBB law restrict the disclosure of confidential information and the fact that Egmont Secure Web is used by the FID in exchange of information requests provides a high level of confidentiality. Further, Bahrain noted that it follows international conventions such as the UNCAC, which refers to information not being used for a purpose different to which the requested State has consented.

***Criterion 40.3*** - Bahrain indicated that in general, for all authorities, no formal agreements are needed to cooperate with counterparts, and that there were several legal bases and mechanisms to provide international co-operation. In addition, international law enforcement networks such as ESW and the Interpol are used to exchange information. Bahrain also indicated that where these have been needed, these have been negotiated. For instance, the FID has 15 MOUs and the CBB signed MoUs with the supervision authorities or central banks of 27 countries as of November 2017, and is a party of IOSCO Multilateral Memorandum.

***Criterion 40.4*** - There is no general impediment to prevent Bahrain's authorities from providing feedback regarding assistance received when requested to do so. The FID regularly provides feedback to other counterparts it exchanges information with, for example, to send additional information that may be useful for that other FIU or LEA, according to their "Policies on Information Exchange" document. They also provide a feedback form that these authorities can complete.

***Criterion 40.5*** - Pursuant to Art. 9 of Decree Law No.4 (2001), as amended by Decree Law No. 54 (2001) [Art. 5 bis (4) and (5)] the FID, FID can exchange information of general nature regarding the ML or TF offence and there are no unreasonable or unduly restrictive conditions on information exchange or assistance with regard to the grounds listed in this criterion.

***Criterion 40.6*** - Bahrain has controls and safeguards for preserving the use and the purpose of information obtained through international co-operation including the provisions in international conventions ratified by Bahrain (as referred in 40.1), the safeguards regarding criminal procedure (i.e. Art. 83 of the CPC) and the Policies on Information Exchange document of the FID. For outgoing requests, Bahrain permits requested FIUs to further disseminate the request to other law enforcement authorities, in all cases (According to the FID's Policies on Information Exchange). For incoming requests, the FID asks the requesting FIUs whether they would allow the dissemination of their requests to a third party, depending on the nature of the request and they apply Egmont Principles for Information Exchange, which includes provisions in this regard. For exchange of information between supervisory authorities, Art. 18 of the CBB's standard MoU template establishes that any confidential information shared pursuant to this Memorandum should be used only for lawful supervisory purposes. Authorities such as the CBB, also provided examples where they make reference to this rule, in their written letters for non-MoU information exchanges.

***Criterion 40.7*** - As mentioned in 40.2 (e) above, for criminal matters, according to Art. 83 of the CPC (and Art. 371 Penal Code), confidentiality of investigations should be kept otherwise anyone who violates confidentiality of an investigation shall be liable to imprisonment and judicial fine. Similarly, CBB Law and standard MoU template include provisions for restricting the disclosure of confidential information. In addition, according to Art. 5 of the Law No.16 (2014), which is the general law for protection of confidential state information and documents, any official is prohibited to disclose any information or documents without legitimate cause. In addition, in practice, FID exchanges information via secure channels, as previously noted in 40.2 (c) and this enhances its ability to preserve confidentiality of requests. There are no provisions regarding DNFBP supervisors, but this tends to

occur through close co-operation between the FID and MOICT for the DNFBP it supervises.

***Criterion 40.8*** - Art. 9.2 of Decree Law No.4 2001 allows Bahrain's authorities to make inquiries on behalf of foreign counterparts and exchange information with them.

***Exchange of information between FIUs***

***Criterion 40.9*** - Pursuant to Art.8 and 9 of the Decree Law No.4 (2001), as amended by Decree Law No.54 (2001) [Art. 5 bis (4) and (5)] the Enforcement Unit (Bahrain's FIU, the FID) can exchange information of specific as well as general nature regarding ML (including its predicate offences) or TF offences. Authorities can also exchange this type of information following Egmont Principles for Information Exchange.

***Criterion 40.10*** - As noted in 40.4, the FID provides feedback with regard to exchange of information requests received.

***Criterion 40.11*** -

The FID has the authority to exchange information with its counterparts under Art. 8 and 9 of the Decree Law No.4 (2001). That authority is in line with this criterion as outlined below.

a) As a law enforcement type FIU, the FID has access to unified criminal system database called Najem which is used in almost all operational directorates in the MOI. In addition, Art. 8.2 allows FID to obtain an order from Investigation Magistrate for the implementation of specific investigation measures to obtain any documents or object relevant to identifying, locating or quantifying any property which reveals the possession, control or transfer of a property. Also, Art. 5(d) of the Decree Law No. 4 (2001) requires reporting institutions to provide information or assistance upon request. All such information gathered can be shared by the FID with its counterparts.

b) FID has the power to exchange any other information which they have the power to obtain or access directly or indirectly at the domestic level, subject to the principle of reciprocity. It is stated in the Policies on Information Exchange Document of the FID, that the FID should seek to provide the broadest range of information, when it comes to international co-operation.

***Exchange of information between financial supervisors***

***Criterion 40.12*** - Art. 122 of the CBB Law provides a legal basis for providing international co-operation with foreign authorities (regulatory and supervisory authority or any foreign central bank as per Art. 1 of the CBB Law). Thus, the CBB is allowed to provide co-operation with its foreign counterparts regardless of their nature and status. Additionally, in line with Art. 118(3) of the CBB Law, it is allowed to exchange confidential information with regard to supervision in co-operation with international financial organisations or competent administrative bodies or authorised committees. The confidential information is defined in Art. 116 of the CBB law and it covers any information on the private affairs of any of the licensee's customers including AML/CFT issues.

***Criterion 40.13*** - Above cited Art. 122 of the CBB Law covers CBB's authority to exchange information with foreign counterparts. Art. 111 and 113 empower CBB to obtain any information or reports from the licensees or their partners by a written notice when needed. Art. 121 of the CBB Law allows appointing investigators in order to respond to international assistance requests (as noted by Art. 122 of the CBB Law).

***Criterion 40.14*** - Above cited Art. 122 outlines the general framework of international co-operation for CBB.

a) CBB is allowed to exchange information with regulatory authorities of foreign countries upon request.

b) CBB is allowed to exchange prudential information with the supervisory authorities of foreign countries, upon request. Examples were given in this regard and the standard CBB MoU template includes provisions for exchange of supervision information between home and host authorities for the operations of cross-border establishments.

c) CBB is allowed to provide information with regard to the licensees' customers upon request and examples were given in this regard.

***Criterion 40.15*** - CBB can conduct inquires on behalf of foreign authorities according to Art. 111, 113 and 121 of the CBB Law. The CBB standard MoUs address the issue of allowing foreign supervisory authorities to conduct inquires in Bahrain or vice versa.

***Criterion 40.16*** - The CBB standard MoU template (Art. 18) includes provisions to ensure that exchanged information be used only for lawful supervisory purposes. The template does not clarify what should be followed in the case of non-supervisory purposes but Art. 115 of CBB Law notes that the CBB can form joint teams with MOI and other authorities for judicial investigations and it is therefore possible to conclude that they would be guided by the same principle. Authorities also provided examples where they refer to this rule in their written letters for non-MoU information exchanges.

***Exchange of information between law enforcement authorities***

***Criterion 40.17*** Art. 9.1 of the Decree Law No. 4 (2001) amended with Art. 5 (bis) of the Decree Law 54 (2006) and Art. 7 of the MOI Decision No. 18 (2002) allow Bahrain's LEAs to exchange information with foreign countries related with ML, related offences and TF and predicate offences. LEAs are allowed to obtain a warrant from investigating judge in the same content to make inquiry. Exchange of information through JCTC and Interpol channel does not require a court order and from examples provided by authorities, this has occurred in many instances.

***Criterion 40.18*** - Bahrain is able to use its domestic powers, including any investigative techniques, for international co-operation requests, as no prohibition exists in domestic law. See R.37.8 above. Bahrain follows the INTERPOL rules for INTERPOL exchanges it makes.

***Criterion 40.19*** - Although there is no indication in domestic law about the possibility of forming joint investigation teams, authorities indicated that they can conduct joint investigations and provided an example in this regard, which was initiated after an MLA request. Bahrain has bilateral judicial and legal co-operation

agreements with Syria, Egypt and India and it is party of the Riyadh Arab Convention for Judicial Co-operation and the Gulf Co-operation Council Security Convention, which enhance Bahrain's ability to provide co-operation, particularly with countries in its same region. Under the GCC Convention, the exchange of information and expertise is encouraged to contribute to prevention methods and combating crimes of all kinds, especially transnational organized or emerging crimes and provide technical support in all security affairs to achieve desired integration. The Convention notes that foreign counterparts shall, collectively or bilaterally, ensure the effective integration of the security services and the field co-operation between them, and provide support, in the case of the request, to any counterparty, in accordance with the circumstances of the requested counterpart. The agreement worked on the exchange of information and expertise in the field of combating crime. The agreement also referred to co-operation in the field of handing over suspects, convicted persons, and combating smuggling. Moreover, the GCC Security Convention included providing ease of training and education in the field of combating crimes, as well as initiating security training institutes for the members. The crimes mentioned in the convention include ML predicate offenses, which makes the FID an integral directorate within the MOI involved in the convention's stipulations; due to the reason that ML predicate offenses can lead to ML offenses, resulting in more efficient AML/CFT framework and operations.

***Exchange of information between non-counterparts***

***Criterion 40.20*** - Bahraini authorities indicated that the FID acts as intermediary body to exchange information with its non-counterparts in ML/TF cases. When an exchange of information request is received by a non-counterparty unit or the subject of the request requires acquiring additional information from a third party agency, they respond to the requests after obtaining the relevant information from that agency. Further, Art. 118(3) of the CBB law covers not only counterparts but international financial bodies and bodies or committees of a judicial function.

### *Weighting and Conclusion*

Bahrain meets many of the requirements under R.40 but there is still room for improvement, for example, regarding the lack of provisions with regard to the timeliness of responses (See criterion 40.1) and that the CBB does not have the authority to spontaneously exchange information. The lack of specific provisions for information to be exchanged related to DNFBPs is also a deficiency (See criterion 40.2).

**Recommendation 40 is rated Largely Compliant.**

# 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 | PC | ML/TF risks have been identified and assessed only to some extent. Bahrain is yet to finalise its first NRA and fully implement a risk-based approach to allocating resources and implementing mitigating measures.<br>• There are currently no requirements for FIs and DNFBPs to ensure that higher risks identified by Bahrain are incorporated in risk assessments.<br>• There are no specific provisions requiring DNFBPs to document their risk assessment or to consider all relevant risk factors while determining the overall level of risk and apply mitigating measures.<br>• Some elements of risk management are missing (See criterion 1.11).<br>• Simplified measures are not risk based (See criterion 1.12). |
| 2. National co-operation and co-ordination | LC | • While Bahrain has put in place a mechanism to create national policies and to ensure co-ordination among authorities, national risk based policies have yet to be developed. |
| 3. Money laundering offences | LC | • The deficiencies identified in R.5 regarding the inclusion of an exemption to the TF offence limits the scope of the TF predicate offence for ML.<br>• Ancillary offences are unavailable to legal persons. |
| 4. Confiscation and provisional measures | C | • All criteria met |
| 5. Terrorist financing offence | PC | • Bahrain's TF offence is not in line with TF Convention. Specifically, its definition of terrorism includes an exemption for "peoples struggle, including armed struggle against foreign occupation, aggression, colonialism, and hegemony, aimed at liberation and self-determination in accordance with the principles of international law". |
| 6. Targeted financial sanctions related to terrorism & TF | PC | • Bahrain's TFS framework does not extend to all natural and legal persons in Bahrain, nor to lawyers, notaries, and real estate agents/brokers, which has an impact in several criteria in this Recommendation.<br>• There is no guidance regarding proposals to the 1988 UN Committee (See criterion 6.1 d).<br>• Limited guidance is available to DNFBPs. Additionally, the MOICT does not require its reporting entities to respond to its email notifications.<br>• The MOICT does not have a procedure to allow access to funds (See criterion 6.7). |
| 7. Targeted financial sanctions related to proliferation | PC | • Bahrain's (PF) TFS framework does not extend to all natural and legal persons in Bahrain, nor to lawyers, notaries, and real estate agents/brokers, which has an impact in several criteria in this Recommendation.<br>• The CBB and MOICT have provided limited guidance to its reporting entities.<br>• The MOICT does not require reporting entities to respond to email notifications.<br>• The MOICT does not have a procedure to allow access to funds (See criterion 7.4 c and 7.5 (a) – (b)). |
| 8. Non-profit organisations | LC | • Bahrain is in the process of following a more risk-based approach to NPOs, in response to the risks identified and this has an impact on several criteria (See criterion 8.1 (a) and (c) and 8.2 and 8.4). Bahrain's NPOs risk assessment needs to be further refined to focus specifically on TF risks.<br>• Bahrain has not encouraged or conducted outreach and educational programmes particularly related to TF. |

| Compliance with FATF Recommendations | | |
|---|---|---|
| **Recommendations** | **Rating** | **Factor(s) underlying the rating** |
| 9. Financial institution secrecy laws | C | • All criteria met |
| 10. Customer due diligence | LC | • There are no specific requirements for FIs to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable.<br>• FIs are allowed to consider returning the funds to the counterparty, when unable to comply with CDD requirements.<br>• There is no provision to allow FIs to not pursue CDD if there is a risk of tipping off and instead file an STR.<br>• The application of requirements to structures other than trusts (e.g. Waqfs) is not clear. |
| 11. Record-keeping | C | • All criteria met. |
| 12. Politically exposed persons | LC | • There is no specific requirement to inform senior management before the pay-out of the policy proceeds, where higher risks are identified. |
| 13. Correspondent banking | LC | • The FC Module allows for simplified CDD measures for FATF/GCC banks in the context of correspondent banking relationships. |
| 14. Money or value transfer services | LC | • There are no explicit requirements that MVTS providers should include their agents in their AML/CFT programmes and monitor them for compliance. |
| 15. New technologies | C | • All criteria met |
| 16. Wire transfers | LC | • There are no specific requirements for financial institutions other than banks for criteria 16.9-16.15.<br>• The potential exception for implementing UNSCRs in the Rulebook should be clarified. |
| 17. Reliance on third parties | C | • All criterion met |
| 18. Internal controls and foreign branches and subsidiaries | LC | • There are no specific provisions to ensure adequate safeguards on the confidentiality and use of information exchanged. |
| 19. Higher-risk countries | LC | • Specialised licensees are not required to apply enhanced due diligence measures when called for by the FATF.<br>• There are no specific procedures in place to ensure that FIs are advised of concerns about weakness in AML/CFT system of other countries. |
| 20. Reporting of suspicious transaction | LC | • The need to report suspicious transactions promptly and to report attempted transactions is not contained in law. |
| 21. Tipping-off and confidentiality | LC | • FIs, their directors and employees are protected from both criminal and civil liability, even though they are not required to report in "good faith". |
| 22. DNFBPs: Customer due diligence | PC | • The main deficiencies relate to identification and verification of BO, timing of CDD, application to existing customers and requirements relating to PEPs. |
| 23. DNFBPs: Other measures | PC | • Attempted transactions are not covered.<br>• Requirements on internal controls and high risk countries are not detailed to meet the FATF standards. |
| 24. Transparency and beneficial ownership of legal persons | LC | • Information on those who may control a legal person through means other than ownership of shares, may not be available (See criterion 24.1 and 24.6).<br>• Bahrain is yet to fully assess ML/TF risks associated with all types of legal persons created in Bahrain.<br>• There is no express bar against nominee shareholders or directors.<br>• There are no measures to monitor the quality of assistance received from other countries in response to requests for basic and beneficial ownership information.<br>• Sanctions for non-compliance may not be dissuasive for large companies. |
| 25. Transparency and beneficial ownership of legal arrangements | LC | • Information on the beneficial owner of a trust (particularly foreign trusts) is not always timely available and the provisions for waqfs are limited; this has an impact on several criteria. |

| Compliance with FATF Recommendations | | |
|---|---|---|
| **Recommendations** | **Rating** | **Factor(s) underlying the rating** |
| 26. Regulation and supervision of financial institutions | LC | • There are some minor deficiencies with regard to measures to prevent criminals or their associates owning or controlling FIs (See c.26.3).<br>• The compliance directorate manual does not include a specific reference to consolidated group supervision for AML/CFT purposes or for review of assessment of the ML/TF risk profile of FIs. |
| 27. Powers of supervisors | LC | • There is no provision for third parties to provide information as required by criterion 27.3, except for partners of licensees;<br>• There is a narrow focussed concern about the maximum level of fining powers. |
| 28. Regulation and supervision of DNFBPs | LC | • The gaps related to the regulatory and sanctions powers mentioned under c.28.3, c28.4, and to the limited application of risk-based AML/CFT supervision mentioned under c.28.5 have a moderate impact on the rating. |
| 29. Financial intelligence units | C | • All criteria met. |
| 30. Responsibilities of law enforcement and investigative authorities | C | • All criteria met. |
| 31. Powers of law enforcement and investigative authorities | C | • All criteria met. |
| 32. Cash couriers | LC | • Bahrain cannot immediately restrain cash or BNIs upon suspicion of a predicate offence. |
| 33. Statistics | LC | • Statistics related to property frozen, seized and confiscated are not consolidated.<br>• Statistics related to MLA or other international co-operation requests (both incoming and outgoing) need improvement by including details on the timeliness and types of requests. |
| 34. Guidance and feedback | LC | • Guidance across sectors should be aligned on issues such as risks, typologies, trends and red flags. |
| 35. Sanctions | LC | • Administrative sanctions available to authorities other than the CBB are not fully dissuasive or proportionate.<br>• There are no specific sanctions for senior management or directors regarding NPOs. |
| 36. International instruments | LC | • Bahrain meets most of the requirements for R.36, except some elements stated in detail in analysis of R.3 and R.5, such as the exemption clause in the definition of terrorism and availability of ancillary offences to legal persons. |
| 37. Mutual legal assistance | LC | • Bahrain did not have a case management system that enabled it to track progress of requests at the time of the onsite. |
| 38. Mutual legal assistance: freezing and confiscation | LC | • Bahrain lacks a mechanism for coordinating the seizure and confiscation measures with other countries;<br>• Bahrain lacks a mechanism for managing or disposing confiscated property. |
| 39. Extradition | LC | • Bahrain did not have a specific case management system at the time of the onsite.<br>• Measures to deal with the non-extradition of nationals are not fully in line with what is required under c.39.2. |
| 40. Other forms of international co-operation | LC | • There is a lack of provisions with regard to the timeliness of responses.<br>• The is a lack of specific provisions for information to be exchanged related to DNFBPs.<br>• The CBB does not have the authority to spontaneously exchange information. |

# Glossary of Acronyms[8]

| | |
|---|---|
| BHD | Bahraini Dinar |
| CBB | Central Bank of Bahrain |
| CCL | Commercial Companies Law |
| CID | The General Directorate for Criminal Investigations |
| CPC | Criminal Procedure Code |
| FC | Financial Crime |
| FI | Financial institution |
| FID | Financial Investigation Division |
| FTFs | Foreign Terrorist Fighters |
| GCC | Gulf Co-operation Council |
| JCTC | Joint Counter Terrorism Centre |
| LEAs | Law Enforcement Authorities |
| MLA | Mutual Legal Assistance |
| MLRO | Money Laundering Reporting Officer |
| MOFA | Ministry of Foreign Affairs |
| MOICT | Ministry of Industry Commerce and Tourism |
| MOI | Ministry of Interior |
| MOJ | Ministry of Justice |
| NPC | National Policy Committee |
| NRA | National Money Laundering and Terrorist Financing Risk Assessment |
| NSA | National Security Agency |
| PPO | Public Prosecutions Office |
| RERA | Real Estate Regulatory Authority |
| SLRB | Survey and Land Registration Bureau |
| UNSCRs | United Nations Security Council Resolutions |

8 Acronyms already defined in the FATF 40 Recommendations are not included in this Glossary.

www.fatf-gafi.org | www.menafatf.org

September 2018

# Anti-money laundering and counter-terrorist financing measures - Kingdom of Bahrain

## *Fourth Round Mutual Evaluation Report*

In this report: a summary of the anti-money laundering (AML) / counter-terrorist financing (CTF) measures in place in Bahrain as at the time of the on-site visit on 7-22 November 2017.

The report analyses the level of effectiveness of Bahrain'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.