



Anti-money laundering
and counter-terrorist
financing measures

Philippines

Mutual Evaluation Report

October 2019





The Asia/Pacific Group on Money Laundering (APG) is an inter-governmental organisation consisting of 41 members in the Asia-Pacific region, as well as organisations, and observers from outside the region.

Under Article 1 of the APG Terms of Reference 2012, the APG is a non-political, technical body, whose members are committed to the effective implementation and enforcement of the internationally accepted standards against money laundering, financing of terrorism and proliferation financing set by the Financial Action Task Force.

This document, any expression herein, 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.

Under the APG Terms of Reference, membership in the APG is open to jurisdictions which have a presence in the Asia-Pacific region.

For more information about the APG, please visit the website: www.apgml.org.

This mutual evaluation report was adopted by the APG at its annual meeting in August 2019.

Citing reference:

APG (2019), *Anti-money laundering and counter-terrorist financing measures - Philippines*, Third Round Mutual Evaluation Report, APG, Sydney
<http://www.apgml.org/includes/handlers/get-document.ashx?d=c0fe3714-bfcf-475e-8ff3-47e9c3cfe496>

© October 2019 APG

No reproduction or translation of this publication may be made without prior written permission. Applications for permission to reproduce all or part of this publication should be made to:

APG Secretariat
Locked Bag A3000
Sydney South
New South Wales 1232
AUSTRALIA
Tel: +61 2 5126 9110

E mail: mail@apgml.org
Web: www.apgml.org

Cover image: No copyright – Image provided by the Anti-Money Laundering Council, Philippines

TABLE OF CONTENTS

EXECUTIVE SUMMARY	5
Key Findings.....	5
Risks and General Situation.....	7
Overall Level of Effectiveness and Technical Compliance	8
Priority Actions	15
Effectiveness & Technical Compliance Ratings	17
MUTUAL EVALUATION REPORT OF THE PHILIPPINES	18
Preface.....	18
CHAPTER 1. ML/TF RISKS AND CONTEXT	20
ML/TF Risks and Scoping of Higher-Risk Issues	20
Materiality	24
Structural Elements	26
Background and other Contextual Factors	27
CHAPTER 2. NATIONAL AML/CFT POLICIES AND COORDINATION	38
Key Findings and Recommended Actions	38
Immediate Outcome 1 (Risk, Policy and Coordination).....	40
CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES	50
Key Findings and Recommended Actions	50
Immediate Outcome 6 (Financial intelligence ML/TF).....	54
Immediate Outcome 7 (ML investigation and prosecution).....	66
Immediate Outcome 8 (Confiscation).....	75
CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION.....	84
Key Findings and Recommended Actions.....	84
Immediate Outcome 9 (TF investigation and prosecution)	87
Immediate Outcome 10 (TF preventive measures and financial sanctions)	93
Immediate Outcome 11 (PF financial sanctions).....	101
CHAPTER 5. PREVENTIVE MEASURES	103
Key Findings and Recommended Actions.....	103
Immediate Outcome 4 (Preventive Measures).....	105
CHAPTER 6. SUPERVISION	122
Key Findings and Recommended Actions.....	122
Immediate Outcome 3 (Supervision).....	124
CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS.....	137
Key Findings and Recommended Actions.....	137
Immediate Outcome 5 (Legal Persons and Arrangements)	138
CHAPTER 8. INTERNATIONAL COOPERATION	144
Key Findings and Recommended Actions.....	144
Immediate Outcome 2 (International Cooperation).....	145
TECHNICAL COMPLIANCE ANNEX	155
Recommendation 1 - Assessing Risks and applying a Risk-Based Approach	155
Recommendation 2 - National Cooperation and Coordination.....	157
Recommendation 3 - Money laundering offence	159

Recommendation 4 – Confiscation and provisional measures	162
Recommendation 5 – Terrorist financing offence	165
Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing.....	167
Recommendation 7 – Targeted financial sanctions related to proliferation	171
Recommendation 8 – Non-profit organisations	172
Recommendation 9 – Financial institution secrecy laws.....	176
Recommendation 10 – Customer due diligence	178
Recommendation 11 – Record-keeping.....	184
Recommendation 12 – Politically exposed persons.....	185
Recommendation 13 – Correspondent banking.....	186
Recommendation 14 – Money or value transfer services	187
Recommendation 15 – New technologies	188
Recommendation 16 – Wire transfers	189
Recommendation 17 – Reliance on third parties	192
Recommendation 18 – Internal controls and foreign branches and subsidiaries	192
Recommendation 19 – Higher-risk countries	193
Recommendation 20 – Reporting of suspicious transaction.....	194
Recommendation 21 – Tipping-off and confidentiality.....	195
Recommendation 22 – DNFBPs: Customer due diligence.....	195
Recommendation 23 – DNFBPs: Other measures.....	198
Recommendation 24 – Transparency and beneficial ownership of legal persons	200
Recommendation 25 – Transparency and beneficial ownership of legal arrangements.....	205
Recommendation 26 – Regulation and supervision of financial institutions.....	208
Recommendation 27 – Powers of supervisors	213
Recommendation 28 – Regulation and supervision of DNFBPs.....	215
Recommendation 29 - Financial intelligence units.....	218
Recommendation 30 – Responsibilities of law enforcement and investigative authorities.....	221
Recommendation 31 – Powers of law enforcement and investigative authorities	222
Recommendation 32 – Cash Couriers	225
Recommendation 33 – Statistics.....	227
Recommendation 34 – Guidance and feedback.....	228
Recommendation 35 – Sanctions.....	228
Recommendation 36 – International instruments	231
Recommendation 37 - Mutual legal assistance.....	231
Recommendation 38 – Mutual legal assistance: freezing and confiscation.....	234
Recommendation 39 – Extradition	235
Recommendation 40 – Other forms of international cooperation.....	236
SUMMARY OF TECHNICAL COMPLIANCE – KEY DEFICIENCIES	243
GLOSSARY OF TERMS	248

EXECUTIVE SUMMARY

1. This report provides a summary of the anti-money laundering and countering the financing of terrorism (AML/CFT) measures in place in the Philippines as at the date of the on-site visit in November 2018. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Philippines' AML/CFT system, and provides recommendations on how the system could be strengthened.

Key Findings

- 1) The Philippines has reasonably assessed a range of its money laundering (ML) and terrorist financing (TF) risks. While the National Risk Assessments (NRAs) did not sufficiently take into account the threat posed by the presence and movement of foreign terrorist fighters, following the Marawi siege, the understanding of TF risk, including foreign terrorist fighters, has been updated and supplemented by tactical analysis and regional TF assessments.
- 2) The understanding of ML and TF risk among stakeholders varies, but is strongest with the Anti-Money Laundering Council (AMLC), which is the primary law enforcement agency (LEA) responsible for ML/TF investigations. There are weaknesses with assessments and understanding of transnational aspects of ML and TF risks.
- 3) In late 2018, the Philippines adopted the National AML/CFT Strategy (NACS) and recently established the National AML/CFT Coordination Committee (NACC), which operates in addition to pre-existing operational coordination committees. The objectives set for supervisory and regulatory authorities respond to identified risks, however this was not apparent for LEAs, with the exception of drugs and corruption. The action plans under the NACS were at various stages of implementation at the time of the on-site visit.
- 4) AMLC, the Philippines FIU, underwent a restructure in June 2018 and is now better structured to perform its functions as a hybrid FIU/investigation/asset recovery agency. AMLC's financial investigation sections were critically under-staffed at the time of the on-site visit. AMLC's Financial Intelligence Analysis Group (FIAG) produces financial intelligence which is primarily used by the AMLC Financial Crimes Investigation Group (FCIG) and, to a limited extent, by other LEAs. The use of financial intelligence does not frequently translate into investigations into ML, TF or predicate offences.
- 5) AMLC is the primary agency in the Philippines with direct access to bank records, which are protected under the bank secrecy legislation, for use in analysis, investigation and supervision. BSP can access bank information to check compliance with AMLA and the OMB can access bank

information under certain conditions. While AMLC is able to assist to overcome challenges in many situations, in some instances banking secrecy legislation effects the ability of other competent authorities to access information to properly perform their AML/CFT functions as it impacts the timeliness of information exchange and the overall effective use of financial intelligence by LEAs.

- 6) AMLC is the only designated authority to investigate ML offences, but only had 18 officers in the FCIG to cover the function at the time of the on-site visit. While the Philippine National Police (PNP) and the National Bureau of Investigation (NBI) have general investigation powers, they are not designated to investigate ML. Given AMLC's sole responsibility for ML investigations, it is critically understaffed.
- 7) Between 2013 and 2018 FCIG conducted 277 financial investigations resulting in 20 petitions for ML, which resulted in 10 ML prosecutions and five convictions. This is not consistent with the ML risk profile in the Philippines.
- 8) AMLC is the main agency which has the responsibility to confiscate criminal proceeds through civil forfeiture actions and has demonstrated a focus in depriving criminals of the proceeds of crime. Between 2013 and 2018 AMLC completed eight civil forfeitures, with 41 civil forfeiture actions pending. The confiscations undertaken have mostly related to proceeds located in the Philippines. There is limited demonstration of authorities pursuing the confiscation of assets sent offshore and the proceeds of foreign predicate crimes, but there have been recent increases in pursuing property of equivalent value and instruments of crime.
- 9) Despite the Philippines TF risk profile, in the six and a half years since the introduction of the standalone TF offence, the Philippines has not conducted any TF prosecutions. Competent authorities focus on pursuing predicate offences associated with the fundraising of terrorism rather than TF and so seek to disrupt financing activity through arrests and convictions for predicate offences.
- 10) There are deficiencies in the framework for targeted financial sanctions (TFS) relating to TF which have significantly impacted its use, including the inability to operate *ex parte* and to designate an individual pursuant to UNSCR 1373. There has been a lack of designations under UNSCR 1373 and proposals for designation under UNSCR 1267, and a low number of freezes of assets and instrumentalities, which is not in line with the high risk of TF in the Philippines, including the known exposure to sanctioned entities.
- 11) The Philippines has a large and diverse non-profit organisation (NPO) sector, which was recently subject to an assessment to identify the features and types of NPOs likely to be at risk of TF abuse. There are still considerable knowledge gaps regarding the composition of the NPO sector. Targeted risk-based supervision and monitoring of those NPOs most at-risk of TF abuse has not fully commenced.
- 12) The Philippines does not have a framework for the implementation of TFS related to proliferation of weapons of mass destruction (WMD).
- 13) Risk-based supervision is broadly applied by Bangko Sentral Pilipinas (BSP) to banks and money services businesses (MSBs), however the Securities and Exchange Commission (SEC), Insurance Commission (IC) and Philippine Amusement Gaming Corporation (PAGCOR) have

only recently commenced risk-based supervision. With the exception of one onsite examination of a casino in conjunction with PAGCOR, AMLC has not commenced its supervision of DNFBPs.

- 14) Most supervisors have a reasonable understanding of ML/TF risks, but do not receive sufficient up-to-date risk information to best support their risk-based approaches.
- 15) The adequacy of market entry procedures differ across sectors, with gaps in the framework of supervisors other than BSP, including a lack of identification of beneficial ownership.
- 16) The legal framework for preventive measures is generally sound, with some deficiencies, mostly in relation to DNFBPs. Implementation across sectors is mixed, and is strongest in the banking sector. The requirements for DNFBPs to comply with AML/CFT obligations are currently being implemented. Real estate agents are not covered persons under the AMLA.
- 17) There is varied, but generally weak, understanding across the public and private sectors of the concept of beneficial ownership and how the beneficial owner can be identified.
- 18) The primary measures to prevent the misuse of legal persons and arrangement are the public access to basic ownership information; and information collected through CDD; regulation and supervision of authorised trustee entities by the BSP; and measures to prevent the misuse of bearer shares. Transparency is weak in relation to parties to private trusts formed under Philippines law or foreign trusts operating in the Philippines. Banking secrecy impacts competent authorities' ability to directly access CDD information held by banks which may be required to identify beneficial ownership of legal persons in a timely manner. BSP is only able to share bank information with the prior approval of the Monetary Board. Competent authorities must request this information from AMLC.
- 19) The Philippines has a reasonable legal framework for seeking and responding to mutual legal assistance (MLA) and extradition, however the use of outgoing requests for MLA and extradition is low considering the risk profile. LEAs preference informal international cooperation rather than MLA and extradition mechanisms due to the delays associated with formal mechanisms. There are often significant with respect to the Philippines providing MLA, although AMLC has taken a number of steps to seek to improve this situation.
- 20) Authorities, in particular the AMLC, use a wide range of mechanisms to support informal cooperation with foreign counterparts, including regular bilateral or multi-jurisdictional operation meetings, international organisations and officer level contacts. Counterparts reported that the cooperation provided by the Philippines is usually constructive.

Risks and General Situation

2. The Philippines is a constitutional republic and one of the fastest-growing economies in South East Asia. As an archipelago, it comprises of over 7,000 islands with a large and young population of 104.9 million, 11% of which live or work abroad.

3. The Philippines is exposed to significant terrorism and TF risks with mature support networks that sustain terrorist groups. These fund a range of activities including recruitment of domestic and foreign fighters, procurement of weapons, and training, particularly in the southern regions of the

Philippines. The severe impact of these risks was demonstrated by the 2017 Battle of Marawi and the ongoing state of martial law in Mindanao.

4. Additionally, a range of offences generate significant illicit proceeds. These include corruption and organised crime. The 2017 NRA highlighted that 20% of the annual budget was assessed by authorities to be lost due to corruption. Organised crime groups operate a robust shadow economy, laundering the proceeds of drug and human trafficking, tax crimes and cyber-crime. ISIS-affiliated groups are also reliant on these predicate offences and others such as kidnapping to raise funds and facilitate operations.

5. These significant threats exploit vulnerabilities including a cash and remittance-based economy, under-resourced authorities, and legislative and procedural hurdles which impede efforts to prevent, investigate and prosecute ML/TF. The banking, MSB and gaming sectors are material and at-risk for the transfer of illicit proceeds in and out of the country.

Overall Level of Effectiveness and Technical Compliance

6. The Philippines has made significant improvements in its technical compliance since its mutual evaluation in 2009. The coverage of predicate offences is now comprehensive, with the sole exception of tax crimes. Progress has also been made through the coverage of preventive measures and the inclusion of DNFBPs in the AML/CFT framework, in particular the notable addition of casinos. The introduction of the Terrorism Financing Suppression and Prevention Law, and a standalone TF offence, has contributed to the level of compliance in the Philippines with FATF standards as revised.

7. However, certain challenges noted in the previous MER remain, in particularly in relation to the timeliness of competent authorities (other than AMLC) accessing records held by banking institutions that are protected under bank secrecy legislation. It is also apparent under the 2013 Methodology that authorities are not effectively targeting ML or TF through financial investigations. While most supervisors (BSP, AMLC, PAGCOR) display an understanding of ML/TF risks within FIs and DNFBPs, the implementation of risk based supervision is mixed across supervisors and only recently implemented in most sectors.

8. The 2018 adoption of a national strategy address several outstanding challenges and is likely to contribute to better coordination and effectiveness in the Philippines AML/CFT efforts.

Assessment of Risks, coordination and policy setting (Chapter 2 - IO.1; R.1, R.2, R.33)

9. The Philippines has a reasonable understanding of its ML/TF risks, with some gaps, as reflected in various iterations of NRAs and Serious and Organized Crimes Threat Assessments (SOCTAs) and shared across government departments, LEAs, and regulatory agencies. The assessment of risks with respect to terrorism and TF in relation to FTF was not assessed in the NRA. However, the understanding of TF risk, including foreign terrorist fighters, is updated and supplemented by tactical analysis conducted on the Maute Group and regional TF assessments on ISIL funding.

10. Responses to identified risks vary across the competent authorities. The NACC operates in parallel with pre-existing operational coordination committees, such as the NALECC sub-committee on AML/CFT and other mechanisms responsible for predicate offences. Nonetheless, NACC has the potential to establish better coordinated responses, but this was not demonstrated at the time of the onsite. There was limited demonstration of cooperation and coordination on PF through the NALECC's respective sub-committees.

11. Objectives set for AMLC and supervisory and regulatory authorities by the action plans under the NACS correspond to key risks. However, the same is not apparent for LEAs. The action plans under the NACS were at various stages of implementation at the time of the onsite visit. Certain enhanced and simplified measures for relevant sectors have been instituted based on the risks identified in various assessments.

12. Private sector stakeholders appear to be aware of the results of the risk assessments undertaken under the NRAs. However, the understanding and response appears most developed amongst larger banks, less developed amongst other FIs and the casinos, and quite low amongst other categories of DNFBPs.

Financial Intelligence, Money Laundering and Confiscation (Chapter 3 - IOs 6-8; R.3, R.4, R.29-32)

Use of Financial Intelligence (Immediate Outcome 6)

13. AMLC is a hybrid FIU, with other responsibilities including financial investigations (ML, TF and asset tracing), civil forfeiture litigation and AML/CFT supervision of DNFBPs. AMLC's Financial Intelligence Analysis Group (FIAG) produces financial intelligence products, which are primarily used by the AMLC's Financial Crime Investigation Group (FCIG). Requests by LEAs to FIAG and spontaneous dissemination of financial intelligence to other LEAs to support predicate crime investigations are limited and not in keeping with the ML/TF risks.

14. AMLC has received a very large number of suspicious transaction reports (STRs) and covered transaction reports (CTRs) from FIs and a small number from DNFBPs. A review conducted by AMLC in 2017 identified that 53% of STRs received in 2016 were of high quality. AMLC has focused on supporting improvements to the quality of STRs received through detailed guidelines and enhanced engagement with various sectors. AMLC has received a very low number of CTRs from casinos and a low number of cross-border currency declarations, which is not in line with the risk profile.

15. AMLC has access to a wide range of information to support its analysis. There are ongoing efforts to improve AMLC's analytical capability, in order to better support operational needs, but the FIU part of AMLC was critically under staffed at the time of the onsite visit.

16. There are no barriers to disseminate information from FIAG to the AMLC's investigation wing, the FCIG, and this has been the main destination of intelligence products by the FIU. AMLC cannot disseminate information on PEPs outside AMLC during election periods. This raises concerns about AMLC's operational independence and affects the timeliness of PEP information exchanged and the overall effectiveness of the use of information by LEAs.

17. AMLC has very rarely proactively disseminated financial intelligence to other LEAs for possible ML, TF or predicate crime investigations. Other LEAs do not regularly seek financial intelligence from AMLC in support of their financial investigations.

18. Beyond AMLC's FCIG, other LEAs do not regularly develop or make use of financial intelligence in their investigations of ML, TF, predicate offences or proceeds of crime. As the primary agency able to access bank records, AMLC's FCIG more regularly shares bank records and other information with other LEAs in support of their predicate investigations, but this is not at a level which suggests those LEAs regularly follow money trails.

19. While there have been some successful instances, disseminated AMLC products have not consistently supported effective outcomes for investigating ML, TF or predicate offences. Feedback

from LEAs on AMLC's finished financial intelligence indicates that 50% of reports received contain information already known to LEAs. This gap has been recognised by AMLC, and prompted efforts to enhance its products.

ML Investigations (Immediate Outcome 7)

20. AMLC is the primary designated authority to investigate ML offences, but the power to investigate ML is also available to PNP and NBI. AMLC FCIG is the only LEA authorised to directly access bank records as part of an investigation and they are able to pass on such information to other LEAs in the context of criminal investigations. While FCIG demonstrated good skills and experience with ML investigations, the number of investigators is low and the agency lacks some of the powers of an LEA to collect evidence and seize property, which detracts from effectiveness.

21. Overall, the number of investigations and prosecutions for ML is low and is inconsistent with the Philippines' risk profile. During the review period only 20 ML investigations were completed, with 10 ML prosecutions and five convictions.

22. The Philippines has demonstrated an ability to prosecute third-party ML and stand-alone ML. However, there is a lack of pursuit of ML involving foreign predicate offences or through legal persons. The external threat assessment in the 2017 NRA concluded that the threat from proceeds of crime committed outside the Philippines is high, yet only a single case relating to foreign predicate offences was prosecuted. The authorities do not regularly pursue international cooperation in relation to ML investigations and prosecutions.

23. There are substantial delays in the Philippines courts, which can take up to five years to reach a first conviction. Nonetheless, in the very limited number of ML cases where convictions were secured and sanctions applied, these were effective, proportionate and dissuasive.

Confiscation (Immediate Outcome 8)

24. There is a policy objective to confiscate criminal proceeds, instrumentalities and property of equivalent value in ML/TF crimes, prioritised on identified high-risk crimes. This is chiefly pursued through civil forfeiture actions. Authorities did not demonstrate that they make use of the conviction-based forfeiture available to them.

25. Authorities have taken initial steps to deprive criminals of their proceeds through the use of provisional measures pursuant to possible civil forfeiture, with a particular focus on drugs, fraud, corruption, cybercrime and human trafficking. There are 41 pending civil forfeiture claims which have an intended value of over USD 117 million. However, despite increased civil forfeiture activity, only eight matters resulted in confiscation in the review period and the overall amount is low (approx. USD 15,500,000) with over 95% obtained in a single matter. This is not proportionate to the scale of the risk of proceeds of crime in the economy. Most cases involved the confiscation of proceeds located in the Philippines. Authorities rarely seek to confiscate assets moved offshore or take action against the proceeds of foreign predicate crimes located in the Philippines.

26. Cases relating to the confiscation of instruments of crime and property of equivalent value were pursued to a limited extent but were increasing in the two years prior to this report. LEAs (other than AMLC) have limited their actions of seizures, mostly for evidentiary purposes.

27. In the context of high risks associated with TF, there has only been one TF-related civil forfeiture action, which remains pending.

28. Confiscation cases relating to cross-border movements of currency and bearer negotiable instruments (BNIs) were low, despite the Philippines' high risks of cash smuggling. Low detection levels, underpinned by limited coverage of sea/airport entry/exit points and the staffing shortages, may be a contributing factor. Competent authorities are not adequately empowered to restrain currency and BNIs suspected of ML/TF or other predicate offences.

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

TF Offence (Immediate Outcome 9)

29. The level of TF investigative activity is inconsistent with the Philippines' high TF risk profile, which includes mature support networks. From 2014 to 2017, there were only 18 TF investigations. There have been no prosecutions or convictions for despite almost 1,000 terrorist incidents occurring in the Philippines during the period under review.

30. It is not clear that LEAs actively consider TF in all terrorism investigations. In practice, agencies charge suspects for predicate crimes with clearer legal requirements and similar available sanctions – for example kidnap for ransom.

31. The TF offence is punishable by up to 40 years imprisonment and fines, however, the sanctions for legal persons are insufficient. Further, the offence does not comprehensively cover the financing of travel for the purpose of providing, or receiving, terrorist training.

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

32. While the Philippines has a TFS framework for terrorism, there are deficiencies in the implementation of TFS as part of the overall prevention of TF. Implementation of TFS by FIs/DNFBPs is not strong and has not resulted in successful asset freezing or denial of funds in keeping with the Philippines' risk profile. Further, the requirement to freeze may not take effect without delay.

33. The Philippines has made limited use of designations pursuant to UNSCRs. Authorities have only used its UNSCR 1373 designation system to dual-list the Abu Sayyaf Group, which is designated by the UN under UNSCR 1267. The Philippines' UNSCR 1373 designation process cannot operate *ex parte* and requires a criminal case to be filed. This has impeded ongoing designation efforts. Generally, only organisations, associations and groups can be designated pursuant to UNSCR 1373. An individual can only be designated if their funds or property are subject to seizure and sequestration under the Human Security Act. Requests from other jurisdictions to designate pursuant to UNSCR 1373 have not led to designations in the Philippines.

34. The Philippines 2018 assessment of the NPO sector rated NPOs as low-medium for risk of TF abuse. The assessment team finds that there are knowledge gaps regarding the NPO sector. The number of unregistered NPOs is unknown and of 101,843 NPOs that are registered with the authorities, 52% have no clear classification. There have been 32 NPOs in the Philippines potentially involved in TF activity. While some outreach to the NPO sector has been undertaken, targeted risk-based supervision or monitoring of those NPOs most at risk of TF abuse has not fully commenced.

Proliferation financing (Immediate Outcome 11)

35. The Philippines lacks a domestic legal and institutional framework for implementing TFS related to proliferation of WMD. Consequently, there are no mechanisms to implement TFS without delay, disseminate relevant UN list updates, freeze/unfreeze assets, or control access to funds. Promisingly, a lead agency has been established for the implementation of TFS related to PF. Private sector entities have indicated they would report any name matches via an STR, however, no such STRs have been submitted.

36. The Philippines authorities indicated some awareness of potential exposure to PF-related sanctions evasion faced and UN obligations to take action. Authorities took a series of actions to impound a DPRK cargo ship subject to UN sanctions. BSP has issued circulars instructing BSP supervised entities to monitor individuals and entities referenced under UNSCR 2321 and 1929.

Preventive Measures (Chapter 5 - IO4; R.9-23)

37. The Philippines' banking and NBFIs sectors have a generally sound understanding of their ML/TF risks and AML/CFT obligations and are implementing preventative AML/CFT measures to a reasonable extent. Banks apply a risk-based approach to CDD, including frequency of reviews and account monitoring. However, challenges remain in fulfilling some CDD obligations, particularly understanding the customer's business activity and source of funds, verifying beneficial owners and establishing ultimate beneficial ownership. Banks, in conjunction with BSP, have taken a cautious approach to the use of new or developing technologies.

38. MSBs have undergone an extensive re-registration process which has resulted in a significant restructure, and consolidation, of the sector. The level of understanding of ML/TF risks and AML/CFT obligations is developing and the newly structured MSB framework provides a strong framework for AML/CFT compliance in the future. There are challenges relating to unregistered MSBs. For SEC and IC supervised FIs, there are variances in the levels of AML/CFT measures in place. This is partly due to the lack of AML/CFT specific supervision for these FIs until recently.

39. TFS screening is a particular concern for bank and non-bank FIs. The lack of false positive freezing actions is a further indicator of deficient TFS implementation.

40. Overall, the level of understanding by DNFBP sectors of their ML/TF risks and the implementation of AML/CFT measures is in its early stages. Large or internationally affiliated DNFBPs, particularly integrated resort casinos, are making progress towards implementing required AML/CFT measures. However, other DNFBPs have yet to commence implementation. Real estate agents are excluded from AMLA and are not subject to AML/CFT obligations.

41. The Philippines' STR reporting regime is developing. There are patterns of defensive reporting and the quantity of STR filed for terrorism, TF and kidnapping-for-ransom is not proportionate to the national risks. AMLC, BSP, SEC and IC are taking steps to address deficiencies and the quality of STRs is assessed to be improving. DNFBPs have only been required to file STRs since 2018. There is no requirement for STRs related to tax offences, as it is not a predicate offence.

42. There are inconsistencies in the AMLA, its Implementing Rules and Regulations (IRRs) and guidance relating to the extent to which DNFBPs are captured as covered persons. This is particularly important in the casino sector, where it is unclear whether AML/CFT requirements only apply to 'cash' transactions, or whether all types of financial transactions in casinos are caught by AMLA.

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

43. Most supervisors have a reasonable understanding of the ML/TF risks posed by their regulated sectors. The NRA process contributed significantly to supervisors' understanding of ML/TF risk, however the lack of timely and adequate information inputs from the FIU and LEAs on risks impacts understanding of sectoral and cross sector risks, especially for supervisors in higher risk sectors.

44. The adequacy of market entry fit and proper controls differ across sectors. BSP has prevented criminal influence to a large extent, notably for banks. Sufficient fit and proper measures are not consistent among other supervisors and there is a gap with identifying and checking fitness and propriety beneficial owners of an FI. BSP's restructure of the MSB sector has strengthened market entry requirements and risk-based supervision of the sector, however there are shortcomings in the identification of, and application of sanctions for, illegal MSB operations.

45. BSP has a prudent risk-based supervisory framework for banks, however thematic reviews have only recently commenced and they are not used effectively. Other supervisors' risk-based approaches are in an early stage of implementation and effectiveness has not been demonstrated. Gaps exist in PAGCOR's supervisory approach due to deficiencies in the coverage of all financial transactions and also in third-party reliance. Further, it is not clear that PAGCOR includes casino agents (including junket operators) in the scope of its examinations. There is a conflict of interest in PAGCOR's role as supervisor and market participant, given its ownership of local-branded casinos. There are scope gaps in the coverage of some financing and lending companies and real estate.

46. Remedial actions and sanctions applied by BSP on larger banks (universal/commercial banks and thrift banks) and MSBs have been proportionate and dissuasive. Improvement is required for AMLC in prioritising deficiencies identified by other supervisors for administrative sanctions. Other supervisors have applied limited, or no, sanctions and demonstrate only minimal impact on the compliance of their covered persons.

47. Supervisors have provided varying levels of outreach to covered persons, Deficiencies remain in relation to the understanding of obligations in some DNFBP sectors.

Transparency of Legal Persons and Arrangements (Chapter 7 - IO5; R. 24-25)

48. Basic information on the creation and types of legal persons and arrangements is publicly available and some documents submitted by legal persons (e.g. the General Information Sheet (GIS)) are able to be either accessed by the public or requested.

49. The Philippines' primary measures for preventing misuse of legal persons and arrangements for ML/TF include access to basic information, as well as CDD documents; regulation and supervision of authorised trustee entities by BSP; and measures which partially address misuse of bearer shares through mandatory recording of share transfers.

50. Trustees to private trusts (including charitable trusts or foreign trusts not formed by trust entities) are not subject to transparency obligations, and are not regulated and supervised. However CDD conducted by an FI or DNFBP on those trustees when they are a customer would capture beneficial ownership and control information and would be available to competent authorities. Requirements are in place for identification parties to a trust that have authorisation as 'trustee entities', but these entities

are governed by contract and while they are regulated for AML/CFT, they are not express trusts in keeping with R.25.

51. Sanctions for non-compliance with mandatory corporate filing are not considered proportionate or dissuasive, with minor fines imposed for the first five years of non-compliance.

52. A broad understanding of the risks associated with legal persons was not demonstrated. Bank supervisors acknowledged unaddressed ML/TF risks including the widespread use of nominee shareholders. There are deficiencies with preventative measures relating to bearer share warrants.

53. Comprehensive and timely information on basic and beneficial ownership of legal persons is difficult for competent authorities to access in a timely manner. Banking secrecy laws prevent any competent authority with the exception of AMLC (and BSP for the purpose of checking AML/CFT compliance) from obtaining CDD information directly from banks. Although aware of SEC's online database, competent authorities advised they only use it to confirm if a company is registered. They prefer to obtain information through a formal request to the SEC or via subpoena, as documents obtained through the online database have no evidentiary value in a future prosecution. Information on cooperatives is available to competent authorities, with access requiring a freedom of information request.

54. Information on parties to a private trust may be obtained via CDD information collected from FI/DNFBPs, if the party to a trust has a relationship with an FI/DNFBP.

55. There appears to be confusion among parts of the private sector and competent authorities on the scope of beneficial ownership and how it was determined. Limited instances were demonstrated where competent authorities have sought access to beneficial ownership information on either a legal person or legal arrangement.

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

56. The Philippines has a reasonable framework for international cooperation for both MLA and extradition. MLA is available through mutual legal assistance treaties (MLATs), under various international conventions or diplomatically through the principle of reciprocity.

57. The number of outgoing requests for MLA and extradition is very low in comparison to the Philippines' risk profile given that significant threats identified in the 2017 NRA are largely transnational in nature. The timeliness of the Philippines' response to MLA requests was raised as a concern in some instances, however the assistance when provided is of reasonable or good quality.

58. The Philippines is able to execute extradition, requests however there is no guarantee of execution without undue delay. Foreign counterparts reported significant delays in the extradition process mainly due to the role of the Philippines' courts in deciding on petitions. In the period 2013 to 2017, the Philippines received 23 requests for extradition and of these, only four requests were completed. Most Philippines' treaties allow the refusal of an extradition request on the basis of nationality, and only some treaties contain a provision that codifies the principle that where extradition is refused, the person must be prosecuted. There is no simplified process in place for managing extradition requests.

59. Outgoing extradition requests are notably low and inconsistent with the Philippines' ML and TF risk profile. In the period 2013 to 2018, the Philippines made a total of five extradition requests, none of which related to ML/TF cases.

60. Competent authorities demonstrated a mixed level of agency to agency cooperation. AMLC and BSP are the most active in their international cooperation, but the scope and intensity of international cooperation is not in keeping with the risk profile. Other LEA and regulatory agencies demonstrated less international cooperation when considering the Philippines ML/TF risk profile.

61. The SEC I-View database allows foreign jurisdictions to access basic information on legal persons operating in the Philippines, although it was not demonstrated that this database was being utilised. There have been limited instances of exchange of beneficial ownership information with international counterparts.

Priority Actions

62. The Philippines should take the following priority actions:

- a) Improve the operation of mechanisms that ensure relevant government agencies may examine bank accounts for a legitimate purpose, and in the exercise of their investigative or supervisory powers, with appropriate integrity controls.
- b) Continue to update assessments of TF risks to enhance understanding of emerging typologies of TF in the Philippines, noting the significant recent events, the role of foreign fighters and impact of Philippines' governmental / military responses to TF networks and changes in the threat environment.
- c) Greatly enhance the development and use of financial intelligence to support financial investigations related to predicate offences, ML and TF by the widest range of LEAs.
- d) Establish a comprehensive legal framework for implementing UNSCR 1373 ex parte and actively consider using the framework as a tool to combat TF risks in the Philippines.
- e) Continue to implement and monitor the implementation of the action plans under the National AML/CFT Strategy, including operationalisation of the newly established NACC and its sub-committees to ensure their effectiveness.
- f) Greatly enhance the use of mechanisms for regular and targeted sharing of risk information from LEAs, security intelligence agencies and AMLC with regulators and supervisors to support their risk-based supervision and regulation.
- g) Implement, or enhance, an effective risk-based approach to supervision across all sectors, including the conduct of off-site and thematic reviews to best utilise resources. Apply sanctions for non-compliance where warranted.
- h) Enhance the identification, investigation and prosecution, of ML arising out of predicate crime investigations and financial intelligence in keeping with the risk profile. Pursue ML arising out of foreign predicate crimes.
- i) Enhance the identification, investigation and prosecution, of TF in keeping with the risk profile. This should include targeting stand-alone TF and investigating terror networks and financing flows. Increase the numbers of dedicated TF investigators and enhance TF investigation and prosecution capacity amongst competent authorities.
- j) Enhance the capability of LEAs to identify and investigate transnational elements of cases with the cooperation of relevant counterparts, including by actively seeking MLA and extradition in

their ML and predicate offences investigations, in accordance with and going beyond the national strategy.

- k) Continue programmes to improve FIs/DNFBPs understanding and implementation of TFS obligations to identify and freeze terrorist assets. This should include information sharing on specific risks for sanctions in the Philippines context.
- l) Pursue assets tracing, restraint and confiscation actions on high risk predicate crimes, foreign predicate crimes and proceeds moved to other jurisdictions. Enhance focus on confiscations of instrumentalities of crime and property of equivalent value.
- m) Continue efforts to identify illegal remittance operations and apply proportionate and dissuasive sanctions.
- n) Implement a legal framework to implement TFS on PF without delay and develop regulatory and operational mechanisms for implementing, monitoring compliance and applying sanctions for breaches.
- o) Ensure effective risk mitigation and risk-based supervision of the casino sector, including casino agents (junket operators). As part of this, resolve PAGCORs conflict of interest in its role as casino operator and AML/CFT supervisor.
- p) Following the release of the Guideline on Beneficial Ownership, the Philippines should conduct outreach to competent authorities, FIs and other covered persons on beneficial owner requirements, risks of misuse of legal persons and arrangements and opportunities for competent authorities to access beneficial ownership information.
- q) Regulators, supervisors, AMLC and other authorities should continue to deliver programs to support FI/DNFBPs to improve their understanding of ML/TF risk and their implementation of their AML/CFT obligations.

Effectiveness & Technical Compliance Ratings

Effectiveness Ratings

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

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

R.1 - Assessing risk & applying risk-based approach	R.2 - National cooperation and coordination	R.3 - Money laundering offence	R.4 - Confiscation & provisional measures	R.5 - Terrorist financing offence	R.6 - Targeted financial sanctions – terrorism & terrorist financing
LC	C	LC	PC	LC	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
NC	LC	LC	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
C	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	PC	C	PC	PC	PC
R.25 - Transparency & BO of legal arrangements	R.26 - Regulation and supervision of financial institutions	R.27 - Powers of supervision	R.28 - Regulation and supervision of DNFBPs	R.29 - Financial intelligence units	R.30 - Responsibilities of law enforcement and investigative authorities
PC	LC	LC	PC	PC	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
LC	PC	LC	LC	LC	LC
R.37 - Mutual legal assistance	R.38 - Mutual legal assistance: freezing and confiscation	R.39 - Extradition	R.40 - Other forms of international cooperation		
LC	C	PC	LC		

MUTUAL EVALUATION REPORT OF THE PHILIPPINES

Preface

This report summarises the AML/CFT measures in place in the Philippines 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 Philippines's 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 Philippines, and information obtained by the assessment team during its onsite visit to the Philippines from 15 to 28 November 2018.

The evaluation was conducted by an assessment team consisting of:

- Mr Young-min Lee, Korea, legal expert
- Mr Hari Nepal, Nepal, legal expert
- Ms Sarah Donald, Australia, legal expert
- Ms Annie Chau, Macao, China, financial expert
- Mr Robert Milnes, New Zealand, financial expert
- Dr Sarah Azlina Che Rohim, Malaysia, FIU expert
- Ms Nantha Phommavongsa, Lao PDR, FIU expert
- Mr Dhammika Priyantha Pallek Kankanamge, Sri Lanka, LEA expert

The assessment process was supported by Mitali Tyagi, Suzie White and David Shannon of the APG secretariat.

The report was reviewed by Ms Ferti Srikandi from Indonesia, Mr Andy Chan from Hong Kong, China and the FATF Secretariat.

The Philippines previously underwent mutual evaluation in 2009, conducted by the World Bank in according to the 2004 FATF Methodology. The 2009 evaluation has been published and is available at www.apgml.org.

The Philippines' 2009 Mutual Evaluation concluded that the country was compliant with 3 Recommendations; largely compliant with 11; partially compliant with 28; and non-compliant with 6. The Philippines was rated compliant or largely compliant with 3 of the 16 Core and Key Recommendations.

The Philippines exited the APG's transitional follow-up process in 2017 as per paragraph 5.11 of the APG Transitional Follow-up Procedures, given the Philippines upcoming third round mutual evaluation. The Philippines had made progress with eight of the 13 core/key recommendations rated NC/C in its 2009 MER, namely R.3, R.4, R.26, SR.I, SR.II, SR.III, SR.IV, SR.V. Five recommendations, namely R.1, R.5, R.13, R.26 and R.35 remained at the NC/PC level.

In 2010 the Philippines entered the FATF's International Cooperation Review Group (ICRG) process due to its 2009 MER results. The Philippines exited the ICRG process in June 2013. As part of the exit decision, the FATF expressed concerns regarding the casino sector risk and the lack of coverage under the Philippines AML legislation. The FATF requested the APG apply enhanced monitoring of this issue under the APG 2nd round ME follow-up process until the deficiency regarding the casino sector was addressed.

Between 2014 and 2017 the Philippines was subject to expedited reporting to the APG on the ICRG issue of concern (regulation and supervision of the casino sector). The casino sector came under AML/CFT regulation and supervision through An Act Designating Casino Operators as Covered Persons to amend the Anti-Money Laundering Act of 2001 which entered into force in July 2017 and its Implementing Rules and Regulations, which entered into force on 4 November 2017.

CHAPTER 1. ML/TF RISKS AND CONTEXT

1. The Republic of the Philippines (“the Philippines”) is an archipelago located in the western Pacific Ocean in Southeast Asia. The Philippines consists of 7,641 islands, with a total land area of approximately 340,000 square kilometres divided into 17 regions, with Manila as its capital. As of 2015¹ the population of the Philippines was 100.98 million.²

2. The official languages for the Philippines are English and Filipino (a standardised variety of the Tagalog language). There are more than 100 languages spoken in the Philippines, and of these, eight are considered main languages; Bikol, Cebuano, Hiligaynon (Ilonggo), Ilocano, Kapampangan, Pangasinan, Tagalog, and Waray.³

3. The Philippines’ Gross Domestic Product (GDP) for 2017 was US\$313.6 billion, with an annual GDP growth of 6.7%.⁴ In 2018, almost 52% of Filipinos were employed in the services sector, with 25% employed in the agriculture sector and 22% in the industrial sector.⁵ The official unemployment rate has remained reasonably constant around 5-6% with no official estimate on underemployment and employment in the illicit economy.

4. The Philippines is a constitutional Republic. The government is comprised of three branches; executive, legislative and judicial. Executive power is exercised by the President, who is elected by direct vote and serves only a single term of six years. The President is also the Head of State, Head of Government and Commander in-Chief of all armed forces in the Philippines.

5. The Philippines’ legal system is a combination of civil, common and customary law. The Philippines also recognise Shari’a law in respect of family and personal matters of Filipino Muslims.

6. Under the 1987 Constitution other sources of law are statutes, treaties and conventions and judicial decisions. The Philippines also adopts generally accepted principles of international law as part of the law of the land. Treaties entered into by the Philippines and concurred with by two-thirds of the members of the Senate are considered to be part of the law of the land.

ML/TF Risks and Scoping of Higher-Risk Issues

Overview of ML/TF Risks

Money Laundering

7. The assessment team broadly agrees with the Philippine authorities assessments that the highest ML threats faced by the Philippines include proceeds from corruption, drug trafficking, investment fraud, smuggling, tax crimes, copyright/intellectual property violations, illegal firearms and environmental crimes. The Philippines faces wide ranging transnational fraud threats.⁶

¹ <https://psa.gov.ph/content/highlights-philippine-population-2015-census-population>

² More recent but unofficial figures estimate that the current population is closer to 108 million. See <https://www.imf.org/en/Countries/PHL#countrydata>

³ <http://ncca.gov.ph/about-ncca-3/subcommissions/subcommission-on-cultural-disseminationscd/language-and-translation/development-of-filipino-the-national-language-of-the-philippines/>

⁴ <http://www.bsp.gov.ph/statistics/>

⁵ <https://data.worldbank.org/indicator/SL.AGR.EMPL.ZS>

⁶ <https://www.pwc.com/ph/en/consulting-pwc-ph/assets/pwc-ph-economic-crime-fraud-survey-2018.pdf>

8. Philippine authorities recognise significant risks from domestic corruption and have considered aspects of the risks of foreign corruption proceeds. For domestic corruption, issues such as bribery, extortion, embezzlement, procurement fraud, patronage, state-owned enterprises and tendering processes, and facilitation of other predicate crime types present particular risks. The 2017 national risk assessment (NRA) estimates that 20% of the Philippines' yearly national budget is lost to corruption.

9. The geographical landscape and vast maritime borders and sea ports make the Philippines susceptible to the smuggling of illicit goods and cash, trafficking of persons, and other cross-border issues. The risk of cross-border issues is increased by well-frequented connections with other major Asian cities, regional transit hubs, unregulated private ports, and the limited resources and ability of customs agencies to detect suspicious activity and transactions. Corruption has also been detected among customs officials, allowing borders to be exploited by organised crime and terrorist groups.

10. The Philippines is a noted transit point for illicit drugs and is a significant producer and transit point for crystal methamphetamine (locally referred to as "shabu"). The 2017 NRA noted an estimated PHP1.6Billion (approx. USD 30.5 million) worth of illegal drugs were intercepted in various smuggling activities in 2016. Transnational crime syndicates, together with local criminal groups, smuggle precursors and chemicals into the country via mislabelled shipments and set up shabu laboratories. Shabu is then distributed both locally and internationally. The 2017 NRA listed 305 high-impact operations conducted in 2016, involving the dismantling of shabu laboratories and chemical warehouses, eradication of marijuana plantations, and operations in major ports.

11. With one of the largest overseas worker populations in the world,⁷ the Philippines' remittance sector is an important source of revenue for the country. It is estimated that 2.3 million Filipinos worked abroad during the period April to September 2017.⁸ Incoming foreign worker remittance during that period is estimated at PHP205.2 billion (approx. USD 4 billion).

12. The size and materiality of the MSB sector contributed to its rating as high risk for sectoral threat in the 2017 NRA. However, the measures in place in the Philippines to mitigate this threat resulted in the vulnerability being assessed as medium-high. Certain investigations by AMLC were mentioned to highlight that criminal elements in drug trafficking and sex trafficking had used MSBs to move funds. Further, PHP 3.8 billion (approx. USD 72 million) of the funds involved in the "Bangladesh Bank Heist" were moved through three remittance services (see IO.7 for case study). All MSBs were subject to the provisions of the AMLA for the period reviewed by this mutual evaluation.

13. There are very significant risks of ML (domestic and foreign proceeds of crime) through the large Philippine casino sector. Integrated resort casinos, standalone land-based casinos, online casinos, junket operators and international movement of funds in relation to junket operations and casino-related tourism, present significant risks for ML.

14. Tax evasion and tax-related crimes are prevalent in the Philippines. The 2017 NRA notes that in 2015, the Bureau of Internal Revenue (BIR) netted 94 cases of tax-related crimes, with an estimated tax liability of approximately USD185.5 million. Tax evasion is not a predicate offence to ML.

⁸ Philippine Statistics Authority 2017 Survey on Overseas Filipinos, accessed at <https://psa.gov.ph/statistics/survey/labor-and-employment/survey-overseas-filipinos>

Anti-money laundering and counter-terrorist financing measures in Philippines @ APG 2019

Terrorism and Terrorist Financing

15. Terrorism threats in the Philippines include the operation of a range of terrorist/threat groups, which are mainly active in the southern provinces, but also active in other parts of the country. The identified terrorist/threat groups are categorized by the Philippines authorities as ISIL-inspired groups, secessionist/separatist movements and insurgency movements. Researchers highlight the draw of foreign terrorist fighters (FTF) to conflict areas in the Southern Philippines, before and since the Marawi siege. Since the creation of the Abu Sayyaf Group in 1989 (the major terrorist group operating in the Philippines), activities have been motivated by foreign influences – first by Al-Qaeda and then the ISIL⁹. Credible research sources indicate that the threat of ISIL persists despite the liberation of Marawi City from pro-ISIL elements in 2017. While the Philippine government signed a peace agreement with the Moro Islamic Liberation Front (MILF) in 2014, the Abu Sayyaf Group and affiliates have been operating in Mindanao and other parts of the Southern Philippines on behalf of, and under the direction of, ISIL since 2014. Media sources indicate a number of groups pledged allegiance to ISIL from 2014 to 2017, with government sources identifying four pro-ISIL groups responsible for the siege of Marawi¹⁰. The authorities indicate that most of these groups named in the media report are only sub-groups of the Abu Sayef Group or smaller groups joining the “bandwagon” for the establishment of wilayat in the Philippines. At the height of ISIL popularity, there was a bandwagon effect with several of the so-called groups pledging their allegiance to ISIL. A number of groups have staged attacks since the end of the Marawi siege, including Daulah Islamiyah Maguindanao and the Suyuful Khilafa Fi Luzon (SKFL)¹¹.

16. The 2017 NRA assessed the risk for TF as high. This is consistent with the TF Regional South-East Asia and Australia Risk Assessment 2016, which noted that criminal activity in the Philippines and cross-border cash smuggling increases the risk of exploitation by criminal and terrorist organisations linked to the conflict in the southern provinces.

17. The last assessment of TF risks was for the period ending 2016. Following the Marawi siege in 2017, AMLC conducted Maute Financial Network Analysis and contributed to the Regional Assessment on ISIL Funding to update understanding of risk. Terror organisations such as the Abu Sayyaf and Maute Groups were noted to use an array of legal and illegal means to raise funds, transported largely through the physical movement of cash and remittances, and thereby facilitate attacks. Misuse of NPOs has been noted as a possible way to raise funds. However, the Philippines has faced terrorism and TF challenges since 2016 with regional and global TF activities continuing to pose a threat including the funding of the movement and activities of FTF to and from the Philippines.

18. An August 2018 UN Security Council report noted that funding of ISIL-linked groups in the Philippines from intermediaries in South East Asia continues. In 2018, the US Department of the Treasury noted individual financing of foreign terrorist groups—including in the Philippines—as the most common TF activity in the United States.¹² AMLC has frozen terrorist assets worth P52 million

⁹ Rommel C. Banlaoi, “Abu Sayyaf Group’s Persistence: A Chronological Analysis of Crime- Terror Nexus in the Philippines and the Isis Connection in Southeast Asia,” *Peace and Security Review* 7, no. 15 (2016): 50-72

¹⁰ “The Lamitan Bombing and Terrorist Threat in the Philippines”
<https://www.rsis.edu.sg/wp-content/uploads/2018/09/CTTA-September-2018.pdf>

¹¹ “2 IS Sympathizers Fall,” *Philippine Daily Inquirer*, April 28, 2018, <http://newsinfo.inquirer.net/985985/2-is-sympathizers-fall>

¹² See para 41, p8: https://www.securitycouncilreport.org/atf/cf/%7B65BF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2018_770.pdf

See p2: https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf

(approx. USD 1 million), which was seized by the military in Marawi. Philippine authorities were also able to neutralise leaders of the Abu Sayyaf Group and the Maute Group during the Marawi siege.

19. Such funding activities appear to sustain material support and ongoing recruitment of followers within and beyond the Philippines. The southern Philippines in particular was noted to be a destination and transit point for FTF, with arrests of suspected FTF who had travelled to the Philippines using stolen or false documents and broken travel routes.¹³

20. The southern province of Mindanao is a conflict zone where terrorism and TF issues are rampant. The province of Mindanao has been under martial law since 2017, and as such, counter-terrorism actions, including any investigation of TF, are conducted in a military context and priorities may often relate to the maintenance of security and control. Complex investigations of identifying and pursuing financiers of the terrorist groups are rarely undertaken.

21. The NPO sector has been largely unregulated and unsupervised in relation to TF risk, although there are existing laws and enforceable means that regulated fund-raising activities and existing monitoring and supervision mechanisms. Media reports suggesting possible abuse of legitimate NPOs for diverting funding to terror groups in the southern province of Mindanao identified foreign aid funds possibly being diverted to Alhayam Sultana Constructions, which allegedly belonged to members of the ISIL-linked Maute family.

The Philippines' assessments of risk

22. The Philippines has completed two NRAs: the first covering the period of 2011-2014 (2015 NRA); and the second NRA (2017 NRA) covering 2015-2016. The reports identify a range of ML and TF threats and sectoral vulnerabilities based on self-assessments conducted by Philippine authorities. The 2017 NRA identifies the significant threats as tax crimes, smuggling, violation of intellectual property rights, illegal manufacture and possession of firearms, ammunitions and explosives, violation of environmental laws, investment scams, drug-related crimes and corruption. Other identified threats include cybercrime, human trafficking and kidnapping for ransom.

23. The Philippines' period of review through its NRAs ended in 2016. The next update to the Philippines' risk assessment is planned for 2020 with AMLC as the designated lead. Under Strategic Objective 7 of the NACS, the periodic updating of the NRA and the Serious Organized Crime Threat Assessment are among the priority actions for continuous awareness on ML/TF risks.

24. Key vulnerabilities include a cash-based economy, cross-border issues, NPOs, banking, MSBs and DNFBPs, particularly the casino sector, and the practical effect of bank secrecy laws.

Scoping of Higher Risk Issues

25. Based on the results of the 2017 NRA, discussions with the Philippines, open-source information and information provided by APG members, the assessment team particularly focussed on the following high-risk issues during the mutual evaluation on-site visit:

- **Governance and capacity** – including the competent authorities' capacity challenges and resources and skills to implement an effective, risk-based AML/CFT system.

¹³ See para 39, p.8: https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2018_770.pdf

Anti-money laundering and counter-terrorist financing measures in Philippines @ APG 2019

- **Corruption** – The 2017 NRA noted that corruption remains a major source of illicit proceeds in the Philippines.
- **Organised crime** – Organised crime groups are responsible for the manufacture of illicit drugs (particularly methamphetamine), drug, cash and weapon smuggling and other predicate offences in the Philippines.
- **Illicit drug trade and smuggling** – The Philippines is a noted transit country for illicit substances and generated proceeds. The 2017 NRA noted smuggling as a high risk issue.
- **Fraud and cybercrime** – The 2017 NRA noted that cybercrime (web-enabled crime) was a medium risk for ML, and fraud is identified as high risk.
- **Tax crimes** – Tax evasion is not a designated predicate offence for ML and is listed as high risk in the 2017 NRA.
- **Trafficking of persons** – The 2015 NRA identified the trafficking of persons as high risk, and this was downgraded to medium risk in the 2017 NRA. The team focussed on the reason for the downgrade. The Philippines has been identified as a source, transit and destination country for forced labour and sex trafficking.
- **Terrorist financing** – TF is considered high risk in the Philippines. As noted in the 2017 NRA, borders in the Southern Philippines have been exploited by terrorist organisations.
- **Cross-border and international issues** – in particular the Philippines cooperation with foreign counterparts to mitigate cross-border ML/TF risks, given the Philippines' strong global connections.
- **Cash economy** – The Philippines is a cash-based economy and the physical movement of cash is a preferred mode to move money or transfer value (including for TF).
- **Remittances** – There is a sizeable, and growing, remittance sector in the Philippines. The MSB sector is inherently high risk and there is evidence that it has been used to move money linked to illegal activity, including drugs and fraud.
- **Trade-based ML (TBML)** – The 2017 NRA noted a large increase in trade mis-invoicing between 2005 and 2014, correlated with the significant magnitude of illicit funds moving into the country, through the cash economy and the financial system.
- **Casinos** – Prior to 2017 the Philippines lacked AML regulation for casinos. This had been a focus for both the FATF and APG.
- **Bank secrecy** – The Philippines' bank secrecy provisions have raised concerns with a range of authorities regarding the ability to 'follow the money'.

26. Initial scoping identified that the insurance sector posed a lower level of threat and vulnerability, so it was given less focus throughout the evaluation.

Materiality

27. The Philippines is a lower-middle income country poised to advance to an upper-middle income country in the medium term.¹⁴ There is increasing urbanisation, a large, young population and

¹⁴ <http://www.worldbank.org/en/country/philippines/overview>

a growing middle class.¹⁵ The services sector, particularly business process outsourcing, real estate and the financial and insurance sectors are strong performers in the Philippines economy.¹⁶

28. The Philippines' GDP in 2017 was USD313.6 billion, composed as follows; services at 59.8%, industry at 30.6% and agriculture at 9.6%.¹⁷

29. The Philippines imported USD 101.9 billion and exported USD 68.7 billion worth of goods globally in 2017.¹⁸ The Philippines' top five export partners in 2017 were Japan (USD 68.7 billion), United States (USD 9.7 billion), Hong Kong, China (USD 9.0 billion), China (USD 8.0 billion) and Korea (USD 4.3 billion). The top five import partners were China (USD 18.5 billion), Japan (USD 11.8 billion), Korea (USD 8.8 billion), United States (USD 8.3 billion) and Thailand (USD 7.1 billion).¹⁹

30. The poverty rate declined in the Philippines, from 26.6% in 2006 to 21.6% in 2015.²⁰ However it is as high as 75% in some areas of the southern Philippines.²¹ Unemployment has declined; however under-employment remains high, as workers transition out of agriculture to low-end service jobs. This has resulted in average wages remaining stagnant between 2006 and 2015.

31. The Philippines is a cash-based economy and the physical movement of cash or cash couriering is the preferred mode to move money or transfer value domestically.

32. The Philippines' has a widespread remittance sector, with cash remittance growing by close to 6% on average between 2014 and 2017. In 2017 60% of OFW (including sea-based) remittances flowed through the money transfer operators (MTOs) sector with a connection to MSBs. Personal remittances in the sector accounted for approximately USD 940 million in 2017.

33. Philippines authorities place an emphasis on financial inclusion, recognising risks from financial exclusion and the adverse impact of 'de-risking' experienced in the Philippines. A 2017 survey by BSP identified that only 22.6% of the total adult population had a formal financial account (e.g. bank account, microfinance, e-money, etc.), with only 11.5% of the population having bank accounts.²² The Philippines has identified that digital financial inclusion is key to reaching the large unbanked population. BSP has established the Inclusive Finance Advocacy Office and has pursued a range of reforms to allow more non-banks to offer financial services including for money transfers and payments.²³ BSP Circular No. 980 (6 November 2017) enforced the adoption of the National Retail Payment System on BSP supervised institutions such that they operationalise an interconnected and interoperable retail payment systems. BSP recognises the role of emerging technologies (e.g. digital identity leveraging on the national ID, KYC utilities, Legal Entity Identifier) in addressing the pain points in on boarding customers to the mainstream financial system.

34. The BSP considers de-risking of MSBs to be a significant issue that is adversely impacting financial inclusion in the Philippines.²⁴ In keeping with other jurisdictions' experience, de-risking has

¹⁵ <http://www.worldbank.org/en/country/philippines/overview>

¹⁶ <http://www.worldbank.org/en/country/philippines/overview>

¹⁷ <https://www.cia.gov/library/publications/the-world-factbook/geos/rp.html>

¹⁸ <https://comtrade.un.org/data/>

¹⁹ <https://comtrade.un.org/data/>

²⁰ <http://www.worldbank.org/en/country/philippines/overview>

²¹ <https://www.cia.gov/library/publications/the-world-factbook/geos/rp.html>

²² <http://www.bsp.gov.ph/downloads/Publications/2017/2017FISToplineReport.pdf>

²³ <https://www.bworldonline.com/philippines-shines-in-terms-of-financial-inclusion/>

²⁴ <https://www.philstar.com/business/2016/04/29/1578095/bsp-tackles-impact-de-risking-strategy#oUiC5qbXbRzvV5z5.99>

Anti-money laundering and counter-terrorist financing measures in Philippines @ APG 2019

reduced the availability of remittance channels and increased the cost of remittance, potentially creating financial exclusion and movement towards informal, unregulated channels. Authorities noted instances of foreign banks de-risking some Filipino MSBs, in part as a response to the ML/TF risks in the Philippines. Reasons cited by the foreign banks when closing accounts of MSBs have included a business strategy to not deal with MSBs in general, more stringent regulatory requirements in the host jurisdiction and business decisions.

35. The Philippines has a sound financial system, with well-capitalised banks.²⁵ The Philippines is not considered to be a regional financial centre. Total assets of the banking system in 2017 were PHP 15,166 billion (approx. USD 289 billion), which constitutes approximately 96% of the 2017 Philippines GDP.

36. The DNFBP sector in the Philippines comprises casinos, jewellery dealers, dealers in precious metals or stones, company service providers, lawyers and accountants. As of 2017 the assets of the casino sector, the most material DNFBP sector, were PHP 30,671.18 million (approx. USD 584 million). The Philippines' casino sector is an important source of revenue for the country's economy and tourism. PAGCOR estimates that in 2017, the Philippine gaming industry generated around USD3.4 billion in revenue²⁶. The revenue of the gaming industry continues to increase at a rapid rate, having grown more than 58% from 2014 to 2017. All DNFBPs are included within the AML/CFT regime, with the exception of the real estate sector, which is not captured under the AMLA.

Structural Elements

37. While the main structural elements required for an effective AML/CFT system are largely in place, the Philippines faces challenges with corruption, practical effects of bank secrecy laws, and de-risking.

38. Governance indices from the 2012 and 2017 World Bank World Wide Governance Indicators Country Snapshots²⁷ show that the Philippines' ranking for voice and accountability, regulatory quality and control of corruption has improved since 2012. Rankings show a decline for rule of law, political stability and absence of violence/terrorism and governance effectiveness since 2012.

Table 1.1: Philippines Governance Indicators 2017 – World Bank World Wide Country Snapshot

Indicator	Percentile Rank (1-100) ²⁸ 2012	Percentile Rank (1-100) 2017
Voice and Accountability	48	49
Political Stability and Absence of Violence/Terrorism	14	11
Government Effectiveness	59	52
Regulatory Quality	52	56
Rule of Law	39	37
Control of Corruption	35	40
Average	41.16	40.83

²⁵ <https://www.imf.org/en/News/Articles/2018/09/27/na092718-the-philippines-economic-outlook-in-six-charts>

²⁶ <https://www.imf.org/external/pubs/ft/bop/2018/pdf/18-23.pdf>

²⁷ <http://info.worldbank.org/governance/wgi/index.aspx#reports>

²⁸ With 100 being the highest score.

39. Although the ranking for ‘control of corruption’ has improved, corruption still remains a significant issue in the Philippines. The 2017 NRA estimates that 20% of the Philippines’ yearly national budget is lost to corruption. The Philippines is ranked 111th out of 180 countries in the Corruption Perception Index 2017.

Banking Secrecy

40. The Philippines’ Bank Secrecy Act and other statutes prohibit competent authorities from directly accessing bank information. S.24 of the AMLA overrides the Bank Secrecy Law, and other similar statutes, in so far as it is inconsistent with the AMLA. AMLC has access to bank account information through its STR/CTR framework and through orders to access to CDD information, including BO information, held by banks, which is used in the conduct of analysis and to support investigations. Results of AMLC analysis and investigations, which includes CDD and BO information obtained by banks can be shared with other LEAs.

41. The AMLC has placed some restrictions on the timing of its disseminations of information related to PEPs, with no information able to be shared during election periods.

42. The bank secrecy laws hinder timely access and exchange of information relating to PEPs, BO and legal arrangements, as competent authorities are required to request AMLC to obtain financial information held by banks on their behalf. The limitation to a single agency being able to lift bank secrecy creates practical challenges and inhibits the ability of other LEAs and competent authorities directly and timely access to banking records to properly perform their functions to combat ML, TF and predicate offences and to trace proceeds of crime.

Background and other Contextual Factors

AML/CFT strategy

43. The Philippines’ National AML/CFT Strategy 2018-2022 (NACS) was finalised in June 2018, adopted on 12 November 2018 and covers AML, CFT and PF. It was developed in response to the NRA findings and includes risks, priorities and an action plan for achieving its seven strategic objectives:

Strategic objective 1: Enhance the Philippines’ AML/CFT legal framework in order to effectively address the country’s ML/TF risk and the deficiencies in the country’s compliance with the international standards.

Strategic objective 2: Strengthen AMLC and its capacity for ML/TF intelligence gathering, investigations and prosecutions in order to become a more effective partner in combating ML, predicate offences, terrorism and TF.

Strategic objective 3: Improve capacity and collaboration among the FIU, LEAs and prosecutors for the effective investigation and prosecution of, as well as the confiscation of proceeds relating to ML, predicate offences, terrorism and TF.

Strategic objective 4: Enhance the AML/CFT regulation and supervision framework to ensure effective and robust AML/CFT systems in supervised institutions for the purpose of protecting the financial system, DNFBPs and the economy from the threat of ML and TF.

Strategic objective 5: Develop and strengthen mechanisms to prevent, disrupt and combat terrorism, TF and PF.

Strategic objective 6: Strengthen domestic and international cooperation mechanisms for the effective exchange of information, facilitate action against criminals and their assets and assist in the capacity building of relevant government agencies.

Strategic objective 7: Promote AML/CFT awareness of government agencies, covered persons and the general public to effectively combat ML/TF.

Legal & institutional framework

44. The legal framework for AML/CFT preventative measures is set out in the Anti-Money Laundering Act of 2001 (AMLA). ML is criminalised under the AMLA and TF is criminalised under the Terrorism Financing Prevention and Suppression Act of 2012 (TFPSA).

45. Since its last mutual evaluation the Philippines has made significant changes to its AML/CFT legal and regulatory framework. These have included: amending the AMLA to increase the range of predicate offences; allowing AMLC to file *ex parte* applications for bank records to the court; designating casinos as covered persons; issuing a number of implementing regulations for covered sectors and issuing further AMLC resolutions and guidelines to expand obligations and support their implementation.

46. The institutional framework for AML/CFT is as follows:

- **Anti-Money Laundering Council (AMLC)** is a hybrid FIU and its primary roles include acting as the FIU of the Philippines; obtaining bank records on behalf of other competent authorities; investigating ML and TF cases; filing civil forfeiture claims (restraint and confiscation); and conducting AML/CFT supervision and enforcement. AMLC's four work streams are as follows:
 - Financial Intelligence and Analysis Group (**FIAG**) - the financial intelligence analysis arm of AMLC which receives and analyses financial transactions and other information, and disseminates financial intelligence to AMLC's investigation arm (FCIG).
 - Financial Crimes Investigation Group (**FCIG**) conducts financial analysis and financial investigations. FCIG is the primary designated authority to investigate ML and TF offences. FCIG financial investigations serve as basis for: a) civil action for asset forfeiture; b) prosecuting ML; and/or c) responding to international cooperation requests. FCIG disseminates financial intelligence to LEAs, other relevant government bodies, and international counterparts to combat ML/TF and predicate crimes.
 - The Litigation and Evaluation Group (**LEG**) evaluates the ML/TF investigation reports of the FCIG investigators, and prepares the pleadings for the filing of appropriate cases for prosecution and civil forfeiture. The LEG also coordinates with the DOJ (for criminal cases), the Office of the Ombudsman (for public officers) and the OSG (for application for bank inquiry, petition for freeze and civil forfeiture cases).
 - The Compliance and Supervision Group (**CSG**) conducts onsite and offsite examination or other forms of compliance checking on covered persons related to compliance with, the AMLA and TFPSA, their respective IRR, and other AMLC issuances. AMLC may issue administrative sanctions for non-compliance.
- **Armed Forces of the Philippines (AFP)** is the primary agency responsible for counter terrorism actions in the Philippines. The AFP also assists LEAs in the enforcement of domestic

and foreign policies against crimes such as slavery, piracy, environmental crimes and smuggling.

- **Aurora Pacific Economic Zone and Freeport Authority (APECO)** is a casino regulator and operator (independently, or through a subsidiary entity, concession or licenses) within its freeport. These include land and online gaming facilities.
- **Bangko Sentral ng Pilipinas (BSP)** is the central bank, and financial supervisor, of the Philippines. The powers and functions of the BSP are exercised by the Monetary Board. The BSP conducts AML/CFT offsite and onsite supervision of FIs under its regulation.
- **Bureau of Customs (BOC)** is responsible for revenue collection, trade facilitation and border protection. BOC is responsible for collecting currency declaration reports and disseminating these to AMLC.
- **Cagayan Economic Zone Authority (CEZA)** is the regulator, AML/CFT supervisor and provider for casinos for Cagayan Economic Zone and Freeport. CEZA has the power to issue gaming licenses or it can outsource its gaming power to private entities through “Master Licensor Agreements” for granting sub-license. CEZA has outsourced its power to two private entities; First Cagayan Leisure and Resort Corporation is the duly appointed Master Licensor for Internet Gaming Operations while the North Cagayan Gaming and Amusement Corporation is issuing sub-licences for land-based casinos.
- **Department of Justice (DOJ)** is responsible for prosecuting offences, including ML and TF. DOJ is the Central Authority for MLA and extradition matters.
- **Department of Trade and Industry – Strategic Trade and Management Office (DTI-STMO)** manages trade in strategic goods including registration of strategic goods-related activities and maintaining a national database on persons trading in strategic goods.
- **Insurance Commission (IC)** is the insurance sector regulator and AML/CFT supervisor.
- **Office of the Ombudsman** is an independent constitutional body responsible for investigating complaints against public officials, employees, government agencies and government owned or controlled corporations in respect of corruption-related crimes. It has the power to initiate action for recovery of proceeds of corruption and/or unexplained wealth.
- **Office of the Solicitor General (OSG)** is an independent office representing the Government of the Philippines, its agencies and its instrumentalities, as well as government officials and agents in any litigation, proceeding or investigation. OSG performs the role of Statutory Counsel for AMLC in applications for bank inquiry, freezing orders, and civil forfeiture.
- **Philippine Amusement Gaming Corporation (PAGCOR)** is the national authority empowered to license gaming entities, except those delegated to special economic zones.
- **National Bureau of Investigation (NBI)** is an LEA responsible for handling high profile criminal of national interest, including counter-terrorism operations, ML and TF.

- **National Intelligence Coordinating Agency (NICA)** is the primary intelligence agency responsible for the coordination of national intelligence activities of government agencies. NICA is also the Secretariat of the Anti-Terrorism Council.
 - **Philippine National Police (PNP)** is the armed civilian police force of the Philippines with a broad mandate to investigate predicate offences and ML/TF.
 - **Philippine Centre for Transnational Crime (PCTC)** is the designated agency for international liaison with LEAs in the Philippines. PCTC coordinates and monitors activities among LEAs in relation to transnational crime. It also exercises general supervision and control over the INTERPOL National Central Bureau.
 - **Philippine Drug Enforcement Agency (PDEA)** is the lead anti-drug LEA tasked to prevent, investigate and combat illicit drugs. It has a broad enough mandate to investigate ML/TF where these are drug related crimes.
 - **Presidential Anti-Organized Crime Commission (PAOCC)** is tasked with eradicating organised crime groups/syndicates. It is responsible for implementing an anti-crime, anti-graft and corruption action plan and program, and conducts intelligence and counter-intelligence operations. It is not empowered to investigate ML related to organised crime.
 - **Securities and Exchange Commission (SEC)** is the regulator and registrar for the corporate sector (i.e. registration of all legal persons). SEC is responsible for the supervision of the corporate sector, capital market, securities and investment instruments market and investors to ensure AML/CFT compliance.
1. There are four coordination bodies within the AML/CFT framework of the Philippines:
- **National AML/CFT Coordinating Committee (NACC)**, established in November 2018 to facilitate inter-agency coordination focused on the development of national policies on AML/CFT, implement the NACS and provide direction to relevant agencies on major issues. The NACC comprises five sub-committees:
 - a) Financial Intelligence, Law Enforcement and Prosecution,
 - b) Supervision of FIs,
 - c) Supervision of DNFBP,
 - d) TF and PF,
 - e) AML/CFT Awareness.
 - **Anti-Terrorism Council** is the national body responsible for implementing the Philippines' anti-terrorism policy. It also serves as the national supervising and coordinating body for terrorism-related matters.
 - **National Security Council (NSC)** is the principal advisory body for the coordination and integration of plans and policies affecting national security. The **Strategic Trade Management Committee (NSC-STMCom)** is a permanent committee under the NSC and is the authority for all matters relating to strategic trade management.

- **National Law Enforcement Coordinating Committee (NALECC)** serves as a forum for dialogue and coordination among government agencies engaged in the enforcement of general and special laws. NALECC coordinates policies/ procedures to facilitate cooperation and integration of effort. The NALECC has 18 sub-committees including a Sub-Committee on AML/CFT (chaired by the AMLC Secretariat Executive Director) which has 35 members and meets monthly. The Sub-Committee on AML/CFT passes resolutions on operational measures.

Financial sector and DNFBPs

47. The Philippines' financial system is dominated by the banking sector, which accounts for approximately 80% of financial sector assets. In 2017 the banking system's assets expanded by 12%.²⁹ Universal and commercial banks constitute 90.8% of the banking system's total assets, with the remainder attributable to rural, cooperative and thrift banks.³⁰ The number of physical offices of banks is increasing due to additional branches of universal/commercial banks and new foreign bank entrants. However there is a decline in the number of head offices, due to the streamlining of the banking landscape. Philippine banks have branches or offices located in the Middle East and Asia-Pacific Regions, which reflects the Filipino OFW diaspora.

48. NBFIs, namely pawnshops, MSBs, non-stock savings and loan associations (NSSLA) and e-money issuers (EMI, now re-categorised as MSBs), are supervised by BSP. The estimated assets of pawnshops, NSSLAs and EMIs is PHP 234 billion (approx. USD 4.4 billion), which accounts for 1.2% of financial assets in the Philippines.

49. The MSB sector includes MVTs providers (money transfer operators), foreign exchange dealers and money changers. The Philippines has recently undertaken an extensive re-registration process in the MSB sector which has seen a significant consolidation in the sector. The re-registration process introduced capital requirements and fit and proper tests to increase the level of AML/CFT competency and compliance. Of 1,621 MSB identified by the BSP as potential re-registrants, approximately 1,000 had re-registered at the time of the onsite visit. MSBs required to register, or re-register, include foreign exchange dealers, money changers, virtual currency exchanges and MVTs providers. MVTs providers are now referred to as Remittance Transfer Companies (RTCs) and include EMIs and any remittance agent with more than one office. Smaller remittance agents (i.e. with only one office) are considered an extension of the RTC.

50. The securities sector comprises securities brokers, investment companies and financing and lending companies. Most investment companies and mutual funds are bank affiliates with 83 subsidiaries of banks that offer securities products, accounting for over 98% of the total assets of the securities sector. The assets of the securities sector and was estimated to be PHP 9,106 billion (approx. 173 billion) in 2017, approximately 58% of GDP.

51. The insurance sector includes insurance companies (life, non-life, composite), reinsurance, mutual benefit associations, pre-need companies and health maintenance organisations. The combined assets of the insurance industry were approx. USD 34 billion in 2017. Total assets of life insurance companies constitute 58% of the total assets in the insurance industry.

52. All of the DNFBP sectors, with the exception of real estate, are subject to AML/CFT obligations. Most DNFBPs were captured in 2013, with casinos included in July 2017.

²⁹ 2017 BSP Annual Report. <http://www.bsp.gov.ph/downloads/publications/2017/annrep2017.pdf>

³⁰ Descriptions of various types of bank available at <http://www.bsp.gov.ph/banking/bspsup.asp>

Anti-money laundering and counter-terrorist financing measures in Philippines @ APG 2019

53. The Philippines' gaming industry posted gross revenue of approximately PHP177 billion (approx. USD 3.4 billion) in 2017. Authorities were unable to provide the higher figure of gross turnover in the sector. The sectors gross revenue grew by more than 58% between 2014 and 2017. In 2017 86% of gaming revenue in the Philippines came from land-based casino operations, with 14% from PAGCORs e-games and less than 1% from internet casino licensing. PAGCOR posted consolidated gross gaming revenue of approx. USD 3.4 billion and CEZA posted gross revenue of over USD 3.9 million in 2017.

54. The estimated assets of real estate, renting and business activities (RERBA) made up 12.8% of the Philippines' GDP in 2017, equating to approximately USD41 billion. While real estate agents are not captured as covered persons under the AMLA, authorities noted that most of the larger players in the real estate sector are part of banking group conglomerates.

Table 1.2: Financial sector and DNFBP numbers as at March 2018

Sector	Number	Licensing Authority	General supervisor	AML/CFT Supervisor ³¹
Financial Institutions				
Banking System	585	BSP	BSP	BSP
a. Universal & commercial	43			
i) Private domestic banks	17			
ii) Government banks	3			
iii) Foreign bank subsidiaries	23			
b. Thrift Banks	55			
c. Rural Banks	462			
d. Cooperative banks	25			
Non – Banks (subsidiaries)	83			
Non – Banks (others)	5,501			
a. Non-stock Savings and Loan Associations	65			
b. Pawnshops with remittance services Non – Banks (subsidiaries)	751			
c. Money Service Businesses ³²	4,679			
d. E - Money Issuers Non-Banks (others)	6			
Brokers and Dealers	142			
Investment Houses / Securities Underwriters	38			
a. Investment Houses	26	SEC	SEC/BSP	SEC/BSP
b. Securities Underwriters (universal banks)	12	SEC	BSP	BSP
Government Securities Eligible dealers (banks)	26	SEC	BSP	BSP
Investment co. /Mutual Fund	85	SEC	SEC	SEC
a. Investment Company Advisers	11			
b. Mutual Fund Distributors	10			
c. Investment companies	64			
Financing companies	681	SEC	SEC	SEC

³¹ AMLC, as central authority for AML/CFT, is also an AML/CFT supervisory for all covered persons.

³² Note that since the restructure of the MSB sector, pawnshops with remittance services and e-money issuers are now combined (all considered Remittance Transfer Companies).

Sector	Number	Licensing Authority	General supervisor	AML/CFT Supervisor ³¹
Lending companies	2,535	SEC	SEC	SEC
Life insurance	27	IC	IC	IC
Non-Life insurance companies	55			
Composite insurance companies	4			
Professional Reinsurer	1			
Mutual Benefit Associations	35			
Insurance Brokers	85			
a. Insurance	65			
b. Reinsurance	20			
DNFBPs				
Land Based Casinos	10 ³³	PAGCOR	PAGCOR	AMLC, PAGCOR
Online Casinos	84 ³⁴	PAGCOR, CEZA	PAGCOR, CEZA	AMLC, PAGCOR, CEZA
Accounting firms ³⁵	28	PRC ³⁶		AMLC
Law firms ³⁸	43	Supreme Court		AMLC
Trust entities ³⁸	39	BSP	BSP	BSP
Company Service Providers ³⁸	11	DTI/SEC		AMLC
Jewellery Dealers and dealers in precious metals and stones ³⁷	30	DTI/SEC		AMLC

Table 1.3: Sectoral ML/TF threat and vulnerability rating in 2017 NRA

Sector	Threat	Vulnerability
Banking	High	Medium
MSB	High	Medium High
Securities	Medium	Medium
Insurance	Medium	Medium
NSSLAs	-	Medium
Lending and Finance Companies	-	Medium
Non-bank e-money issuers	-	Medium
Casino	High	High
Lawyers & Notaries		Medium
Accountants		Medium
Dealers in Precious Metals		Medium
Company Service Providers		Medium
Real Estate		Medium

³³ 9 PAGCOR licensees and 1 PAGCOR operated

³⁴ 57 PAGCOR licensees and 27 CEZA licensees.

³⁵ This is not the total number of covered persons, rather the total that have been prioritised for registration with AMLC.

³⁶ Professional Regulatory Commission

³⁷ Businesses and trade associations. See IO.4 for individual covered persons total.

Anti-money laundering and counter-terrorist financing measures in Philippines @ APG 2019

Preventive measures

55. The AMLA contains the Philippines' AML/CFT preventive measure obligations, with the 2018 Implementing Rules and Regulations (IRR) (for all covered person except casinos) and 2017 CIRR (for casinos) prescribing the implementing rules and regulations. The AMLA and IRR/CIRR are enforceable means as per the FATF definition, and are supported by instruments issued by supervisors, as follows:

- AMLC – AML/CFT Guidelines for DNFBPs (Regulatory Issuance B(1)) - May 2018
- BSP – Manual of Regulations for Banks (MORB), updated November 2018; and Manual of Regulations for Non-Bank Financial Institutions (MORNBFII), updated November 2018
- SEC – 2018 Guidelines on AML/CFT for SEC Covered Institutions, issued November 2018
- IC – AML/CFT Guidelines for Insurance Commission Regulated Entities, issued September 2018, updated November 2018.
- PAGCOR – CDD Guidelines for Land Based Casinos 2018; and CDD Guidelines for Offshore Casinos (Feb 2019)
- CEZA – Memo Circular No. 18-001, adopting the Implementing Rules and Regulations of An Act Designating Casinos as Covered Persons” - the AML/CFT framework of CEZA casino licensees.

56. These rules and circulars are also enforceable means as per the FATF definition. Supervisors are only able to impose enforcement actions for violations of their own respective circulars and rules. Sanctions for violations of AML/CFT requirements not contained in a supervisor's respective rules and circulars may only be imposed by AMLC (including on referral from a supervisor).

57. While real estate agents are not subject to AML/CFT obligations, AMLC can require, under Section 7 of the AMLA, the Land Registration Authority (LRA) to submit reports to AMLC on all real estate transactions involving an excess of PHP500,000 (approx. USD 9500) within 15 days from the date of registration of the transaction. AMLC may also require the LRA and all its Registries of Deeds to submit copies of relevant documents of all real estate transactions.

Legal persons and arrangements

58. The different types, forms and basic features of corporations (including associations) are set out in the Corporation Code, and the Civil Code for partnerships, as are the processes for creating these types of legal persons. For cooperatives, the governing legislation, and detail on creation is contained within the Cooperative Code. The SEC website outlines the administrative steps and documents required to register a legal person with the SEC. Title V (Trusts) of the Civil Code sets out the basic legal framework and features of legal arrangements in the Philippines.

59. The Philippines has approximately 650,000 legal persons active and registered with the SEC (as at the end of December 2017), the most being domestic corporations (over 80%), followed by domestic partnerships and less than 1% registered as foreign entities. There are over 10,000 legal persons registered with SEC but not classified by SEC as domestic corporations, domestic partnerships or foreign entities.

60. The Philippines has not formally assessed vulnerabilities related to legal persons or arrangements with respect to abuse for ML/TF. However the 2017 NRA acknowledges that legal persons and arrangements are avenues for criminals to mask their true identity and that they pose a high ML/TF risk to banks and other covered persons.

Table 1.4: Registered Legal Persons (SEC) (as at 31 December 2017)

Type of Legal Person	
Stock Corporation	355,1990
Non-stock corporation	174,401
Partnerships – General	90,306
Partnerships – Limited	10,953
Partnerships - Professional	3,259
Domestic (Total)	634,109
Foreign stock corporations	4,031
Foreign non-stock corporations	251
Foreign partnerships	37
Foreign Entities (Total)	4,319
Unclassified elsewhere by SEC	10,782

61. Express trusts established under Philippines law are used for a range of purposes including: controlling and protecting family assets; passing on assets before or after death; or managing the assets of someone who is incapacitated or too young. It is not known how many private express trusts have been established in the Philippines. All business trusts must be formed and managed by trustee entities regulated by BSP. There are 39 such trustee entities, with over 80% of these being subsidiaries of banks. The BIR does not maintain any data on express trusts paying tax. Payment of appropriate tax is required by the BIR, however the BIR captures the conveyance transaction and not the (express trust) relationship between and among the concerned parties.

62. The Philippines reported that there were 101,843 registered NPOs in the Philippines as at 31 December 2017. The 2018 assessment of the NPO sector concluded that the overall risk of the Philippines NPO sector for TF abuse was low-medium. The assessment identified 32 NPOs for which there has been possible TF abuse.

Table 1.5: Non-Profit Organisation sector

NPO Classification	No of NPOs	% of total
Foundations (service/expressive NPOs)	11,734	11.5%
Religious organisations (service NPOs)	19,511	19.2%
Education providers (service NPOs)	13,139	12.9%
Other service NPOs (parent-teacher, livelihood & neighbourhood assoc.)	1,558	1.5%
Other expressive NPOs (political; environmental; alumni; cultural; sports)	2,984	2.9%
Not elsewhere classified	52,917	52%

63. Some organisations that can be characterised as NPOs are not registered with the SEC as there is no legal requirement to do so. The requirement to become registered as a NPO is linked to the ability to obtain legal personality to operate as a NPO, open a bank account and generate or raise funds. There is no accurate picture of the number of unregistered organisations. Authorities have detected cases of TF in relation to NPOs used to raise and channel funds to local terrorist groups in the southern province, however authorities note that this remains unconfirmed.

64. In addition to the registration of NPOs by the SEC to obtain a legal personality, regulatory functions in the NPO sector are also undertaken by the Department of Social Welfare and Development

(DSWD) and by the Philippine Council for NGO Certification (PCNC) in relation to NPOs seeking to conduct certain activities (e.g. social welfare and development, or certification of NPOs as charitable “donee” institution status).

65. In November 2018, SEC published new guidelines for the protection of registered NPOs from ML/TF. All NPOs are now required to establish a system that will enable them to know where their funds are coming from, who their beneficiaries are and where they are located. All NPOs must also ensure funds reach their target beneficiaries or that they are used for the purpose intended. NPOs must also report to SEC any fact that gives rise to a suspicion that it is being exploited for ML/TF.

66. Concerns have been raised in civil society regarding the multiplicity of requirements across the SEC, DSWD and PCNC, and the burden of the requirements imposed by the SEC 2018 Guidelines. It is notable that the mandatory disclosure imposed by SEC under the Guidelines is a one-time disclosure to capture baseline data on various aspects of NPO sectors.

Supervisory arrangements

67. The AMLA, 2018 IRR and the CIRR empower the BSP, SEC, IC, PAGCOR, CEZA, APECO and AMLC as AML/CFT supervisors. Table 2 above sets out the regulator and supervisor/s of each sector.

68. The banking and some NBFIs sectors (including MSBs) are regulated and supervised by BSP, both for prudential and AML/CFT compliance.

69. The SEC regulates and supervises the securities sector and commenced AML/CFT supervision of securities brokers in 2018. The Capital Markets Integrity Corporation (CMIC), a self-regulatory organisation, is tasked by the SEC to conduct periodic examination of broker dealer firms to determine compliance with relevant laws, including the AMLA. The SEC also regulates and supervises lending and financing companies for AML/CFT compliance.

70. The IC regulates the insurance sector. IC commenced AML/CFT supervision in 2015.

71. PAGCOR, APECO and CEZA perform licensing and operational regulation and/or supervision over casinos while AML/CFT obligations are co-supervised by AMLC. PAGCOR is a government-owned corporation which has the power to grant licenses to private casino operators, except those under the jurisdiction of CEZA or APECO. In addition to its role as supervisor, PAGCOR owns and operates its own casinos in the Philippines, which presents potential for a conflict of interest. CEZA is a government-owned and controlled corporation which has the legal authority to approve casino licence applications within its economic zone. Casino gaming is regulated by CEZA through its master licensor. APECO is authorised to license gaming within its freeport. APECO has not yet issued any gaming licences.

72. AMLC is responsible for overseeing compliance by DNFBPs, including co-supervision of casinos and BSP supervised trust entities. However AML/CFT supervision of sectors other than casinos (lawyers, accountants, jewellery dealers, dealers in precious metals and stones and company service providers) has not properly commenced as the Guidelines for DNFBPs only took effect on 29 June 2018. There is no designated authority responsible for AML/CFT monitoring and ensuring compliance for the real estate sector as it is not covered under AMLA.

73. Pursuant to the IRR/CIRR, covered persons must register with AMLC for the purpose of submitting CTRs and STRs. There has been a steady increase in the number of FIs registered with AMLC for the purpose of reporting. However, as at the time of the onsite visit a very low number of DNFBPs had registered with AMLC (all land based casinos, four online casinos, two jewellers, one CSP and two

accounting firms), noting that DNFBPs (except casinos) had until 29 December 2018 to register, while casinos were required to be registered by August 2018.

International Cooperation

74. The main proceeds-generating crimes identified by the Philippines' NRA are all transnational in nature. With a vast maritime border, the Philippines' archipelago presents a risk for predicate crimes and ML/TF generally. The porous southern borders of the Philippines have been exploited by terrorist elements, and present a continuing vulnerability.

75. In addition to its location, connected by well frequented marine routes, the Philippines is also connected to an extensive diaspora spread across the globe. It is considered one of the largest in the world and spans over 100 countries. In particular, there are large populations of foreign workers from the Philippines in the United States, Canada, and the Middle East. This presents risks particularly in the flow of remittances, which some sources estimate to be considerably higher than formal figures due to the use of illegal channels.

76. The DOJ, the Philippines' central authority, is responsible for MLA and extradition. AMLC and BIR also have the ability to respond to MLA requests. The BIR is the central authority for MLA requests with respect to tax offences and taxation related matters. While the Philippines has had modest formal international cooperation relating to ML/TF, it has access to a wide range of informal and other mechanisms to cooperate internationally on criminal issues relevant to ML/TF.

CHAPTER 2. NATIONAL AML/CFT POLICIES AND COORDINATION

Key Findings and Recommended Actions

Key Findings

10.1

- 1) The Philippines has reasonably assessed a range of its ML/TF risks in iterations of national risk assessments (NRAs), serious and organized crimes threat assessments (SOCTAs) and various stand-alone risk assessments or strategic analyses such as for NPOs, virtual currency, external threats and cross-border fraud, tactical analysis and regional assessments on TF (including foreign terrorist fighters (FTF)), though some gaps remain.
- 2) The understanding of ML and TF risk varies amongst stakeholders, but is strongest in AMLC, which is the primary LEA responsible for ML/TF investigations. LEAs' understanding of overall risk is reasonable.
- 3) There are weaknesses with the assessments of and understanding of transnational aspects of ML. The NRA assessment of TF risks recognised the use of cash couriers/bulk cash smuggling and remittance agents, but it did not sufficiently take into account transnational threats, including the presence and movement of FTF into and out of the Philippines. However, the authorities' understanding was updated and supplemented by the regional tactical analysis of the Maute financial network and regional assessments.
- 4) Although some assessment was undertaken in the NRA and other thematic assessments, the ML/TF vulnerabilities of legal persons/ legal arrangements, inter-linkages between covered persons and crimes, external threats/ foreign proceeds and the vulnerabilities of the cash economy are not fully understood.
- 5) The National AML/CFT Strategy (NACS) is broadly in line with identified risks. Given its recent formulation, the action plans were at various stages of implementation at the time of the onsite visit. Some of the recommended actions in the MER are in line with the NACS.
- 6) The National Law Enforcement Coordinating Committee (NALECC) has various operational coordination committees including a sub-committee on AML/CFT and others covering predicate offences. However, the policy coordinating platform for monitoring NACS implementation – the National AML/CFT Coordination Committee (NACC) – was only recently established. The Joint Terrorism Financing Intelligence Group (JTFIG) and bilateral case conferences demonstrate successful cases of operational coordination. However, the multiple and similar coordination mechanisms potentially have a duplicative effect.
- 7) There is limited demonstrated cooperation and coordination on PF, although PF issues have been occasionally discussed in the NALECC Sub-Committee on AML/CFT.
- 8) AMLC's objectives and activities align with the risk profile. With the exception of drugs and corruption, the alignment between other LEAs' objectives and activities and identified ML/TF risks is still developing. Objectives set by supervisory and regulatory authorities respond to identified risks and align, to a certain extent, with the risks identified in main sectors such as

banking and MSBs,. The implementation of action plans by supervisory and regulatory agencies across all sectors has not yet occurred.

- 9) Based on the risks identified in the NRAs, competent authorities have instituted limited enhanced and some simplified measures (particularly to balance financial inclusion with AML/CFT obligations) for some sectors. The Philippines recognises and understands financial inclusion products and financial exclusion may be a source of vulnerability and has taken concrete and effective steps to address such vulnerabilities.
- 10) Private sector stakeholders are aware of the results of the NRAs, with the understanding and response to risk more developed amongst FIs than DNFBPs. Casinos have an awareness of transactional risks, but awareness of ML/TF risks within other DNFBPs in general is still developing.

Recommended Actions

- a) Update the assessments of TF risks to enhance the understanding of emerging TF typologies, TF associate with significant recent terrorism-related events, TF associated with the role of foreign fighters, and the impact of the Philippines' governmental / military responses to TF networks and transnational flow of funds for TF.
- b) Enhance understanding of specific areas of risks (crime-specific threat assessments, transnational movement of proceeds of crime, misuse of legal persons and legal arrangements, interrelatedness of crime types and sectors and external threats/ foreign proceeds of crime) and vulnerabilities of the cash economy, and at the same time continue to understand emerging risks (e.g. financial technologies) and take appropriate mitigating actions.
- c) Continue to implement and monitor the implementation of the action plans under the NACS, including operationalising the newly established NACC and its sub-committees to ensure their effectiveness and appropriate prioritisation.
- d) Continue efforts to align LEAs' objectives and agency-level action plans with identified ML/TF risks. Prioritise implementing those agency-level action plans. Review the pre-existing coordination committees and clearly demarcate the areas of focus between NACC and its sub-committees and other coordination committees.
- e) Consider the participation of AMLC in the ML High Risk Crimes sub-committees under the NALECC, of which it is not currently a member.
- f) Enhance government agencies' and the private sector awareness of the Philippines' ML/TF risk through further outreach and awareness raising activities.
- g) Ensure the NACC TF/PF sub-committee operates as a mechanism for effective coordination on PF issues.

77. 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 R1-2.

Immediate Outcome 1 (Risk, Policy and Coordination)

2

*Country's understanding of its ML/TF risks**ML risk understanding*

78. The Philippines has reasonably assessed many of its ML risks through two NRAs (the 2015 NRA covering 2011-2014 and the 2017 NRA covering 2015-2016), SOCTAs in 2013, 2014 and 2016 and other stand-alone risk assessments. The 2017 NRA is a forthright document that identifies various factors contributing to ML/TF risk in the Philippines. The NACS contains an action plan to periodically update the NRA from 2018.

79. Agency and private sector understanding of risks has been developed by involvement in developing and sharing the results of various risk assessments. The NRA process was largely driven by AMLC through the NRA Working Group, which consisted of 32 government agencies, 15 private sector representatives and nine industry associations. The Working Group considered quantitative and qualitative data and involved benchmarking at the national level.

80. The NRAs drew on many of the relevant public and private sector stakeholders. For the 2017 NRA in particular, the cumulative effect of various sectoral assessments by respective working groups, which consisted of relevant supervisors, added depth to the assessment.³⁸ While some private sector stakeholders were not involved in the consultative process leading up to the 2017 NRA (mainly DNFBP representatives), this did not appear to have a significant impact on the overall findings of the NRA process based on the availability of other data and onsite inputs by the sectors' representatives.

81. The level of understanding of its ML/TF risks is stronger amongst FIs than DNFBPs. Sectoral risk assessments for the banking, insurance and securities sectors contains more detail on elements such as the quality of AML supervision, commitment and leadership management, quality of AML policies and procedures, compliance level of staff, quality of AML/CFT framework, quality of AML controls and product vulnerability. In addition, in-depth analysis (in both NRAs) on financial inclusion products has usefully been undertaken.

82. The 2017 NRA considered both inherent risks and AML/CFT mitigating controls in determining the risk rating in relation to both threats and sectoral risks, unlike SOCTAs which focussed mainly on threats. The 2017 NRA used an improved methodology (compared to the 2015 version), a widened scope of threats, inputs from sectoral assessments and the inclusion of a more detailed assessment of TF.

83. Gaps in data availability were recognised in the 2015 NRA, however these gaps remained unresolved in the 2017 NRA. Both NRAs and the SOCTAs noted the challenges of data availability³⁹ including data not being up to date, limitations in information sharing between agencies, unavailability/uncaptured data (e.g. proceeds of crime data not captured in relation to kidnapping for ransom) and manual/non-centralised databases. These gaps were somewhat mitigated through the assessment of qualitative information, including surveys and other literature, as well as expert interviews and

³⁸ The risk ratings derived for DNFBPs are not comparable as these DNFBPs underwent different strategic risk assessments in the 2015 and 2017 NRAs. In the 2015 NRA, DNFBPs were assessed based on the inherent risk on services DNFBPs provide. Meanwhile, in the 2017 NRA, DNFBP assessment focused on the sector's vulnerability to ML.

³⁹ Various sources of quantitative data were used including STRs, CTRs, cases investigated, prosecuted, forfeiture and other literature sources.

national validation workshops. An action plan designed to fill the gap in the availability of quantitative data is set out in the NACS.

84. SOCTAs soundly identify trends and emerging risks with serious crime, gaps in the current frameworks and priority areas along with relevant recommendations for specific risks/gaps identified. The SOCTAs predate the NRA process, and also include an assessment of ML and the nexus between serious crimes and overall security concerns. SOCTAs are driven by the NALECC Sub-Committee on Organized Crime, which consists of more than 30 agencies. Other agencies and relevant NGOs were also consulted a part of the process. The SOCTA 2016 reviewed the findings and validated the 2013 and 2014 SOCTAs. SOCTAs are not public documents, rather they are used by LEAs and relevant agencies to formulate strategies and action plans in their respective areas. Some findings from SOCTAs on specific crime features and typologies were taken into account in the NRA analysis.

85. The NRAs assessed ML and TF threats to be of medium-high level overall, as a result of a high level of threats and a medium level of vulnerabilities. The threat from foreign proceeds of crime for ML is assessed to be high. The assessment team believes these conclusions are reasonable. Based on the meetings held during the on-site, these conclusions and understanding appear to be consistent across stakeholders. For the predicate crimes that remain high risk for ML, LEAs generally agree that the level of risks did not change much throughout the iterations the NRAs and SOCTAs.

86. The assessment team broadly agrees with the authorities that the main threats faced by the Philippines include the laundering of proceeds from drug trafficking, corruption, investment fraud, smuggling, tax crimes, copyright/intellectual property violations, illegal firearms and environmental crimes. Overall, the authorities' responses to the higher risk crimes, including intelligence shared as well as investigations, prosecutions and confiscation are generally low (see IO.6, 7, 8 and 9).

87. While the NRA did not rank kidnap for ransom and cybercrime amongst the highest risks (rated medium in the NRA), the authorities' responses to these crime types suggest that they are also high threats. The assessment team took note that kidnapping for ransom was assessed separately for ML (medium) and TF (high), where kidnapping for ransom is predominantly used, while cybercrime risk perception was also elevated due to the Bangladesh Bank Heist.

88. In terms of ML vulnerabilities, assessments highlight higher risks associated with MSBs, pawnshops (with corollary businesses), e-money issuers, company service providers and the casino sector. These findings appear reasonable. Despite the NRA assessing banks⁴⁰ as having net medium risk (the same level as the securities and insurance sectors), the Philippines' supervisory response and demonstrated understanding to this sector appears to be in line with a higher inherent risk rating in comparison to securities and insurance sector. For DNFBPs, more emphasis was given to the sectoral vulnerabilities (inherent risk) in the 2017 NRA. ⁴¹

89. While some elements of transnational ML risks was assessed, these ML risks are not comprehensively understood. The Bangladesh Bank Heist demonstrated the interconnectedness of the vulnerabilities of the FI and DNFBP sectors. Given the risk and context of the Philippines, particularly the interconnectedness of sectors, threats and linkages to foreign jurisdictions, this is a deficiency. Further, the assessment team finds that there is a need for enhanced understanding of the vulnerabilities of the cash-based nature of the Philippines' economy. The SOCTAs, which predate the

⁴⁰ The medium net risk for banking sector to medium risk rating assigned to the quality of AML control, despite the sector high inherent risk vulnerabilities.

⁴¹ There are five ratings assigned for 2017 NRA, i.e Low, Medium Low, Medium, Medium High and High. While for 2015 NRA, the ratings assigned are Low, Medium Low, Medium, Medium High, High and Very High
Anti-money laundering and counter-terrorist financing measures in Philippines © APG 2019

Bangladesh Bank Heist, recognise the interrelation between some serious crimes and organised nature of those crimes. To mitigate the lack of information on the interconnection of external threats and sectors, AMLC undertook a study⁴² seeking to understand the external threat posed generally by considering the inflow and outflow of illicit funds based on international cooperation requests and relevant STRs. It is also found that fraud, narcotics and tax crimes posed a high level of external threat.

Table 2.1: ML Rating for Threats under First and Second (2017) NRA

CRIME	1st NRA 2011 - 2014	2nd NRA 2015 - 2016
Tax Crimes	NA	HIGH
Smuggling	HIGH	HIGH
Violations of intellectual property rights	HIGH	HIGH
Illegal manufacturing and possession of firearms	HIGH	HIGH
Violation of environmental laws	HIGH	HIGH
Investment scams/ fraud (fraud)	HIGH	HIGH
Illegal drugs-related crimes	HIGH	HIGH
Plunder and corruption	HIGH	HIGH
Web-related crimes	NA	MEDIUM
Illegal trafficking of persons	HIGH	MEDIUM
Kidnapping for ransom	NA	MEDIUM
Others	NA	LOW

Table 2.2: Sector Net Vulnerabilities Ratings under the First and Second NRA

SECTORS	1st NRA 2011 - 2014	2nd NRA 2015 - 2016
Banking Sector	MEDIUM	MEDIUM
Securities Sector	MEDIUM	MEDIUM
Insurance Sector	MEDIUM	MEDIUM
NBFI	MEDIUM (assessed based on products)	MEDIUM HIGH
		MEDIUM HIGH
		MEDIUM
		MEDIUM
		MEDIUM
DNFBP	VERY HIGH	HIGH
	MEDIUM HIGH	MEDIUM
	MEDIUM HIGH	MEDIUM
	MEDIUM	MEDIUM

⁴² A study on Strategic Analysis on Cross-border Investment Fraud (CBIF): A study of cross-border investment fraud involving the Philippines as a destination of proceeds from crime and money laundering activities undertaken in 2015.

Accountants	MEDIUM	MEDIUM
Trusts	MEDIUM LOW	Assessed under banking
Company Service Providers	MEDIUM	MEDIUM
Car Dealers	MEDIUM HIGH	MEDIUM

90. The findings of the 2017 NRA with have been supplemented by other risk assessments, some of which form part of the strategic analysis work of AMLC. This has included: (a) a preliminary assessment of the transaction profile of accredited virtual currency exchanges, particularly in relation to suspicious transactions, clients with suspected links to illicit activities, and large transactions (June 2018); (b) strategic analyses of cross-border fraud and pawnshops/MSBs (November 2018); (c) assessment of the development of AML reporting compliance of the pawnshop and MSB industry(November 2018); (d) an NPO assessment (November 2018); and (e) data mining exercises. These additional, specific risk assessments add to the overall understanding of risk.

91. The 2017 NRA assessed some elements of risks of legal persons including company service providers and some trust products offered by BSP-supervised FIs. The 2018 NPO assessment also considered certain legal persons. The understanding of the vulnerabilities of legal persons and arrangements in posing ML/TF risk, beyond acknowledgement that they present avenues for criminals to hide their identity and pose a high risk to covered persons, was not demonstrated (see IO.5).

TF risk understanding

92. Authorities have conducted reasonable assessments of TF risk, however understanding of TF risk is mixed across agencies. In the 2017 NRA, the Philippines classified both terrorism and TF as high risk, given the high number of violent incidents associated with terror/threat organisations. Terrorist organisations or groups posing threats related to terrorism are acknowledged as having a systematic and established method of raising funds for their operations predominantly through proceeds of certain offences, with kidnap for ransom and extortion as the main source of TF. Proceeds from kidnapping for ransom is mainly undertaken through bulk cash smuggling with some cases involving bank deposits. While the total amount raised by these terrorist organisations remains unknown, competent authorities accept that the groups are well funded. The authorities have assessed that cash transactions, including the use of cash couriers, remain the preferred mode for transfer of value for Philippine terrorist/threat organisations. Remitters are also used for funds transfers, especially from abroad.

93. The 2017 NRA noted the use of legitimate funds for TF through the abuse of NPOs, family funding and legitimate business fronts. Funds derived from both illegal and legal sources were thought to have been used for the purchase of arms, vehicles and to support the communities wherein terrorist/threat groups operate. The 2018 NPO assessment recognised risks of TF abuse of the NPO sector as medium-low and noted particular vulnerabilities. These included the diversion of funds to support terrorist entities and affiliates; and NPOs knowingly or unwittingly providing logistical support to terrorist/threat groups. NPOs that are likely to be abused include those with charitable, social development, humanitarian disaster relief or educational activities (see IO.10 for further information).

94. The Philippines assessment of TF risks under the NRA had not fully assessed the threat of foreign terrorist fighters (FTF), including the risks of such fighters travelling to the Philippines (see Chapter 1 for context). However, relevant authorities' understanding was updated and supplemented by tactical analysis conducted on the Maute Group (and related groups), undertaken under the multilateral analyst exchange programme and by regional TF assessments under the South East Asia

Counter Terrorism Financing Group⁴³. These contributed to further understanding of the risk posed by certain aspect of foreign fighters, and provided a regional comparison. Philippine authorities have instituted measures to address these risks. Given the risk and context of the Philippines and the escalation of terrorist activity in Mindanao, including the 2017 Marawi Siege that led to a military response, the Philippines' understanding of TF needs to be further updated.

Case Example 2.1: Southeast Asia Counter-Terrorism Financing Working Group Regional TF Assessment

In 2018 the Southeast Asia Counter-Terrorism Financing Working Group (SEACTFWG) of the Financial Intelligence Consultative Group produced a comprehensive study on ISIL and Regional TF in response to ISIL's increased influence in the region and the need to understand how ISIL and ISIL-affiliated groups fund their activities. The study consisted of four thematic reports: 1) 'ISIL's Financing in Southeast Asia: The Regional Environment', led by Australia; 2) 'External Funding to ISIL Southeast Asia', led by Indonesia; 3) 'Self-Funding of ISIL Southeast Asia', led by the Philippines; and 4) 'Hawala Dealers Financing of ISIL and Other High Threat Terrorist Organisations in Southeast Asia', led by Malaysia.

The methodology comprised questionnaires disseminated to SEACTFWG members, who gathered quantitative and qualitative data from relevant stakeholders (i.e. military/intelligence/law enforcement agencies, supervisors, private stakeholders), and considered financial intelligence, regulatory data, classified and open source information. Two workshops were conducted (in Jakarta in April 2018 and in Brunei Darussalam in August 2018), where the results of the survey were jointly analysed to form key judgements.

AMLC led the examination of ISIL-SEA's modes of self-funding and the disruption strategies in place. The report considered ISIL-affiliated organisations, attacks perpetuated, statistical data (i.e. intelligence reports, investigations, freezes, and inquiries), methods for raising funds, trends and context, channels, vulnerabilities and case studies. The study found that self-funding methods include (i) criminal means, such as kidnapping for ransom, extortion from the local population and drug trafficking or smuggling and (ii) self-funding through legitimate sources, such as family support, sympathisers' donations, business profits and legitimate income. Members of the SEACTWG agreed to collaborate on priority targets to develop disruption strategies, which may be done through analyst exchange programs; and work with LEAs or regional agencies to implement these strategies.

The 2018 study complemented the 2016 Regional Risk Assessment on TF, noting the impact of the 2017 Marawi siege in the Philippines.

In addition to the study, tactical Maute Network Analysis⁴⁴ was undertaken to identify and understand the financial networks and interaction of terrorist groups within the region, through both legal and illegal means. This included the use of remittance, the NPO sector and physical cash movements into and out of the Philippines, which uncovered previously unknown financiers/ facilitators and foreign terrorist fighters. The findings of the analysis were widely shared and validated by the relevant Philippines authorities.

⁴³ Both under the auspices of the regional Counter Terrorism Summit/ Financial Intelligence Consultative Group founded by AUSTRAC and PPATK, which members include FIUs in the SEA region.

⁴⁴ The Maute Network Analysis was a collaboration of analytical and investigative effort by the FIUs in Indonesia, Malaysia, Australia and the Philippines. This analysis including coordination with relevant law enforcement agencies.

95. There is a need to enhance the understanding of the transnational movement of funds related to FTF and other terrorist activities. Despite the high number of threat incidents and the estimated amounts raised by the terrorist/threat groups, STRs submitted by covered persons on TF remain low, however has improved in recent years, and the total amount frozen compared to the estimated amounts raised is minimal. These gaps, as recognised in the NRA, and are attributed to the focus of intelligence gathering on terrorism and not TF.

National policies to address identified ML/TF risks

96. Following the 2015 NRA, several mitigation measures were implemented in response to threats and vulnerabilities identified in the NRA. These included requiring banks to adopt sound risk management practices for dealing with clients engaged in MSBs (identified as a high risk sector), increasing the number of analysts within AMLC, giving BSP explicit authority to supervise and regulate electronic money issuers, credit card companies and money transfer operators, and implementing a new licensing framework for pawnshops.

97. There was no specific national policy in relation to AML/CFT matters prior to late 2018. A national-level policy framework was developed over a number of years, taking into account the findings of two NRAs and other assessments. The National AML/CFT Strategy (NACS) NACS was approved in June 2018, with relevant agencies commencing implementation from that time. The NACS was formally adopted in November 2018, immediately prior to the onsite visit, to cover the period of 2018-2022.

98. The NACS, is a comprehensive AML/CFT policy document, and many of the action plans set out in the NACS are aligned with the risk aspects identified in the 2017 NRA. Examples include plans to strengthen the border control for cash and other instruments, strengthening of terrorism and TF investigative powers in relation to exploitations of cyberspace, increase / update MOA between higher risk crime agencies, improving casino and MSB supervision, expanding the scope of the National Intelligence Committee to include a focus on TF, conducting targeted outreach on high risk crimes (i.e. corruption, terrorism and TF) and monitoring emerging risks associated with technology.

99. Since the approval of the NACS in June 2018, key government agencies have started implementing their respective actions plans. At the time of the onsite, Philippines authorities reported that approximately a quarter of the action plans had been adopted by the relevant agencies with varying levels of implementation.

100. Certain NACS action plans items are within the purview of pre-existing mechanisms, and have improved effectiveness in mitigating identified risks or addressing scope gaps in the Philippines' AML/CFT measures. Some completed action plans items include:

- passing of the Philippines Identification System Act for a single reliable ID (to address KYC challenges);
- requiring casinos to apply a risk-based approach to AML/CFT based on the NRA findings;
- issuing CDD regulations for land-based casinos;
- approving an information exchange portal for AMLC and direct access to MOA by AMLC; and
- establishing an information sharing protocol for a public-private partnership programme.

101. The NACS requires all action plans to be reviewed in 2020, or earlier if circumstances warrant, so that all action plans remain updated and relevant. This is complementary to the plan to conduct periodic review of the NRA.

Exemptions, enhanced and simplified measures

2

102. The Philippines has implemented some enhanced and simplified measures, in response to identified risks. Based on the findings of the 2015 NRA, stand-alone MSBs are recognised as high risk, which prompted enhanced measures to be applied to MSBs, including the imposition of mandatory registration.⁴⁵

103. The previous supervisory framework for MSBs (which included registration and limited AML/CFT supervision) identified vulnerabilities of MSBs, and was strengthened by BSP adopting measures in 2017 and 2018⁴⁶ to address the vulnerabilities. The amended registration requirements and supervisory framework of the sector (see IO.3 for further details on the MSB re-registration process and new supervisory framework). Based on the 2015 NRA, BSP issued a memorandum⁴⁷ to remind banks to take extra caution and vigilance, and conduct enhanced due diligence (EDD) when dealing with MSBs. In addition, the banks must conduct an assessment of risk on their MSB clients. This was further strengthened by a memorandum issued in 2017⁴⁸ requiring banks to obtain the BSP licence of all MSB customers in order to continue business relationships.

104. Guidance in relation to high-risk sectors has also been provided to banking institutions to support application of appropriate EDD and vigilance. This includes a memorandum issued to banks on sound risk management practices in dealing with customers engaged in gambling.⁴⁹

105. Authorities have implemented some simplified measures to improve financial inclusion. This includes products in the MSB and rural bank sectors. Since higher ML/TF risks have been identified in the MSB sector, more detailed assessments of financial inclusion products have been included in both NRAs. In essence, the Philippines seeks a balance between financial inclusion and ML/TF risk mitigation and management in line with BSP's strategic goals in the promotion of financial inclusion. For example, the BSP issued a circular⁵⁰ which requires all BSP covered persons, including MSBs, to formulate a risk-based and tiered customer acceptance, identification and retention policy that involves reduced CDD for potentially low risk clients and enhance CDD for higher risk accounts.

106. The lack of inclusion of the real estate sector as covered persons is a gap in the legal framework rather than a risk-based exemption.⁵¹

Objectives and activities of competent authorities

107. Some supervisory activities have been implemented to respond to identified risks. These include the enhanced measures taken in the course of mandatory re-registration of MSBs with BSP and the requirement to register with AMLC for reporting by 30 April 2018. At the end of the onsite, a total of 937 out of 1,621 MSBs had registered. While BSP has commenced work to identify MSBs which are operating without a licence, enforcement actions should be undertaken to ensure that non-registered MSBs do not continue to operate. Circulars were issued to pawnshops operators requiring notification to BSPs on changes in operational processes and compliance with the AML/CFT requirement. BSP also

⁴⁵ BSP Circular no 471, dated 24 January 2005

⁴⁶ BSP Circular No. 942, dated 20 January 2017, and subsequent BSP memoranda No 2017-2014 (15 March 2017), BSP Memoranda 2017-015 (15 March 2017) and BSP Memoranda No 2018-030 (2 October 2018)

⁴⁷ Memorandum No. M-2016-004 and M2017-009

⁴⁸ Memorandum No.2017-009)

⁴⁹ Memorandum No. M2018-002

⁵⁰ BSP Circular No. 950

⁵¹ There is a pending bill (Senate Bill 1256) to amend the AMLA to include real estate as covered persons.

adopted network-based supervision for pawnshops and MSBs that are systematically connected. This has resulted in at least 80% of total pawnshops industry assets being examined by BSP.

108. The alignment between LEAs' objectives and activities and identified ML/TF risks is still developing. Actions undertaken by LEAs which demonstrate an improved alignment of objectives/activities with national AML/CFT policies and ML/TF risks include the following:

- a. *Drugs*: 2017 expansion of the financial investigation team; designation of 17 financial investigation officers in 17 PDEA regional offices; and integration of the AMLA into the PDEA manual.
- b. *Corruption*: the 2014 SOCTA identified a lack of transparency of government documents as a source of vulnerability. In response, Executive Order No. 2 (2016) requires agencies under the Executive Branch to make available public records, contracts, transactions and any information requested by the public, except for matters affecting national security. In addition, the prescriptive period for violations of the Anti-Graft and Corrupt Practices Act was increased from 15 years to 20 years.⁵²
- c. AMLC reorganised its staffing and structure, implementing separation and specialisation between financial intelligence and investigation. Investigation teams focused on TF, drugs, corruption and fraud were created. Guidelines were issued for the digitalisation of customer records for AMLC investigation purposes.

National coordination and cooperation

109. There is a wide array of AML/CFT coordination and cooperation structures in the Philippines. This has benefits in terms of operational cooperation, which have had some success including providing platforms for the NRA and SOCTA processes and the NACS. Philippines authorities established the streamlined NACC, when the NACS was adopted in November 2018.⁵³

110. The NACC is chaired by the Executive Secretary of the Philippines⁵⁴, with the BSP Governor the Vice-Chair, and consists of 11 other high level government officials⁵⁵. The Committee is supported by AMLC as its Secretariat, and it has mandated AMLC as the focal point of the AML/CFT regime. The NACC has five sub-committees which consist of supervisory/ regulatory authorities, law enforcement and policy-making agencies and meet quarterly. These committees may invite any other agencies to attend when necessary. As at the time of the onsite visit, the sub-committees had not yet convened, meaning no determination could be made about their impact on effective AML/CFT coordination.

111. Prior to this, coordination in relation to predicate offences and AML/CFT was conducted through the NALECC, either periodically or on an ad-hoc basis, and through a series of independent and/or ad hoc mechanisms that operated in isolation. NALECC has 59 permanent member agencies and 18 sub-committees. The main functions of NALECC are: a) to coordinate policies/ procedures to facilitate cooperation and integration of effort; b) identify priority areas for coordinated/joint law

⁵² Republic Act No. 10910,

⁵³ See Chapter 1 for further details on the NACC

⁵⁴ The Executive Secretary is the head and highest ranking official of the Office of the President.

⁵⁵ Secretary of Foreign Affairs, Secretary of Finance, Secretary of Justice, Secretary of National Defence, Secretary of the Interior and Local Government; Secretary of Trade and Industry, Securities and Exchange Commission Chairperson; Insurance Commissioner, Chairperson of the Philippine Amusement and Gaming Corporation, Administrator of the Cagayan Economic Zone Authority, and President of the Aurora Pacific Economic Zone and Freeport Authority

Anti-money laundering and counter-terrorist financing measures in Philippines © APG 2019

enforcement activities; and c) provide recommendations on LEA issues to the Chairman of Peace and Order Council (POC).

2

112. Some relevant outputs resulted from this coordination mechanism, with the most notable being the SOCTAs. One of the 18 sub-committees under NALECC is the Sub-Committee on AML/CFT, chaired by the Executive Director of the AMLC Secretariat. It meets on a monthly basis and is comprised of 35 member agencies. The Sub-Committee has had some success in passing resolutions that have resulted in operational outcomes, such as the motion to establish a national ID system, installation of scanning machines at the international airports, and sharing of risk information for anti-terrorism and anti-cybercrime campaigns.

113. AMLC also participates in other sub-committees of the NALECC, namely: Sub-Committee on Dangerous Drugs and Controlled Chemicals, Sub-Committee on Intelligence Coordination, Sub-Committee on International Law Enforcement Cooperation and Sub-Committee on Organized Crime, which enhance sharing of financial intelligence and requests for information in support of predicate crime investigations. AMLC could consider participating in other high ML risk crime committees, such as the Sub-Committee on Financial Fraud, Tax Evasion and Currency Violation and the Sub-Committee on Cyber Crimes.

114. LEAs meet at regularly scheduled or ad hoc meetings or case conferences (referred to as 'workshops') on specific operational matters, with successful results demonstrated from the case conferences between PDEA-AMLC (see IO.6). In addition, coordination relating to terrorism also occurs through the Anti-Terrorism Council (ATC) and Joint Terrorism Financing Intelligence Group (JTFIG), and coordination relating to drugs occurs through the Inter-Agency Committee against Drugs (ICAD).

115. In relation to terrorism and TF, the NRA recognised that domestic coordination should be further strengthened. To address TF risks and to strengthen support given to intelligence/security agencies, the Task Force on Terrorism and Terrorism Financing (TFTF) was established within the AMLC Secretariat in 2017. The primary function of the TFTF is to centralise coordination and collaboration efforts in combating terrorism and TF with other government agencies, particularly the National Intelligence Coordinating Agency (NICA), Intelligence Service of the Armed Forces of the Philippines (AFP), Philippine National Police Intelligence Group (PNP-IG), National Bureau of Investigation (NBI), and JTFIG. Another relevant coordination structure is the National Peace and Order Council (NPOC) Secretariat, which includes the Department of Interior and Local Government (DILG) and the Bureau of Immigration (BI). This Secretariat is entrusted to implement specific measures to combat terrorism, which include monitoring and preventing the illegal entry of foreign nationals into the Philippines for the purpose of terrorism.

116. Overall, these specific coordination platforms garner better results in terms of terrorism and drugs investigations, compared to other higher risk crimes.

117. Prior to the recent establishment of the Supervision of Financial Institutions Sub-Committee (SFISC) under the NACS, the Financial Sector Forum (FSC) comprised of BSP, SEC, IC and the Philippine Deposit Insurance Corporation and met monthly. Given its focus on FIs, not all DNFBP supervisors were included in this mechanism. The forum served as a platform for harmonisation and coordination of supervisory/regulatory methods and policies, reporting and information exchange, and undertaking consumer protection and education initiatives.

118. MOAs are in place between AMLC and supervisors for the exchange of information to aid supervisory activities in relation to higher risk sectors, such as banking and MSBs, to support risk-based supervision (see IO.3).

119. Although Weapons of Mass Destruction (WMD) issues have occasionally been discussed at the NALECC sub-committee on AML/CFT, matters relating to related TFS were not clearly discussed. The ATC Project Management Centre has organised ad-hoc meetings with DFA, DTI-STMO, AMLC and BOC to discuss implementation of DPRK-related UNSCRs. There is now a sub-committee on TF/PF under the NACS, but its effectiveness was not demonstrated given its recent establishment. It is noted however that there is a lack of operational and financial supervisors in its membership. While the NACC may invite any agency to sub-committee meetings, clear and standing mechanisms for cooperation and coordination on PF are not apparent in the newly established NACS. Cooperation and coordination on PF through the NALECC was not demonstrated, despite the relevant agencies being part of the coordination committee.

Private sector's awareness of risks

120. The findings of the two NRAs were widely shared with the private sector, through participation in the risk assessment exercise, awareness raising activities and via distribution of the reports via the AMLC website. AMLC has delivered multiple workshops and conferences to covered persons to disseminate the NRA findings. Across the Philippines workshops have been held for FIs, particularly banks and MSBs, delivered by AMLC in association with BSP and industry associations. Some supervisors have also discussed the NRA findings with covered persons during onsite supervisory visits. AMLC also publishes other assessments, such as the 2018 NPO assessment, strategic analysis reports by the FIU, and the quality of STR review.

121. Many FIs and DNFBPs appear generally familiar with the results of the NRA, with many having been involved in the process. Some sectors which were not part of the consultation during the 2017 NRA indicated that they wished that their sector was rated at a lower risk, but generally agreed with the reasonableness of the overall findings. However, it is also noted that since a specific risk assessment in relation to legal persons and legal arrangements has not been undertaken, there may not be a comprehensive understanding of risks in the corresponding DNFBP sectors, i.e. lawyers and TCSPs.

Overall conclusions on effectiveness with Immediate Outcome 1

122. The Philippines has reasonably assessed its ML risk through various iterations of risk assessments (NRAs or other assessments) which have drawn from the data and experience of multiple stakeholders. Further, the understanding of risk has been supplemented by various topical risk assessments. The Philippines has conducted reasonable assessments of TF risk, however understanding of TF risk is mixed across agencies, but strongest in AMLC as the primary ML/TF investigation agency. The assessment of risks with respect to terrorism and TF in relation to FTF was not assessed in the NRA, however the understanding of TF risk, including of the Philippines FTF risks, is supplemented and updated by tactical analysis and regional TF assessments. Responses to the identified risks vary across competent authorities, with weaknesses noted in responses to ML/TF risk in LEAs. There is a long standing and wide array of coordination committees and mechanisms, including the NALECC, with some success seen in operational case conferences, specific risk mitigation action plans and the provision of platforms for key national outcomes, such as the NRAs, SOCTAs and NACS. The multiple mechanisms are potentially duplicative, which may be mitigated with clear demarcation of roles. While the NACC and implementation of NACS has the potential to further improve coordination, its full impact could not be ascertained at the time of onsite visit given its recent implementation. Large segments of the private sector appear to be aware of the results of the risk assessments.

123. The Philippines is has a substantial level of effectiveness for Immediate Outcome 1.

CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

*Key Findings and Recommended Actions***Key Findings**

10.6

- 1) Intelligence analysis and dissemination is undertaken by AMLC's FIAG and FCIG, which produce quality operational intelligence including financial profiles and network analyses. The intelligence shared is mainly related to limited higher risk crimes i.e. fraud, drugs, corruption and TF.
- 2) Following the June 2018 restructure, AMLC is now better structured to perform its role as an FIU, with a reasonable allocation of analytical resources. AMLC has taken steps to improve its analysis, but a large number of roles remain unfilled, which leaves AMLC with insufficient staff to effectively perform its full range of intelligence and investigation functions, including being the agency responsible for obtaining bank records for most competent authorities.
- 3) Financial intelligence is used to a limited extent to trigger or support investigations into ML, TF or predicate offences. AMLC's financial intelligence is primarily used by the FCIG for ML and TF and, to a very limited extent, by other LEAs for predicate crime investigations. Very few ML and predicate investigations originate from financial intelligence produced by FIAG, and there was an insignificant number of proactive disclosures made by AMLC to LEAs during the review period.
- 4) There are serious practical impediments to other LEAs developing and using financial intelligence arising from AMLC being the primary agency able to access bank records on behalf of LEAs. AMLC lacks sufficient staff to effectively perform the role on behalf of all LEAs. There is also an impediment in relation to disclosures outside AMLC on PEPs during election periods. Other LEAs did not demonstrate that they regularly develop their own financial intelligence, or request bank records or request and receive financial intelligence from the FIU for use in their investigations. While they are able to access financial records from FIs/DNFBPs other than banks and depository institutions, this was not demonstrated in practice.
- 5) AMLC's disseminations to LEAs are predominantly reactive, in relation to investigations into predicate offences and terrorism, in particular to further develop evidence and trace criminal proceeds. Intelligence provided by FIAG includes identifying information, financial profiles and network analysis, and other relevant information.
- 6) AMLC is receiving an increasing number of STRs, mostly from the banking sector. AMLC and BSP have worked to improve STR quality. AMLC receives a very large number of CTRs, which include transaction type, parties, amount, nature and purpose and KYC information. The number of cross-border currency declarations received is low, which is not in line with the Philippines' risk profile.
- 7) AMLC has access to a wide range of information, either directly or via request. AMLC is able to request information and other related documents from covered persons. For information that is not already available to AMLC, AMLC requests submission of an STR on a specific account/person of interest. While this enables access to records at the intelligence stage, it potentially impede timeliness and availability of information for analysis.

10.7

- 1) The number and extent of ML investigations, prosecutions and convictions is not commensurate to the ML risk profile of the Philippines. Since 2013 there were 20 ML investigations submitted for prosecution, with 10 ML prosecutions and five ML convictions, all of which were done by AMLC.
- 2) AMLC is the primary designated authority to investigate ML offences, although it is not resourced, or given full LEA powers, which would allow it to conduct all ML investigations in keeping with the risk profile.
- 3) AMLC's FCIG has only 18 staff and the primary responsibility for ML investigations, proceeds of crime actions, and access to bank records for all other LEAs. This does not leave FCIG with appropriate resources to investigate ML in line with the high risk of ML in the Philippines.
- 4) While PNP and NBI have general investigation powers, unlike the AMLC, they have not been designated to investigate ML and do not do so in practice. OMB, which investigates graft and corruption, does not have the mandate to investigate ML.
- 5) AMLC investigations support both civil forfeiture actions and ML cases, but with a greater focus on civil forfeiture matters. From 2013 to 2018 FCIG conducted 277 investigations resulting in 42 petitions for civil forfeiture and 20 potential ML cases.
- 6) AMLC FCIG is not fully empowered in its own right to conduct search and seizure of evidential materials/assets, to take all witness statements (presently limited to covered persons and government agencies) or to use certain special investigative techniques. AMLC does not sufficiently seek assistance to have LEAs use their powers to support AMLC ML investigations.
- 7) While it does occur in some cases, LEAs do not regularly seek AMLC's assistance to pursue parallel ML investigations in keeping with the risk profile of major proceeds generating predicate offences.
- 8) There are challenges in ML investigations leading to prosecutions; and with prosecutions leading to convictions, which appear to stem, in part, from investigators needing additional support and guidance from prosecutors at an earlier stage in complex cases. Prosecutors are not actively involved in assisting FCIG during investigations to support successful ML evidence collection.
- 9) ML prosecutions have mostly largely related to self-laundering by natural persons, in relation primarily to domestic predicate criminal activities. ML prosecutions have had a negligible emphasis in pursuing ML from foreign predicate offences and ML through legal persons.
- 10) In the very limited number of cases, where convictions were secured and sanctions applied, these were shown to be effective, proportionate and dissuasive.

10.8

- 1) The Philippines does not apply confiscation and provisional measures commensurate to the risk profile. This is demonstrated by the low confiscation figures (USD 15.5 million over six years (15 million of which was one case). USD 117 million has been restrained across 41 cases in the same period, which is also very low.
- 2) Civil forfeiture is the predominant mechanism for depriving criminals of their unlawful gains, however the numbers of restraints are low (41 remain pending over a six year period) and completed civil forfeiture actions are very low (eight over six years). There are very significant

delays with civil forfeiture actions. Many restraint actions have been in place for over a decade pending forfeiture.

- 3) AMLC is the main agency responsible for confiscating criminal proceeds through civil forfeiture actions. AMLC has demonstrated a focus in depriving criminals of the proceeds of crime, but it is critically under-resourced to perform the function.
- 4) Authorities did not demonstrate the regular use of the available powers for confiscation of proceeds or instruments of crime. Neither prosecutors nor LEAs have a policy or practice of seeking confiscation orders at the point of conviction or sentencing for predicate or ML offences. AMLC does, however, seek confiscation through non-conviction based civil forfeiture.
- 5) The legal framework on confiscation of assets does not provide mechanisms to ensure proper asset management and preservation during the investigation stage and after the forfeiture decisions.
- 6) The new NACS includes a policy objective to pursue asset recovery in ML, predicate offences and TF cases, focusing on identified high-risk crimes. However, this policy has not yet been implemented.
- 7) With the exception of AMLC, most LEAs rarely conduct financial investigations to trace property that may be subject to restraint or confiscation. LEAs other than AMLC have mostly conducted seizures for evidentiary purposes. LEAs other than AMLC face constraints in their ability to conduct financial investigations to trace assets due to the lack of timely access to bank records.
- 8) Confiscation results mostly relate to proceeds located in the Philippines; there is limited demonstration of authorities pursuing confiscation of assets moved to other jurisdictions and pursuing proceeds of foreign predicate crimes and property of equivalent value in the Philippines.
- 9) Despite the high risks faced by the Philippines from smuggling including currency, implementation of the cross border declaration system is very weak and there were only 15 instances of confiscation of falsely / not declared cross-border movements of currency and BNIs during the review period which is very low. The limited coverage of sea/air port entry/exit points and the shortage of human resources are notable.
- 10) There were no confiscations, including in instances where instrumentalities and equivalent value in respect of terrorism and TF, which is not in line with the risk profile.

Recommended Actions

IO. 6

- a) Significantly enhance the staffing and capability of AMLC's FIU function (including filling vacant positions and going beyond the planed establishment).
- b) LEAs (other than AMLC) should enhance their development and use of financial intelligence and other relevant information to develop evidence and trace criminal proceeds in keeping with each LEA's areas of responsibility and the Philippines' risk profile.
- c) Enhance AMLC's proactive dissemination to other LEAs, including spontaneous disclosures to support other LEAs' operational needs for predicate investigations, parallel ML or TF

investigations and asset tracing investigations, as well as the operational needs of AML/CFT supervisory authorities.

- d) Further improve the quality of intelligence analysis by FIAG.
- e) Continue to take measures to improve STR quality and address challenges with defensive reporting of STRs, and support greatly improved cross border cash reporting to ensure AMLC has sufficient relevant and accurate information that assists it to perform its duties.
- f) Further enhance AMLC's information sharing, and broader support to LEAs on terrorism and TF, and predicate offences (beyond fraud, drugs and corruption) that pose a higher level of threat for ML.
- g) AMLC should ensure the confidentiality of information is protected when sharing intelligence in an informal manner.

10.7

- a) Taking into account AMLC's role as the lead ML investigation agency, greatly increase FCIG staffing to add appropriately skilled investigators for ML and financial investigations up to and beyond the 2018 establishments. Ensure dedicated staff, with the specialised knowledge on financial crimes, within LEAs with financial investigation units.
- b) Ensure certain LEAs seek expedient access to bank records (with appropriate integrity controls) for AML/CFT functions and predicate crime investigations; amend legislation to include tax crimes as predicate offences to ML; and empower AMLC, as an LEA, to exercise the fullest range of investigative powers.
- c) Implement objective 2 and other related objectives of the NACS, to enhance the effective identification of ML arising out of predicate crime investigations and financial intelligence in keeping with the risk profile. This can include mechanisms and guidelines related to the referral by LEAs of possible ML elements arising out of predicate crime investigations.
- d) Apply significantly greater resources and to more effectively pursue ML arising out of high risk predicate crimes and foreign predicate crimes whilst focusing on prosecuting different types of ML, including third party and stand-alone ML.
- e) In order to address the significant need for greater resources to be allocated to ML investigations, the Philippines should consider certain LEAs be designated to conduct their own ML investigations (with appropriate integrity controls).
- f) LEAs should regularly refer possible ML aspect to AMLC to pursue parallel ML investigations, whilst continuing with predicate crime investigations. However, LEAs should also support AMLC in ML investigations where their investigative powers are insufficient.
- g) Review the impact of the civil forfeiture mechanism and applicable timelines on the pursuit of ML investigations with a view to increasing the numbers of ML investigations.
- h) In order to address the challenges with the number and range of ML investigations leading to prosecutions and convictions, the Philippines should consider prosecutors being actively involved

in assisting LEAs (including FCIG) during investigations to support successful ML evidence collection and to advise more broadly on the approach to investigations.

IO. 8

- a) Implement priority actions of the NACS, in relation to confiscation; ensure agency level policies and specific action plans are in place with effective implementation in line with the risk profile. This should include prosecutors and all LEAs prioritising asset tracing and obtaining confiscation orders at the point of conviction and sentencing for profit driven crimes, including orders for property of corresponding value.
- b) Taking into account AMLC's role as the lead asset tracing and civil forfeiture agency, greatly increase FCIG staffing to add appropriately skilled staff up to and beyond the 2018 establishments.
- c) Amend provisions in AMLA and other statutes to address the technical compliance gaps outlined at Recommendation 4.
- d) Prosecutors, AMLC, NBI, PNP, PDEA, etc. should prioritise the assets tracing, restraint and criminal confiscation actions on all high risk predicate crimes, foreign predicate crimes and proceeds moved to other jurisdictions. This should include obtaining confiscation orders at the point of conviction and sentencing for profit driven crimes.
- e) All relevant LEAs and prosecutors should implement strategic actions to widen the use of civil forfeiture and support activities that speed up the process to complete civil forfeiture actions.
- f) Take action to ensure that relevant cross border measures are applied to all main entry/exit, sea/air ports of the country and provide more resources to BOC, especially human resources.
- g) Provide specialised training to investigators, prosecutors and judges, in line with the recommended action in the IO.7 as the lack of designated courts to file charges in relation to financial crimes and the turnover in the judiciary are also challenges with respect to freezing and forfeiture actions.
- h) As identified by the NACS, create an Asset Management Office, providing mechanisms for the preservation and management of assets subject to provisional and confiscation actions.

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

Immediate Outcome 6 (Financial intelligence ML/TF)

125. AMLC is a hybrid FIU/investigative/supervisory agency. AMLC's Financial Intelligence Analysis Group (FIAG)⁵⁶ performs the FIU function while the Financial Crime Investigation Group (FCIG)⁵⁷ conducts further analysis and investigations. FCIG is the main user of FIAG's intelligence products in its designated role to conduct ML and TF investigations. AMLC has the authority to provide financial intelligence to other LEAs to support and assist their investigations of predicate crimes

⁵⁶ Known as Financial Intelligence Analysis (FIA) before 2018

⁵⁷ Known as Compliance and Investigation Group (CIG) before 2018

depending on the LEA's jurisdiction. In practice, other LEAs focus on predicate offence investigations while AMLC focuses on ML and asset tracing, as this aligns with agencies' expertise and skill sets.

126. In response to the NRA findings, in July 2018⁵⁸ AMLC restructured and increased its staffing establishment to better support its functions as a hybrid FIU and to separate the FIU function from the investigation function, with the overall size of AMLC increasing from 175 to 254. FIAG and FCIG were created, reflecting AMLC's functions of financial intelligence and investigations. The new structure, and intended staffing levels, are expected to increase specialisation of analysts and investigators and overall capability. The previous Financial Intelligence Analysis Staff (FIAS) section was expanded and renamed FIAG which is now divided into four areas: Tactical Analysis; STR Analysis; Strategic Analysis; and Data Mining (CTR Analysis). FIAG is devoted solely to the conduct of financial intelligence analysis. This analysis supports the work of FCIG, which undertakes investigations. FIAG is expected to undertake full analysis of financial intelligence before disclosure to FCIG, LEAs or foreign FIUs, which differs from the previous model where investigators needed to undertake further analysis of financial intelligence before commencing investigations and disclosures. In practice FCIG undertakes further analysis before dissemination occurs.

127. In July 2018 FIAG's established positions increased from 9 to 35, but only 15 were filled at the time of the onsite visit. Recruitment for the remaining positions was expected in late 2019. Filling these positions is required to meet the FIAG's workload.

Use of financial intelligence and other information

128. FIAG produces a modest number of financial intelligence reports to support LEAs' intelligence development and evidence collection for ML, TF and associate predicate offences. The main recipient of FIAG intelligence is FCIG, for the purpose of ML and related asset tracing. Given the risk and context of the Philippines, the number of intelligence products produced is relatively small, with a total of 1,555 financial intelligence reports (FIRs) utilised by FCIG to undertake investigative actions between 2013 and 2018. These disseminations were either based on a request made by FCIG (or its predecessor) to FIAG (which includes requests on behalf of other LEAs), or proactive dissemination from FIAG to FCIG (see Table below). While the number of disseminations is low, all were used to support various stages of ML, TF or predicate offence investigations, or confiscations. Overall, a total of 6,444 STRs (1% of all STRs) and 155,102 CTRs (0.06% of all CTRs) were used in proactive disclosures and 182,225 STRs (30%) and 24,102,207 CTRs (10%) in reactive disclosures.

Table 3.01: Intelligence Reports Disseminated by FIAG to FCIG

	2013	2014	2015	2016	2017	2018	Total
Reactive Intelligence Reports	112	98	68	446	411	158	1,293
Proactive Intelligence Reports	78	97	23	13	8	43	262
Total Disseminations	190	195	91	459	419	201	1,555

129. FCIG utilises FIAG FIRs in four phases of investigation. The 1,555 FIRs disseminated to FCIG between 2013 and 2018 were utilised in cascading sequence as follows:

- a) *Phase 1 (case evaluation)*: all 1,555 FIRs were evaluated to assess whether there was unlawful activity. FCIG generally prioritises cases based on pre-set parameters (mostly related to high risk crimes), as per the FCIG manual; hence, not all FIRs received may warrant further investigation.

⁵⁸ On 12 July 2018, the AMLC Reorganisation was approved by the Monetary Board (MB) under MB Resolution No. 1150 Anti-money laundering and counter-terrorist financing measures in the Philippines © APG 2019

- b) *Phase 2 (in-depth analysis)*: 824 FIRs were used to support the development of 277 cases for further investigation, including the determining of probable cause for banking inquiries and freeze orders.
- c) *Phase 3 (bank inquiry/ freeze order)*: 567 FIRs were used to support 141 cases which were referred to LEG and eventually resulted in either banking inquiries for documentary evidence or freeze orders (see table 12 for further breakdown).
- d) *Phase 4 (investigation report)*: 485 FIRs were used to support 81 cases which were referred to LEG (total 20 ML complaints, 10 ML prosecution and two TF complaints) and the filing of civil forfeiture cases (42 for ML and one for TF) (see table 12 for further breakdown.)

Table 3.02: AMLC FGIC use of FIRs in Phase 2-4 of Investigation

	Reactive	Proactive	Total
Phase 2 of investigations			
FIRs used	683	141	824
Cases/investigation report supported	257	20	277
Phase 3 of investigations			
Number of FIRs used	442	125	567
Cases/investigation report supported	128	13	141
Phase 4 of investigations			
Number of FIRs used	392	93	485
Cases/investigation report supported	72	9	81

130. Between 2015 and 2018, the cases filed for ML prosecution, asset freezing and banking inquiry related to the offences of fraud, drug trafficking, human trafficking, terrorism and TF. In total, 10 cases were converted to eventual ML prosecutions (see IO.7).

Table 3.05: AMLC ML Investigative Activities following Disseminations (between FIAG to FCIG)

	2013	2014	2015	2016	2017	2018	Total
Phase 3: Investigation Process (Banking enquiry and freeze order)							
FIRs (reactive/proactive) used by FCIG	78	75	78	139	104	93	567
Cases/FCIG Investigation Report (IR) for ML	25	33	19	30	15	16	138
IRs for TF	1				2		3
FCIG IRs referred to LEG for banking enquiry or freeze order (ML/TF)	26	33	19	30	17	16	141
Phase 4: Investigative Process (Investigation Report)							
FIRs used	70	72	73	151	87	32	485
FCIG Investigation Reports referred to LEG	14	9	17	16	12	13	81
Of which (for ML):							
<i>(a) Petitions for Civil Forfeiture</i>	6	7	8	6	9	6	42
<i>(b) ML complaints filed before the DOJ</i>	1		5	6	1	3	16
<i>(c) ML complaints filed before the OMB</i>						4	4
<i>(d) ML cases filed before the RTC</i>	3	1	1	3	2	0	10
FCIG TF Inv. Reports referred to LEG	1	-	-	-	2	-	3
Of which (for TF):							

	2013	2014	2015	2016	2017	2018	Total
(a1) Petitions for Civil Forfeiture	-	-	-	-	-	1	1
(b)TF complaints filed before the DOJ	-	-	-	-	-	2	2

131. The use of financial intelligence by LEAs other than AMLC is limited to supporting investigations of predicate offences, as FCIG conducts all ML investigations. Other LEAs submit requests for financial intelligence to FCIG, who forwards the request on to FIAG. Of the 1,293 reactive intelligence reports FCIG received from FIAG (between 2013 and 2018), 437 requests were made on behalf of other LEAs, with the FIR forwarded onto the requesting party. This is a 44% response rate by AMLC, noting however that some FIRs addressed multiple requests.

132. Since 2013 there has been an increase in requests from other LEAs for AMLC financial intelligence in support of predicate offence or terrorism investigations. Other LEAs' requests correlate with only some of the higher risk predicate crime threats identified in the NRA as risks for ML, particularly drugs, corruption and fraud. Outside FCIG, the main recipients of AMLC financial intelligence are PNP-ACG (cybercrime), NBI (organised crimes), PCTC (transnational crime), Ombudsman (corruption) and PDEA (drugs/corruption).

Table 3.06: Reactive Disclosures shared by FCIG (AMLC) to LEAs

	2013	2014	2015	2016	2017	2018	Total
Reactive Intell Reports - from FCIG to LEAs	55	52	37	68	79	146	437

133. In addition to reactive disclosures to other LEAs, there were also a very small number (5) of spontaneous disclosures made to other LEAs for predicate offence investigation. AMLC shared other proactive intelligence reports from FCIG with LEAs, formally or informally, through case conferences.

134. Statistics show a more regular pattern of disclosure for drugs offence investigations, where the main disclosures since 2016 were undertaken through bilateral workshops (case conferences) between AMLC and PDEA. The usage of financial intelligence in supporting other predicate offences investigation is not available, however some case examples are provided below.

Case Example 3.01 - STR triggered fraud case

In 2015 AMLC filed an ML cases against three subjects for fraud. The investigation was triggered by an STR on cheques payable to a government agency, which were deposited into the personal account of one of the subjects. The funds were subsequently withdrawn by the subject for personal use. The amount detected was PHP966,000 (approx. USD18,000) in one account. Over PHP200,000 (approx. USD3,800) was seized.

Case Example 3.02 - STR Triggered Drug Trafficking Case

In August 2013, several STRs were lodged on a subject named JAM in relation to multiple domestic remittances made to various individuals with unclear purposes and relationship between the parties involved. In an effort to establish the modus operandi of JAM and identify possible suspicious patterns of remittance activities, FIAG conducted open source searches and analysis on related beneficiaries. The intelligence resulted in identification of more accounts possibly involved in illegal drug activity.

Based on FIAG's intelligence findings, ML and civil forfeiture cases were filed by FCIG against the identified drug suspects, involving 23 bank accounts in four local banks. Subsequently, the PNP arrested JAM and AMLC

filed a civil forfeiture case. In 2015, an asset preservation order (APO) was issued amounting to PHP 4.1 million (approx.: USD 78, 000) worth of assets for five entities involved in drug trafficking.

Case Example 3.03 – STR Triggered Drugs Case

In 2011, an STR was submitted in relation to transactions which were not commensurate with the business of the customer. Deposits were made to the account from various branches ranging from PHP22,750 (approx. USD 522)⁵⁹ to PHP452,000 (approx. USD 10,376). Funds were then withdrawn and deposited into the accounts of persons who were the subject of separate STRs. The intelligence report prepared by FIAG contained profiles of the subject and identified new persons of interest.

FIAG identified 21 involved bank accounts in five local banks and one foreign institution, amounting to PHP6.89 million (approx. USD 131,000). The accounts were believed to contain deposits from the sale of drugs.

In 2014, the AMLC successfully froze the accounts of parties identified in the drug trafficking scheme and filed a civil forfeiture case, with an APO granted in 2015.

The intelligence report was shared with PDEA, which resulted to the arrest of the subjects in a buy/bust operation. The AMLC case was submitted for ML prosecution by the DOJ.

135. LEAs use financial intelligence in TF investigations to a limited extent. As recognised in the 2017 NRA, intelligence gathering has focused on terrorism rather than TF for the period 2014-2016. Despite the high level of TF risk, there has been a low number of STRs on TF (0.06% of the total number of STRs). However, the number of STRs is growing (2015: 44; 2016: 96, 2017: 349 and 2018: 100). Case studies show that TF analysis is more often triggered by information from LEAs and/or foreign FIUs. Financial intelligence has been used for investigative actions such as controlled delivery and freezing actions rather than to a completed TF investigation (for the purpose of prosecution) per se.

136. Although TF financial intelligence has been shared during the JTFIG weekly meetings, as at the time of onsite visit there had been no TF investigation (for the purpose of prosecution) originating from these disclosures. Nevertheless, as noted in IO.9, there have been 18 TF investigations between 2014 to June 2017. Most of these cases were a result of referrals made by Intelligence Services of the AFP⁶⁰ and LEAs (including PCTC, PNP, NBI and the SEC). AMLC intelligence was used in the TF investigation of a TF case relating to the Maute Group in the Marawi Siege. AMLC intelligence and foreign disclosures supported the investigation of financial networks of the group, including uncovering of previously unknown financiers/ facilitators and FTF. This resulted in a civil forfeiture case against Maute Group (total PHP52 million, approx. USD 1 million).

STRs received and requested by competent authorities

137. The number of STRs and CTRs received by AMLC is increasing. The number of cross border currency declarations is low, considering the extensive use of cash and the cash smuggling risks.

⁵⁹ 1 USD= 43.56 PHP in 2011

⁶⁰ It is unclear whether such referrals included financial intelligence. The 2017 NRA states the focus of intelligence is more on terrorism rather than TF. However, at the time of onsite, the AFP had recently created a TF unit which had engaged with AMLC for capacity building on TF investigations. There is an ongoing negotiation for an MOA with AMLC to enable information sharing, including the names of persons of interest, financial documents and information obtained during ground operations.

Table 3.07: STR, CTR and Cross-Border Declarations received by AMLC (as at 27 Nov 2018)

		2013	2014	2015	2016	2017	2018	Total
STRs Received		94,549	94,939	146,398	132,306	287,265	442,108	1,197,565
CTRs Received		45,674,856	44,381,819	36,322,064	36,981,140	39,940,922	39,295,290	242,596,519
Cross-Border Declarations	Inbound	395	490	519	32	162	64	1662
	Outbound	904	1,044	958	919	943	570	5338

Table 3.08: STRs Received by AMLC from Reporting Entities

Reporting Entity	2013	2014	2015	2016	2017	2018	Total	% of Total
Banks	84,743	80,287	133,420	115,716	235,124	327,936	977,226	82.60%
Non-banking sector	9,806	14,652	12,978	16,590	52,141	113,797	219,964	18.37%
DNFBPs						375	375	0.03%
Total	94,549	94,939	146,398	132,306	287,265	442,108	1,197,565	100%

138. Overall, between 2013 and 2018 STRs and CTRs were submitted by around 40% of all covered persons. The banking and MSB sectors submitted the highest volume, which aligns with their risk profile. Between 2013 and 2018, the majority of STRs related to swindling (308,542); violations of the E-Commerce Act (170,018); fraudulent practices and other violations of the Securities Regulation Code of 2000 (132,726); graft and corruption (33,558); and drug offences (23,275).

139. The offence of fraud (which includes the top three most common STR offence categories) accounts for 80% of the total STRs submitted by covered persons. For other high risk crime types (smuggling, intellectual properties violation, illegal firearms, environmental crime, corruption and drugs), although there is variation between years, the number of STRs received in relation to these offences is generally disproportionately low compared with the number of STRs on fraud, and generally does not align with the high risk crimes identified by the Philippines. In 2015, AMLC received a 54% upsurge in STRs. The bulk of STRs reported were related to violation of the Securities Regulation Code of 2000. These STRs pertained to a global investment scam involving several entities and individuals allegedly selling unregistered securities (i.e. gold) to the public without a license. Swindling was one of the top predicate crimes in 2015. Most of these STRs were related to ATM/credit card fraud. There was also an increase in STRs related to corruption and drug trafficking, which the Philippines attributed to intensified LEA focus on these crimes.

140. During the same period, a small but increasing number of STRs were reported for terrorism (1,065) and TF (613). In the context of the Philippines, cash transactions remain the preferred mode for movement and usage of funds for TF, and transactions may not involve the use of covered persons.

141. A review of STR quality conducted by AMLC in 2017, covering 132,306 STRs received from 149 covered persons in 2016, found that 53% were of high quality. Areas of weakness, and STR quality more broadly, are being addressed by AMLC through the preparation and distribution of detailed guidelines on STR submission and enhanced engagement with compliance officers and supervisors.

142. To further improve the effectiveness of STR reporting, in July 2018 AMLC approved the Information Sharing Protocol with covered persons. The Protocol allows for the sharing of preliminary intelligence with covered persons to trigger STR submission. It is however too soon to judge the effectiveness of this new measure.

143. In addition to the large numbers of STRs, CTRs and small number of cross-border declaration reports, AMLC has direct access to information or data including Articles of Incorporation and General Information Sheets (GIS) from the SEC, and trade name registration data from the Department of Trade and Industry (DTI) for single proprietor entities. Under the AMLA, all real estate transaction in excess of PHP500,000 (approx. USD 9500) must be reported by the Land Registration Authority (LRA) to AMLC within 15 days of the transaction occurring. At the time of the onsite visit AMLC had recently signed a MOA with the LRA and the signing of a MOA with the Bureau of Immigration (BI) had been approved by both agencies. These MOAs will facilitate direct access to LRA's and BI's databases, which was not in effect as at the time of the onsite visit.

144. Overall, the access and information available for the purpose of analysis by FIAG has added value to FIAG's products. AMLC can request information under MOAs or enlist other agencies to provide information from their databases. There include criminal records from the PNP; travel records from the BI and motor and vehicle registration records from the Land Transportation Office. AMLC can obtain any relevant document from information from relevant domestic agencies and can request information from foreign partners.

145. AMLC updated its prioritisation and classification procedure for processing and referring STRs in 2017 to enhance its analytical capacity. STRs are categorised as either high, medium or low priority for dissemination based on the unlawful or suspicious activity (STR categorisation). The high priority classification is mainly focused on predicate crimes that do not require a court order for AMLC to inquire into and selected high risk crimes under NRA, rather than being closely linked to all crimes classified as 'high' ML/TF risk. For instance, kidnapping for ransom is rated 'medium' in the NRA but is prioritised along with other high risk crimes, while fraud, smuggling and environmental crimes rated high risk in the NRA but are classified as 'medium' in the STR prioritisation.

Table 3.09: Classification of STRs as High, Medium and Low Priority

Priority	2013	2014	2015	2016	2017	2018	Total
HIGH	74,642	29,982	47,217	12,267	27,262	10,716	202,086
MEDIUM	4,566	22,539	41,437	55,583	160,327	191,031	475,483
LOW	15,340	42,418	57,744	64,456	99,676	240,361	519,995
Total	94,548	94,939	146,398	132,306	287,265	442,108	1,197,564

146. In 2017 the AMLC introduced the requirement for KYC documents to be submitted with STRs which relate to (a) kidnapping for ransom; (b) drug trafficking; (c) hijacking; destructive arson; and murder, including those perpetrated by terrorists against non-combatant persons and similar targets; (d) terrorism and conspiracy to commit terrorism; and (e) TF. This supports the timeliness and effectiveness of analysis. Between January and November 2018, 10,350 KYC documents were uploaded with STRs. Those STRs related to drug trafficking (87%), terrorism (5%), TF (2.2%) and kidnapping for ransom (4%). For other crime types, FIAG and FCIG are authorised to request all relevant documents from covered persons for analysis or investigation.

147. In addition to the KYC documents lodged with particular STRs, AMLC has access to KYC documents through CTRs. AMLC's database contains 11.34 million KYC documents relating to all transactions above PHP500,000 (approx. USD9,500) conducted between 2004 and 2017. In addition to KYC documents, the CTR database contains a significant amount of transactional information (including type, parties, amount, nature and purpose of transactions). For information not available in the AMLC

database, targeted requests are made to covered persons for specific information to be submitted under Section 7(2) of the AMLA. Between 2013 and 2018, AMLC made 1,767 requests for additional information from covered persons via new STRs.

Operational needs supported by FIU analysis and dissemination

148. In supporting the operational needs of investigation into ML/TF and predicate offences, AMLC has continued to upgrade its analytical software to ensure higher quality STR and CTR analysis, both in terms of tactical and strategic analysis. In supporting and increasing its capacity, AMLC invested significantly in data mining tools and analysis systems in 2017, with full implementation by the end of 2018. Prior to this, the FIAG was conducting manual analysis to identify trends and methods based on typologies. With the acquisition of the relevant tools, data mining in pattern-based queries, searches, or other analysis of the AMLC database is conducted to discover or locate a predictive pattern or anomaly, which indicates terrorist or criminal activity.

149. Since 2014 FIAG has produced reports on boiler room frauds (for the period 2013 – 2016) and on illegal drugs and investment scam (in 2017). While FIAG has not yet produced strategic analysis reports using the full features of its new software, the data mining tools and analysis systems have improved the quality of some tactical analysis reports.

150. AMLC has produced other strategic analysis reports that include typologies and mitigation measures for identified issues. Some of these reports are published on the AMLC website. Between 2015 and 2018, AMLC produced the following strategic analysis reports:

- Strategic Analysis on Cross-border Investment Fraud (2015)
- Strategic Analysis on STR Quality Review (2017)
- Strengthening AML Surveillance alongside Advancements in Financial Technology (2017)
- Towards Deepening Regulatory Compliance: An Assessment of the Development of AML Reporting Compliance of Pawnshops and MSBs (2018)
- A Close Look into the Philippine Exposure to External Threats based on STRs (2018)

151. AMLC provides financial intelligence analysis reports and relevant information to LEAs (mainly through responses to requests for information), while FCIG has direct access to FIAG's financial intelligence products to further develop evidence and trace criminal proceeds. Financial intelligence provided by AMLC supports predicate offence investigations by providing LEAs additional investigative leads in the form of identifying information, financial profiles and networks, and other relevant information available from financial intelligence analyses.

152. While there have been some successes (see case study below), overall, the financial intelligence shared has not frequently translated into effective outcomes. As a matter of practice, AMLC requests feedback from LEAs on each disclosure made. In 2017 the LEAs which received AMLC's financial intelligence reported that 50% of AMLC disseminations contained information already known to the LEAs and provided minor contribution to their analysis or investigation. This issue has been recognised by AMLC, which has undertaken measures to enhance its analysis, as outlined above.

153. From 2013 to 2018 LEAs and other domestic agencies made only 989 requests (from 49 agencies) to the FIU, an average of 165 per year. Of these, 437 were responded to. The number of requests from LEAs has increased over the years. AMLC explained that the lower response rate can be

attributed to the fact that multiple similar requests are responded to collectively in one report, or the information sought from LEAs is unavailable.

Table 3.10: Request from domestic agencies to AMLC (2013 and November 2018)

Requesting Agency	Requests to AMLC	Responded by AMLC
PNP-ACG	292	127
PCTC	107	58
NBI	93	70
PDEA	91	27
CIDG	66	20
SEC	45	20
OMBUDSMAN	44	38
DOJ	39	16
PNP	17	8
PNP-AKG	16	9
Others (across 39 agencies/departments/ offices)	178	44
Grand Total	989	437

154. Between 2013 and November 2018, the top 10 predicate offence investigation types which AMLC's responses to LEA requests related were; swindling (106), fraud (61), illegal drugs (57), graft and corruption (30), estafa fraud (17), violations of SRC (13), kidnap for ransom (11), terrorism (10), TF (eight) and ML (five).

155. Investigations which utilised AMLC financial intelligence related to fraud, drugs and graft and corruption, which are rated high risk for ML (along with five crime types, as discussed in IO.1). From the reactive FIRs, there were 277 investigations, which included some of the major cases in the Philippines (i.e. PDAF and Bangladesh Heist Cases), some of which also resulted in parallel ML investigations, particularly for drug offences⁶¹. Examples of the cases where FIRs supported predicate offences investigation are outlined below.

Case Example 3.04 - PE et al.

In 2016 PNP-IG and PDEA requested information from AMLC on the bank accounts of 'PE' and related parties. At the same time AMLC received 134 STRs from a bank on the suspect, due to large deposits, funds transfers and cheques which were not commensurate with their declared source of funds. AMLC investigations and intelligence gathered by PDEA showed banking transactions that suggested PE's accounts were used for laundering drug proceeds by several actors within the company. AMLC tracing resulted in the freezing of PHP187million (approx. USD 36 million) in 177 accounts across nine banks and six remittance companies. An APO was granted and a civil forfeiture case filed.

Case Example 3.05 - NL Case (Drug Trafficking) - STR and Case Conference with PDEA

AMLC conducted an investigations triggered by STRs and intelligence reports with PDEA and PAOCC during a case conference. The information led to the arrest of the subject and identification of new persons of interest. Associates of the earlier subject of STRs were identified, who were the local distributors of stolen vehicles in Zamboanga and neighboring areas and were involved in trafficking illegal drugs from Luzon to Mindanao.

⁶¹ At least 10 coordination bilateral/multilateral meetings have been held for parallel ML / predicate crime investigations between AMLC and PDEA, OMB, NBI and PNP-CIDG.

In 2014 freezing actions were taken by AMLC for PHP3.49 million (approx. USD 66,000) involving 18 accounts in three local banks and two remittance companies involving eight individuals. A civil forfeiture case was subsequently filed in 2016, and an APO issued for the total amount frozen. An ML case was also initiated.

Case Example 3.06 - CJ (Fraud)

In May 2018, the PNP Anti-Cybercrime Group (PNP-ACG) requested information from AMLC on a fraud case. FIAG identified KYC documents confirming that Ms. E was the account holder of the subject bank account and found STRs reported by a virtual currency exchange and the bank. AMLC suspected that Ms. E was involved in an internet scam using investments to falsely promise high returns to victims through Facebook accounts.

PNP-ACG investigations based on the AMLC disclosure resulted in charges of a predicate offence. PN-ACG found that the suspect offered 30% to 300% return of investment and prizes that enticed people to invest money.

3

156. In addition to responding to written information requests and disclosures made by AMLC, AMLC and PDEA have held numerous bilateral workshops since 2016 to exchange information, including information relating to persons of interest. Subsequent actions taken which resulted in predicate offence investigation, freeze order, Provisional Asset Preservation Order / Asset Preservation Order (PAPO/APO) and ML investigation are set out below.

Table 3.11: PDEA's use of information provided by AMLC

	2016	2017	Up to Aug 2018
Shared information/ intelligence	36	130	80
Predicate investigation	1	6	34 ⁶²
Freeze order	-	1	9
PAPO/APO	12	24	30
ML investigation (by AMLC)	-	2	2

157. Between 2013 and 2018 AMLC provided only 10 terrorism and 8 TF related intelligence products to LEAs in support of the LEAs' operational needs to combat terrorism and/or TF. It is notable that these 18 disclosures covered 842 individuals. During the same period, there were 986 terrorism incidents associated with known terror/threat groups as noted in the NRA. From the case studies provided by AMLC, intelligence supplied to LEAs was often used for controlled delivery or freezing actions, which led to the filing of one TF case.

158. In relation to investigating corruption and related ML, as noted in the analysis of R.9 and R.29, AMLC does not share information on PEPs outside AMLC during election periods. However this does not prevent the internal sharing of PEP information from FIAG to FCIG⁶³. Further, information on PEPs can be shared after the election concludes. AMLC confirmed that all requests pertaining to intelligence on PEPs are approved by the Council during their monthly meetings and on average the Council approves such applications within two to three days of submission of a memorandum by the AMLC Secretariat. In some cases and in urgent matters outside their scheduled monthly meetings, approval of the Council has occurred within a day. In some cases, the Council requested resubmission of

⁶² Under investigation or pending LEG

⁶³ AMLC advised that the policy of not sharing information on PEPs to other LEAs during an election period was implemented as a measure to support democracy and prevent AMLC from being used for political persecution during election periods. The policy is in effect for 120 days during elections, which are held every three years.

memoranda in order to clarify some matters; however, the Council has then always approved the re-submitted memoranda within an average of two to three days from re-submission.

Table 3.12: Number of Resolutions and Re-submission Made to the Council (PEPs and others)

Year	Approved Resolutions	Resolutions resubmitted for Approval	
			% of Total
2013	117	9	8%
2014	121	2	2%
2015	72	2	3%
2016	117	1	1%
2017	131	20	15%
2018 (to Nov)	201	15	7%
Total	759	49	6%

159. Of the instances where the Secretariat has sought Council approval, there were 48 applications made involving 100 PEPs for the purpose of dissemination. Of these, 54 PEP disclosures related to drug cases and 46 related to graft and corruption. The recipients of the intelligence on PEPs have included Office of Ombudsman, PDEA, NBI, PNP and foreign FIUs.

Table 3.13: Number of Intelligence Reports Involving PEPs

	2013	2014	2015	2016	2017	2018	Total
Intelligence Reports made by FIAG	3	11	7	18	6	3	48
PEPs referenced in Intelligence Reports	3	1	1	58	32	5	100

Case Example 3.07 - PDAF/Pork Barrel case

A request for financial investigation was made to AMLC in relation to the Priority Development Assistance Fund (PDAF) (commonly known as the 'pork barrel' cases, see also IO.8), which involved approximately 1,400 bank accounts. The investigation resulted in the filing of a civil forfeiture case for approximately PHP75 million (approx. USD 1.4 million) and four ML cases. The investigation commenced from a referral by the OMB to AMLC of reports that included copies of cheques representing PDAF funds issued by the Department of Budget and Management to government implementing agencies, and cheques subsequently issued by said agencies to NGOs used as dummies to facilitate laundering the proceeds of the crime.

As a result of the STR analysis, review of banking and other FI transactions and further investigation by AMLC, the OMB received 17 financial investigation reports which presented as part of the evidence in its prosecution of the graft cases against high ranking government officials.

Cooperation and exchange of information/financial intelligence

160. AMLC has entered into MOAs and MOUs with 27 domestic agencies and 40 foreign counterpart FIUs, which encourages coordination and the exchange of information relating to the investigation of ML, predicate offences and TF to effectively prevent, control, detect and investigate unlawful activities. Based on the case studies submitted by the Philippines, many of the requests for information from AMLC were initiated by LEAs in instances where the operational investigation process involved coordination between AMLC and the agencies requesting the financial intelligence. AMLC also

supported requests from supervisors, including BSP, IC and SEC. As reflected in the statistics for the requests for information from AMLC, most of its MOAs are operationalised, with counterparts utilising the agreements to seek information. AMLC also makes regular requests for information from some agencies to support its analysis.

161. With respect to domestic requests for information or disclosure, replies are made via sealed individual envelopes and are hand carried to the requesting agency by authorised AMLC personnel. An electronic information sharing protocol was developed and is currently being tested to enable faster, more efficient and secure sharing of intelligence with LEAs.

162. In relation to terrorism and TF, there are various coordination mechanisms established to share information, including the JTFIG. This serves as a platform to validate intelligence, which feeds into the investigations of relevant agencies. JTFIG intelligence provided support in TF investigations, including the filing of TF cases. AMLC provided an example of a TF case that resulted in the freezing of accounts and prosecution for kidnaping for ransom for TF, arising from intelligence sharing via JTFIG

163. Information exchange between AMLC and other competent authorities is required to be carried out securely⁶⁴, to ensure the confidentiality of the information exchanged and used. At the time of the onsite visit, the assessment team was advised that there had not been any breaches of confidentiality of the information exchanged or used. According to the Philippines authorities, to ensure timeliness of information sharing, informal exchange of information among LEAs and domestic partners occurs and works effectively. AMLC also disseminate financial intelligence information during meetings, seminars, dialogues, case conferences, or training courses for LEAs. If it is necessary, intelligence is shared through text messages or emails for faster response. Both parties meet to discuss the overall modus operandi for the predicate offence and the ML, identify cohorts, the extent of financial transaction and network, identify gaps in the investigation and determine how to address them. However, the protection of the confidentiality of information exchanged and used through these informal channels may not be entirely secure due to the medium of exchange.

Overall conclusions on effectiveness with Immediate Outcome 6

164. While short on resources to fully implement its functions, AMLC's FIU is generally functioning appropriately, with access to a wide range of information, in particular the wealth of information provided under the CTR framework. AMLC continues to increase its capacity by streamlining its resources and investing in appropriate tools and systems. The number of proactive and reactive intelligence products disseminated for the purpose of ML, TF or associated predicate offence investigation is modest in the context of the Philippines. There has however been some success achieved through intelligence sharing in cases conference and task forces. As a hybrid FIU, AMLC's FCIG is the biggest user of FIAG financial intelligence, which supported some ML investigative processes. There are impediments in relation to disclosures on PEPs to other LEAs during election periods. The use of financial intelligence (by FCIG or other LEAs) does not frequently feed into investigations into ML, TF, associated predicate offences or tracing of assets in line with the risk, materiality and context of the Philippines. There are practical impediments to other LEAs developing and using financial intelligence arising from AMLC being the sole agency able to access bank records. AMLC would need to be a far larger agency to effectively perform the role on behalf of all agencies if financial investigations were pursued in keeping with the risk profile.

165. **The Philippines has a moderate level of effectiveness for Immediate Outcome 6.**

⁶⁴ Pursuant to the 2018 Implementing Rules and Regulations of the AMLA as amended
Anti-money laundering and counter-terrorist financing measures in the Philippines © APG 2019

Immediate Outcome 7 (ML investigation and prosecution)

ML identification and investigation

166. AMLC is the primary designated authority to investigate ML offences, in addition to its function as the FIU of the Philippines. PNP is empowered to enforce all laws and investigate and prevent crimes, including ML. NBI has authority to investigate specific crimes, including transnational crimes, commercial, economic and financial crimes and also to undertake the investigations of any crimes as authorised by the Secretary of Justice or the President of the Philippines. Thus, both PNP and NBI are also able to conduct ML investigations. However, neither PNP nor NBI investigate ML in practice.

167. AMLC's FCIG is responsible for investigating ML/TF offences as well as financial investigations to trace assets. At the time of the onsite visit the FCIG consisted of 18 persons skilled in law, IT and forensic accounting. In July 2018 a decision was taken to increase the established positions in FCIG to 51. FCIG's 18 officers are responsible for investigating ML, but also supporting other agencies to access banking and other financial records.

168. FCIG investigators have generally well developed financial investigative skills and expertise and conduct investigations guided by a financial investigations manual. They use their limited investigative powers under the AMLA to conduct ML investigations and have the ability to enlist assistance of other government agencies, including LEAs, to access the fuller range of LEA powers. FCIG has direct access to the financial intelligence of the FIAG. FCIG has received financial investigation training internationally and/or locally. AMLC has developed a financial investigation training module, with the support of an international organisation. In addition to development of expertise within AMLC, investigators in LEAs with financial investigation units reported that they had received financial investigation training.

169. FCIG is able to access a very wide range of records from FIs and DNFBPs. FCIG is the only LEA able to access bank records for its own investigations or on behalf of other LEAs and must show probable cause that the deposits or investments, including related accounts, may be connected with any of the unlawful activities listed in the AMLA.

170. FCIG, as the designated ML investigating agency, is not empowered in its own right to conduct searches and seize evidential materials/assets, take witness statements (presently limited to covered persons and government agencies) and use of special investigative techniques. The team finds that AMLC's lack of the full suite of LEA powers hinders the extent to which FCIG can effectively investigate ML. Notably, the AMLA provides AMLC with the authority to draw on the powers of other LEAs to overcome some of these gaps and coordination agreements are in place to assist with evidence collection by FCIG.

171. FCIG has initiated a total of 277 investigations related to ML between 2013 and 2018. These were initiated from a range of sources including through FIAG intelligence reports, STRs and CTRs deemed suspicious; referrals from LEAs; requests for assistance or information (domestic or international); confidential informants; and media reports. For example, the complex Bangladesh Bank investigation was initiated by a phone conversation and a SWIFT message from the Governor of Bangladesh Central Bank (see case study 3.08).

Table 3.14: Triggers directed to the FCIG for investigation (2013 - 2018)

Trigger	2013	2014	2015	2016	2017	2018*	Total
Reactive Financial Intelligence Reports (RFIRs) including requests for information & LEA referrals	112	98	68	446	411	158	1293
Proactive financial intelligence reports (PFIRs)	78	97	23	13	08	43	262
Total	190	195	91	459	419	201	1555

3

172. As displayed in Table 18 above, there were 1555 total triggers, comprising of RFIRs and PFIRs, during the review period 2013 to November 2018, which led to the conduct of 277 investigations by the FCIG. This comprised of 257 investigations arising from RFIRs and 20 arising from PFIRs. As a result of these investigations, FCIG referred 81 cases to the Legal Evaluation Group (LEG) within AMLC for filing of civil forfeiture and/or ML complaints. Out of these 81 cases, 42 petitions were filed for civil forfeiture and 20 ML cases filed before DOJ (16) and OMB (4). While the exact proportion of the 20 ML investigations that were triggered by PFIRs and RFIRs including LEA referrals cannot be determined, this number is extremely low in comparison to the high number of predicate investigations into high risk proceed generating crimes, such as drugs - 146,624 (2013-2017); graft and corruption - 46,654 (2013-2017); fraud/fraud and swindling - 19,645 (2015-2017); human trafficking - 920 (2015-2017) and intellectual property violations - 962 (2015-2017).

173. Amongst the 20 ML cases filed before DOJ and OMB, none related to the predicate offences of smuggling, intellectual property violations, environmental crimes or firearms, all of which pose a high level threat to the ML risk in the Philippines. A number of the 89 pending ML investigations relate to smuggling and IP violations.

Case Example 3.08- Bangladesh Bank Heist

The Bangladesh Bank / US Federal Reserve Bank of New York (FRBNY) heist took place on 4 February 2016, with 35 fraudulent instructions via the SWIFT System to withdraw USD1 billion from the account of Bangladesh Central Bank (BCB) held at the US FRBNY. This was the result of an unauthorised access into BCB's computer system which instructed the transfer of the funds from BCB's account with the FRBNY. Five of the 35 fraudulent transfer instructions were followed resulting in transfers of USD101 million. Of this, USD20 million was transmitted to Sri Lanka and USD81 million was transmitted into four personal accounts in the Philippines.

An investigation into the USD81 million transferred to the Philippines was initiated by AMLC on 11 February 2016, following a phone call and a SWIFT message from the Governor of BCB. There was no domestically generated initial alert or STRs reported by a covered person. However, Remittance A, a money transfer agent later reported the transaction to AMLC via a letter on 17 February 2016. The report was not in the required STR format because Remittance A was not registered to report to AMLC.

AMLC investigations revealed that five Philippine bank accounts were involved, with four of these accounts opened on 15 May 2015, more than eight months prior to the heist. The identities of the account holders were found to be fictitious. A fifth account was opened in the name of WSG, a businessman on 5th February 2016, with the initial deposit via fund transfer of USD22,735,000 from one of the fictitious account. The manager of a Bank B Branch, referred to as MD, personally attended to the opening of these fictitious accounts in her branch.

KW, a junket agent in M and S Casinos introduced GS, a Chinese casino player, and the purported account holders, to MD who allegedly gave them the account opening forms to fill out. The initial deposit was USD500

per account. USD65 million (including the initial fund transfer USD22,735,000) was transferred to the account opened in the name of WSG from 5 to 9 February 2016. Finally, Remittance A received a total of USD80,884,641 from these fund transfers including a direct transfer of USD 15 million.

Remittance A claims that it disbursed the \$80.8 million via remittances of USD29 million on 5 and 10 February 2016 to BMB Resort and Hotels (BMBRH) for S Casino; remittances of USD 21,245,500 on 10 and 11 February 2016 to Corporation C (owned by KW); and cash deliveries of more than USD30 million on 5 to 13 February 2016 to WX, who is a Chinese player in S Casino.

On its own initiative, S Casino (which was not a covered person at the time) suspended and held chips worth PHP 107 million (USD2.06 million) and cash of PHP 1.3 million (approx. USD25,000). Eventually KW turned over USD15 million to AMLC, which he alleged to be part of the money abandoned by GS and his group. The said amount was returned by the Philippines to Bangladesh on 10 November 2016 pursuant to the Partial Order of Forfeiture issued by the Regional Trial Court in Manila.

Investigators concluded that KW was accountable for some USD19 million and Remittance A for some USD17million. As the amounts subject to AMLC forfeiture cases against individuals and companies do not provide full recovery for Bangladesh Bank, further investigations are being conducted.

Evidence gathered by AMLC during the investigation also showed that officials of Bank B had either: (i) knowledge of the illegal source of the funds; or (ii) opportunity to stop the transactions but chose to ignore the red flags, constituting wilful ignorance or constructive knowledge that the funds transacted were related to a predicate offence.

AMLC submitted investigation materials to the DOJ recommending ML charges against the bank manager (MD) (being the only individual in the bank charged) and 11 other individuals (including employees of the Remittance A). Having considered AMLC recommendations, the DOJ filed charges against MD for facilitating ML. However, recommended ML charges against five responsible officers of Corporation C and Remittance A was dismissed by DOJ due to lack of sufficient evidence. AMLC is seeking a review of this decision by the DOJ. In addition DOJ has resolved ML charges against six officials of Bank B. However, these respondents filed motions with the DOJ to reconsider its decision.

Table. 3.15: ML investigations completed by AMLC

Predicate Crime	Number of ML Investigations submitted to DOJ and OMB						
	2013	2014	2015	2016	2017	2018	Total
Fraud	-	-	2	-	-	-	2
Qualified Theft	-	-	1	1	-	-	2
Drug Trafficking	1	-	2	1	-	3	7
Violation of e-Commerce Act	-	-	-	4	-	-	4
Human Trafficking	-	-	-	-	1	-	1
Graft and Corruption ⁶⁵	-	-	-	-	-	4	4
Total	1	-	5	6	1	7	20

174. The primary LEAs for investigating predicate offences in the Philippines are PNP, NBI, PDEA, OMB, SEC and BOC. These LEAs routinely investigate predicate crimes. PNP, NBI and PDEA have

⁶⁵ Referred to OMB and pending decisions

financial investigation units, with operational manuals on investigating financial aspects of predicate crimes. These units can approach AMLC with a specific request to access the bank records necessary for financial investigations, although this is rarely done in practice.

175. Financial information contained in non-bank transactions may be accessed by LEAs through the use of subpoena powers and other investigative tools, including by requesting AMLC. In these circumstances, the LEAs' clear focus is to secure evidence to support their predicate crime investigations. If any matter relates to ML, it is referred to AMLC.

176. FCIG conducts ML investigations in collaboration with the respective LEAs. This collaboration is facilitated by case conferences and MOAs between AMLC and the LEAs. Some relevant information to support FCIG ML investigations are received from amongst the 989 referrals (from 49 competent authorities) made to the AMLC during the six-year review period. However, these 'referrals' include requests for AMLC financial intelligence or bank records to be provided to LEAs or other competent authorities. AMLC indicated that 437 of the requests were responded to with available information or the information sought from LEAs is unavailable (see IO.6).

177. Challenges to LEAs conducting financial investigations, as a consequence of limited access to financial information, is addressed in the recently approved NACS. Strategic objective 1, Action No. 2 seeks to allow relevant government agencies to examine bank accounts for a legitimate purpose, including while exercising their investigative or supervisory powers. It is noted that it will be very important for strong safeguards and integrity checks to be in place for other LEAs to directly access bank records.

178. One of the primary outcomes of FCIG's participation in the investigation of predicate offences is the application for civil forfeiture (discussed further in IO.8). This is reflected in the statistics, where out of 277 inquiries addressed by AMLC, 42 related to the pursuit of civil forfeiture actions; whereas only 20 cases were identified for ML. There were 57 petitions for freeze orders within the review period. Notably, the period of validity of a freeze order of six months is likely inadequate to complete complex ML investigations, especially those involving cross border organised crimes or ML connected with foreign predicates. Pursuit of civil forfeiture actions in preference to ML investigations may be a consequence of this time limitation. A high proportion of freeze orders have resulted in petitions for civil forfeiture (42). This may be in pursuit of securing a Provisional Asset Preservation Order (PAPO) within the six months period of validity of a freeze order. The following case study illustrates this point, with opportunities to pursue ML are clearly overlooked in favour of civil forfeiture action.

Case Example 3.09 - PEP

In 2014 OMB investigated the former Mayor of the City of M, following complaints of overpricing of construction contracts. The allegation was that a new parking building was built at an excess cost of PHP1.3 billion, which is over 500% above expected costs. The building was ultimately constructed at a cost of PHP1.56 billion. It was further alleged that a new high school should have cost approximately PHP147 million, although the building contractor was paid PHP1.3 billion.

In 2014 FCIG initiated a financial investigation based on media reports, Senate hearings and a referral from the OMB in relation to the former Mayor of the City of M, members of his family and alleged dummies. Two investigation reports were provided to OMB in November 2016 and May 2017 showing several bank accounts, especially those of the former Mayor (referred to as JB) and his joint accounts with his secretary (EM) and his finance officer (GL) among others, exhibited multiple large transactions amounting to billions of pesos coinciding with the period of the construction of the parking and high school buildings.

FCIG also investigated the bank accounts of AT, a close friend of JB, suspected to be acting as a dummy for the latter in several companies and acquiring properties. These companies though disclosed as owned by AT, were in fact controlled by JB and his wife. AMLC also inquired into the accounts of SB Law Firm which has multiple links to JB, whose daughter was a partner in the firm. One of the senior partners of the firm is a major shareholder in GH, Inc., a company managed by AT and also allegedly owned by JB through dummies. AMLC's investigation discovered that multiple cheques involving millions of pesos were drawn against the accounts of persons linked to JB and his alleged dummy entities, and eventually deposited, credited, or transferred to SB Law Firm's accounts. Bank documents also established that SB Law Firm was principally involved in the transfer of funds across accounts owned by persons and entities with clear links to JB.

AMLC froze 242 bank accounts, insurance policies, and securities of JB, his son and daughter, SB law firm and GH inc., a company managed by AT and also owned by JB through dummies, through the OSG, in May 2015. In November 2015, AMLC filed a petition for civil forfeiture in relation to violation of Anti-Graft and Corrupt Practices Act and to plunder under the Plunder Act.

While FCIG engaged in complex analysis of the financial background of the case initiated by OMB, no action was taken in relation to ML. The response to identification of proceeds of crime was limited to civil forfeiture.

179. The very high workload of AMLC, and in particular the newly formed FCIG results in too few resources for the FCIG to identify and investigate ML elements of many cases. There are presently 18 officers responsible for investigating ML, who also carry the weighty responsibility of supporting other agencies with their investigations of related predicate crimes through seeking access to banking and other financial records. The assessment team was informed that the number of investigators will be increased up to 51 once fully staffed, however this is unlikely to occur until the end of 2019. Even with that number, they would not have enough staff to meet demands of bank records from other LEAs if they were conducting financial investigations in keeping with the risk profile.

180. Overall, the quality of investigations and subsequent briefs of evidence appear to be of reasonable quality, but the numbers of completed investigations that have led to prosecutions is low. There is no indication that prosecutors or the courts identify weaknesses with evidence collection. One area requiring greater attention is the pursuit of MLA to include foreign evidence as part of the briefs, when transnational elements are present.

181. LEAs make very few requests to AMLC to conduct ML investigations in parallel with their predicate investigations. A number of factors contribute to this lack of focus on the ML aspect, including a lack of priority assigned by LEAs to 'following the money' related to stand-alone or third party ML; a perception that there are already dissuasive sanctions available for high risk predicates; a lack of capability amongst LEAs to identifying potential ML elements; and practical delays posed by the bank secrecy legislation to access financial information via AMLC.

182. Considering the risk profile of proceeds from corruption and bribery, there were very few requests for AMLC to conduct parallel ML investigations. OMB, the lead anti-corruption agency, investigated 46,654 cases of graft and corruption between 2013 and 2017. While not all of these may have been predicate offences, only 41 cases were referred to AMLC in that period, with only four ML investigations being submitted to OMB, in its capacity as prosecutor, by AMLC, in order to consider ML charges. This is significant given that graft and corruption pose a high risk of ML, as documented in the 2015 and 2017 NRAs. Contributing factors may be the limitation placed by courts (Marquez v. Desierto

G.R.No. 135882. June 27, 2001) on OMB's access to financial information and pursuit of ML not being a priority within the agency.

183. One of the AMLC's most complex corruption-related matters was the investigation into the PDAF scam (see IO.8 case study), originally referred to AMLC in 2013 by NBI and OMB, and four ML cases were submitted to the OMB to consider ML charges, with civil forfeiture action having been filed in 2014. The matter involved wide reaching parallel predicate investigations which resulted in at least 32 Plunder and Corruption cases against high ranking officials. While this case is amongst the most complex ML case, there is a concern that other LEAs reluctance in seeking parallel ML investigations may be the influenced by long timeframes for complex ML matters to be complete, which reflects the nature and complexity of the case and the resource limitations.

184. The availability of civil forfeiture influences decisions regarding the priority given to ML investigations in response to referrals from LEAs. AMLC's focus on following the money relates mostly to forfeiture of assets, due to a lower burden for civil forfeiture than building a criminal ML case. Statistics in relation to civil forfeiture actions filed (see IO.8) demonstrate that the Philippine authorities prioritise the use of this mechanism to seek to deprive criminals of their assets, in preference to pursuing ML. In recent cases AMLC ML investigations have continued even after the filing of the civil forfeiture case.

185. The assessment team acknowledges that AMLC works well with other agencies, with several examples of joint investigations (see case study below). However this collaboration does not often extend to the prosecution of ML.

Case Example 3.10 - Joint investigations

- AMLC investigation against a Vice Mayor and his brother was supported by PNP-CIDG and PDEA whereupon AMLC was able to submit the investigation file to the DOJ in order to consider ML charges.
- AMLC investigations into a drug personality was a combination of work with PNP and PDEA which ended with the filing of a civil forfeiture action.
- AMLC investigation into the Bangladesh Bank heist was conducted with the collaboration of NBI and PNP. AMLC submitted investigation files to the DOJ to consider ML charges which resulted in an individual being charged by the DOJ for ML. In addition, AMLC filed civil forfeiture actions.
- AMLC investigation into the PDAF scam was the combined effort of the NBI and OMB. AMLC submitted investigation files to OMB to consider ML charges. In addition, AMLC filed civil forfeiture actions.

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

186. As outlined above, FCIG conducted 277 investigations into ML. 20 ML investigations have been finalised and referred to DOJ or OMB for prosecution, which resulted in 10 prosecutions of ML.

187. Primarily, there are three prosecuting agencies involved in AML/CFT related investigations and prosecutions. OSG acts as the legal counsel to all government agencies, including AMLC, and in particular assists in the filing of bank inquiries, freeze orders, civil forfeiture actions initiated by AMLC. However, ML prosecutions are within the mandate of the DOJ, as the public prosecutor. However, at the appellate level, OSG acts as the counsel and prosecutor. OMB, being Philippines' leading anti-corruption agency, plays a dual role as prosecutor for cases of graft and corruption, including where they relate to ML. Prosecutions by OMB occur upon referrals by AMLC, as the OMB does not investigate ML.

CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

188. The Philippines' 2017 NRA allocated a high level of overall risk to ML; and the following predicate offences are assessed to pose a high level threat: drug trafficking, graft and corruption, fraud and swindling, smuggling, intellectual property violations, environmental crimes, firearms for crimes and tax crimes. Tax crimes are however not included as predicate offences for ML. Sectors posing a high risk for ML are casinos, MSBs and banks.

3

189. Complex financial investigations are not generally directly supported by prosecutors until very late in the process, which may contribute to the few ML investigations which result in referrals for prosecution. During the onsite, DOJ advised that as a policy practice it is not authorised to interfere in investigations, nor give opinions during the investigation stage. However, DOJ is open to reviewing this separation of roles for ML cases, in light of the rate of attrition between ML investigations by FCIG (277 investigations) and those filed in court as prosecutions (10 prosecutions of ML). DOJ representatives supported establishing a separate unit to provide guidance to LEAs on ML cases, in order to maintain the policy of non-interference in ongoing investigations.

190. In relation to ML prosecutions discussed above, the predicate offences involved were fraud (3), qualified theft (4) and one prosecution each for drug trafficking, kidnapping for ransom and violation of Electronic Commerce Act. Of these, only fraud (3) and drug trafficking (1) are high risk predicate offences. There have been no prosecutions for ML related to graft and corruption, smuggling, intellectual property violations, environmental crimes and firearms for crimes. In terms of sectoral threats, while the casino sector poses a high level of overall vulnerability, ML abuse in that sector has only been investigated once.

Table 3.16: ML Trials pending in courts

Predicate Crime	Number of ML Cases Filed in the Courts					
	2013	2014	2015	2016	2017	Total
Fraud	1	-	1	1	-	3
Qualified Theft	2	1	-	1	-	4
Drug Trafficking	-	-	-	1	-	1
Kidnapping for Ransom	-	-	-	-	1	1
Violation of Electronic Commerce Act	-	-	-	-	1	1
Total	3	1	1	3	2	10

191. Investigations that were completed by FCIG and referred to a prosecutor relate mostly to domestic predicate offences, with a single case relating to foreign predicate offences. This is despite the external threat assessment in the 2017 NRA concluding that the threat from proceeds of crime committed outside the Philippines is high.⁶⁶ Predicate offences occurring in the Philippines, with the proceeds laundered overseas, have been pursued to prosecution in only one instance; the large and complex PDAF case. Investigations into ML have not sufficiently extended to high level organised crime, with very few examples (including the Bangladesh Bank heist case) involving cross border ML offences.

192. As seen in the case example below, it is apparent that opportunities have been missed in relation to the investigation of foreign predicate offences with laundering taking place in the Philippines.

⁶⁶ NRA 2015-2-16, page 13

Case Example 3.11- MLA request

In March 2016, DOJ referred an MLA request received from a foreign partner to the AMLC in connection to the prosecution of two individuals for fraud related to options/futures scam in that country which had generated approximately USD240,000 in proceeds. The MLA sought pertinent banking information from the Philippines to determine account opening details and trace the flow of funds. After filing an *ex parte* application for bank inquiry before the Court of Appeals, AMLC secured the relevant bank records and transmitted the same to the DOJ in November 2016. Authorities did not demonstrate that ML or predicate investigation were initiated in the Philippines in relation to the funds or individuals.

193. Despite fraud-related ML being a serious risk in the Philippines, and the evident use of Philippines' FIs in ML, domestic fraud-related ML investigations have not been conducted, either jointly with the other jurisdiction or separately. The exception shown to the team was the Bangladesh Bank heist case, which did not take criminal action in relation to possible breaches by the FI. A senior employee of the bank branch involved has been convicted for facilitating ML.

194. Prosecutions for ML, ten in total over the review period, are disproportionately and remarkably small in number compared to prosecutions for predicate offences in the Philippines.

Types of ML cases pursued

195. The ML prosecutions pursued were mostly connected to self-laundering from domestic predicate crimes. Prosecutions have been undertaken for third party laundering and stand-alone ML. In six cases pursued by AMLC, individuals such as bank managers or officers, remittance company officers or persons involved in real estate transactions were charged with ML despite not being involved in the commission of the underlying offence (third party laundering). Prosecutors in some cases have also demonstrated the use of ML charges in standalone ML prosecutions without the associated predicate offences being charged at the same time (for example the Bangladesh Bank Heist).

196. The Bangladesh Bank Heist is the only example of a local ML investigation linked to foreign predicate offences. While this case reflects AMLC's ability to investigate stand-alone ML. The dismissal of aspects of the case on the grounds of inadequate evidence appears to show some missing links within the processes connected with investigation and prosecution; however it is noted that further investigations were continuing at the time of the onsite visit.

197. The authorities' main focus in pursuing ML cases is in respect of natural persons. FCIG's investigation into the PDAF scam is the only instance involving abuse by legal persons and third parties to launder funds. There is an example of information exchanged with a foreign jurisdiction involving funds being laundered through legal persons in the Philippines, but no ML investigations were initiated in this respect.

198. As a part of the PDAF investigation, 525 bank accounts were initially frozen involving nearly PHP 98 million (approx. USD2.180 million) and USD593,000. Thereafter, an additional 384 accounts in 26 financial institutions were frozen. The investigators were able to identify the use of NGOs and third parties to launder funds. On conclusion of the investigation, AMLC filed civil forfeiture action and four ML complaints with the OMB for filing ML charges. It was not demonstrated that ML charges are being considered against legal persons (NGOs) or third party laundering (see IO.8).

Effectiveness, proportionality and dissuasiveness of sanctions

199. The Philippines has secured five ML convictions of natural persons over the period 2013-2018 for ML. No convictions have been secured against legal persons. The ML convictions related to proceeds from fraud, kidnapping for ransom and qualified theft (akin to embezzlement). Sanctions primarily consisted of lengthy terms of imprisonment and fines. There have been no acquittals of ML charges.

3

Table. 3.17: ML Convictions - Sanctions Applied

Case	Number of counts	Terms of imprisonment	Fine (PHP)	USD (approx.)
Case 1	1	7 to 14 years	3,000,000	57,000
Case 2	55	7 years for each count	9,860,615	188,000
Case 3	1	8 years	500,000	9,500
Case 4	1	7 to 13 years	34,099,195	649,590
Case 5	55	4 to 5 years for each count	1,500,000	285,750

200. In the very limited number of cases (5) where convictions were secured, sanctions applied, were effective, proportionate and dissuasive.

201. There are substantial delays in progressing prosecutions in the courts, with ML trials routinely taking upwards of five years to reach first conviction. Information was provided that AMLC was reviewing possible improvement strategies with the Supreme Court to reduce delays.

Other Criminal Justice Measures

202. There are no criminal justice measures specifically pursued as an alternative to ML convictions. It is also not apparent that there are any justifiable reasons why ML convictions are not possible to secure.

Overall conclusion on Immediate Outcome 7

203. The Philippines has the systems in place to investigate and prosecute ML. However, there are limitations in the capability and empowerment to investigate and prosecute ML. The ML investigations and prosecutions that have been conducted are not sufficiently aligned with the ML risk profile. There are significant discrepancies between the investigation of predicate offences, the resulting referrals or triggers for related ML investigations, the number of completed ML investigations filed for prosecution and ultimately the number of prosecutions undertaken, and convictions secured. The preference of LEAs to use civil forfeiture mechanism as a swift response to proceeds generating crimes also contributes to the low level of ML cases (10 prosecutions, 5 convictions, 0 acquittals). ML investigations related to foreign predicate offences are infrequently pursued.

204. **The Philippines has a low level of effectiveness for Immediate Outcome 7.**

Immediate Outcome 8 (Confiscation)***Confiscation of proceeds, instrumentalities and property of equivalent value as a policy objective***

205. NACS includes a policy objective (Objective 3) to pursue asset recovery in ML, predicate offences and TF cases, focusing on identified high-risk crimes. AMLC has taken a good number of steps, but this policy goes well beyond the AMLC and the policy has not yet been effectively implemented.

206. AMLC has authority to freeze assets and initiate civil forfeiture actions under the AMLA in relation to any unlawful activity. OMB has the power to initiate civil indemnity actions against assets unlawfully amassed by government officials.

207. AMLC and OMB lack some powers of seizure (moveable property) and are empowered to seek the assistance of other empowered agencies. In situations where the property is movable and can be subject to flight, power to seize is essential to protect against risk of flight pending a freezing order. Notably, AMLC has authority to administratively freeze assets related to TF for up to 20 days; and subject to extension for six months upon petition to Court of Appeals. Other LEAs, particularly NBI, PNP, PDEA and BOC, have the power to seize property, but in practice this is mostly done for evidentiary, rather than asset recovery purposes.

208. AMLC, as the main agency with the responsibility to confiscate criminal proceeds through civil forfeiture actions, demonstrated a focus on depriving criminals of the proceeds of crime. However, for AMLC and LEAs, following the money and asset tracing actions have been focused on domestic assets, with limited demonstration of efforts extending to assets moved to other jurisdictions and proceeds of foreign predicate crimes.

209. The AMLA provides for confiscation of property of equivalent value. There has been an increase in cases of seeking civil forfeiture in this regard since 2017-18, which is a welcome development and reflects a heightened policy priority on property of corresponding value.

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

210. The Philippines has several laws with provisions for confiscation and provisional measures, such as the AMLA, Act Declaring Forfeiture In Favor of the State Any Property Found to have been Unlawfully Acquired by Any Public Officer or Employee, Revised Penal Code, the Comprehensive Dangerous Drugs Act, Revised Forestry Code of the Philippines, Philippine Fisheries Code, The National Internal Revenue Code (NIRC), the Customs Modernization and Tariff Act, the National Caves and Cave Resources Management Protection Act.

211. The primary mechanism to recover assets in the Philippines is the use of non-conviction based civil forfeiture by AMLC and OMB. This has mostly been limited to property discovered over the course of investigations and extends to proceeds and instrumentalities involving foreign predicate offences (two instances, discussed below) and proceeds which have been moved to other countries (one instance, the PDAF case), in limited instances only. Only two cases of repatriation and sharing (discussed below) to another jurisdiction were shown. Restitution to victims within the jurisdiction has occurred in the period prior to this assessment.

212. AMLC is the competent authority primarily engaged in the confiscation of assets related to ML and TF (through civil forfeiture). Other LEAs perform confiscations primarily for evidentiary purposes as part of their responsibility for predicate offences.

213. Article 45 of the Revised Penal Code provides that every penalty imposed for the commission of a felony carries with it the forfeiture of the proceeds of the crime and the instruments or tools with which it was committed. LEAs indicate that items discovered during searches, including seizures arising from violation of intellectual properties and drug related offences, are seized as evidence and subsequently forfeited to the courts, if a conviction is achieved against the defendant/s. The PDEA provided details of one confiscation involving vehicles and a real property. In the absence of any data demonstrating the implementation of art.45 of the Penal Code, the assessment team can only conclude that conviction-based confiscation of instruments and proceeds of crime is not being regularly pursued in practice.

214. AMLC was able to secure only eight confiscations during the review period, amounting to 39 million PHP (Approx. USD15,760,000). Over 95% of this total was confiscated in a single matter (the Bangladesh Bank Heist). The predicate crimes associated with these confiscations were fraud (5), drugs (1), corruption (1) and Violation of E-commerce Law (1). There were no confiscations on instrumentalities of crime or assets of equivalent value, but assessors note that pending civil forfeiture actions include instruments of crime and property of equivalent value.

Table 3.18: Completed confiscations by AMLC

Predicate Crime	No. of Petitions for CF	Year Filed	Value	Other Assets (Approx. value in PHP)
2013				
Fraud	2	2003 & 2009	21,724,671	-
2014				
Fraud	2	2003 & 2009	963,351	-
2015				
None	-	-	-	-
2016				
Drug trafficking	1	2004	3,700,770	-
Corruption	1	2015	3,430,783	-
E-commerce violations	1	2016	USD15,000,000	-
2017				
Fraud	1	2003	10,069,800	-
Total	7	NA	PHP789,889,375 million PHP (Approx. USD15,760,000)	-

215. The table below sets out the details of the 41 civil forfeiture actions pending in court (filed within the review period). The assets in these cases are subject to Asset Preservation Orders (APO). In addition, there are 32 pending civil forfeiture actions filed between 2003 and 2012. Notably, some of them have been pending since 2003. The prosecutors explained that the lack of designated courts to file charges in relation to financial crimes and the turnover in the judiciary were the main challenges in progressing these cases.

Table 3.19: Civil Forfeiture Actions pending in Court

Predicate Crime	Petitions for CF	Estimated Value (PHP)	Other Assets (Approx. value in PHP)
2013			
Fraud	4	3,877,911,807	Real Properties - 26 million; Motor Vehicles - 58 million; Insurance Policies 22 million;
Drug trafficking	1	36,541,292	-
Kidnapping for ransom	1	65,434,369	-
2014			
Fraud	1	10,123,684	-
Graft/Corruption, Plunder, Malversation of public funds	2	163,294,333	Insurance Policies 22 million real property 171,321,595 Motor vehicles(15);15,142,000
Drug trafficking	4	34,077,385	Motor vehicle;430,000
2015			
Graft/Corruption, Plunder, Malversation of public funds	2	124,228,450	Shares of Stock;44,116,578, Nineteen (19) Real Properties 54,421,920
Human trafficking, illegal recruitment	1	13,440,764	-
Drug trafficking	4	55,730,078	4 Real Properties; 3.8 million; 8 motor vehicles – 4.6 million
2016			
Fraud	2	12,054,540	-
Drug trafficking	3	9,779,000	-
Violation of E-Commerce act	1	729,137,396	-
2017			
Human trafficking, illegal recruitment	1	3,761,046	-
Drug trafficking	6	819,198,158	2 motor bancas, 7 motorcycles, 26 motor vehicles (3 as instrumentalities of the predicate crime), 14 real properties (1 as an equal value asset); 3 vessels; 8 firearms
Violations of the e-Commerce Act	2	99,684,114	incl estimated value of 19 real properties and 6 motor vehicles - forfeited as equal value assets
2018			
Fraud	2	21,510,249	-
Drug trafficking	2	29,666,829 (4,234,896 forfeited as equal value assets)	1 motor vehicle & motorcycle (being forfeited as an instrumentality of the predicate crime), 2 real properties (lots); 2,311,364, 2 motor vehicles;1,260,000
Kidnapping for Ransom	1	509,560	-
Terrorism and TF	1	498,653	-
Total	41	PHP 6,106,581,707 (approx. USD 117 million)	

216. Amongst the civil forfeiture actions pending in court listed in the Table above, there were two instances of civil forfeiture actions filed based on instrumentalities of crime, comprising of four motor vehicles and a motorcycle and these are relatively low. Forfeiture actions in three instances cover assets of equal value represented by 20 real properties, six motor vehicles and two bank accounts with the total balance of PHP 4,234,896 (approx. USD 80,675).

217. As such it cannot be said that competent authorities are taking action to confiscate instrumentalities of crime, and property of equivalent value to a large or proportionate extent.

218. Filing of cases for civil forfeiture has increased since 2013. In the early period, fraud was the main unlawful activity. Since 2013 fraud, drugs, corruption and hacking (cybercrime) have been the main areas of unlawful activity. Notably, the Philippines can file civil forfeiture actions against legal persons. As a part of the Bangladesh Bank Heist investigation (see IO.7), civil forfeiture cases were filed against the remittance company involved and its responsible officers.

219. Considering the Philippines risk profile, forfeited assets and pending civil forfeiture actions are not proportionate. In terms of results achieved it is also to noted that from 2013 onwards there has been a significant difference between the value of forfeited assets (totalling USD 15 million) and the pending claims (with an intended value of over USD 117 million).

220. No proceeds of TF have been forfeited, although two cases are pending, with approx. USD10,000 restrained in total.

221. AMLC uses provisional freezing orders (valid for a period of six months) in relation to ongoing investigations or prosecutions. There were 57 freezing orders reported during the review period valued at PHP 5,677 million (approx. USD 113 million). These freezing orders included bank accounts, real properties valued at PHP 251 million and vehicles/other properties valued at PHP 16 million. Within six months these freezing orders may be replaced by filing civil forfeiture actions to secure Provisional Assets Preservation Orders (PAPO). Amongst these freezing orders, there has been only two instances of TF and others are linked to high risk predicate offences, such as drugs, swindling, corruption, human trafficking and kidnapping for ransom. It is noted that the AMLA does not include a provision for the freezing of assets in situations where there are risks of transferring or hiding the assets.

222. OMB uses the remedy of civil indemnity to recover funds misused by government officials. However, there is a limitation in law to undertake civil forfeiture actions and OMB cannot petition for forfeiture within 12 months of a general election or six months of a special election, although the same provision holds that any limitation of actions cannot be invoked by, nor shall benefit the respondent, in respect of any property unlawfully acquired by him, which would see this provision only lead to delays, rather than avoidance of civil remedies to recover funds. The OMB's civil indemnity actions recovered amounts totalling PHP426 million (approx. USD 7.8 million) and USD17,547 from 2013-2018.

Table 3.20: OMB's Civil Indemnity Actions

Year	Case Counts	Amounts of Civil Damages/Indemnity (PHP)
2013	24	6,515,210
2014	24	5,435,587
2015	41	112,623,128
2016	76	271,121,972
2017	147	22,045,395
2018	78	9,077,716 & USD 17,547
Total	390	426,819,008 (approx. USD 8.1 million) & USD 17,547

223. BIR routinely recovers amounts on the basis of tax assessment procedures in relation to proceeds of crime. The Run After Tax Evaders Program (RATE) initiated in 2005 is a program to investigate and prosecute cases of tax evasion and other criminal violations of the National Internal

Revenue Code (NIRC). As of 31 October 2018, a total of 877 cases with assessments in relation to PHP143.95 billion (approx. USD2.66 billion) had been filed before the DOJ. It is unclear whether the above amounts include tax recoveries linked to criminal proceeds/instrumentalities. The RATE program has generated seven convictions, with only two convictions within the review period. Some of the amounts recovered by BIR likely relate to tax evasion, which is not designated as a predicate offence to ML in the Philippines. However, no clear statistics were provided to assess whether they have applied the tax assessment tools to detect and confiscate instrumentalities and proceeds of crime.

224. BOC conducted a similar program to RATE, a Run After Smugglers Program, and filed 113 cases with the DOJ. However, statistics provided were not sufficiently clear to come to a conclusion regarding the confiscation activity as a consequence of the program.

225. The assessment team is aware of two instances where the Philippines took action to repatriate assets based on foreign requests: one to the United States (see case study below) and to Bangladesh (see IO.7), both being the proceeds of foreign predicate offences. The case below with the US demonstrates very long delays in giving effect to processes to dispose of property and repatriate assets (almost five years). Notably, civil forfeiture proceedings in relation to the Bangladesh Bank Heist occurred much more quickly with the court issuing a partial order of forfeiture of USD 15 million, which was turned over to the Government of Bangladesh.

Case Example 3.12 – Repatriated assets to United States

In 2009, the US requested assistance in relation to investigations into frauds committed in the United States. AMLC conducted financial investigation which led to the discovery of bank accounts and several real properties in the Philippines in the names of the suspects. In 2010, AMLC secured a freeze order on these accounts and real properties and then filed a petition for their forfeiture.

The US District Court ordered the forfeiture of the real property and bank account. In May 2013, AMLC received a copy of a Motion for Approval/Recognition of Foreign Agreement seeking approval of the Second Preliminary Order of Forfeiture issued by the US Court and for issuance of a decision based on the said order.

The RTC-Makati City rendered a Partial Judgment directing the forfeiture of the real property and bank account. Accordingly, AMLC turned over the balance in the forfeited bank account.

With respect to the real property, the process is underway for the sale so the proceeds can be turned over to the US Government.

226. This is only one case where authorities pursued proceeds that had been moved outside the Philippines. The Philippines authorities also sent an MLA request to United States authorities to recoup the funds moved out of the Philippines in the PDAF scam (see case example below). International cooperation feedback received from foreign counterparts specifically noted that at least in one known instance, despite the identification of funds in other jurisdictions linked to suspected criminals, no further request came from the Philippines to seek restraint or confiscation of the funds.

Case Example 3.13 – PDAF / Pork Barrel Scam

The PDAF scam, also called the ‘pork barrel scam’, involves the alleged misuse of ten billion pesos (approx. USD185 million) by several members of the Congress of the Philippines of their Priority Development Assistance Fund (PDAF) allocation through the funding of agricultural "ghost projects". The PDAF allocated to certain legislators was deposited to the bank accounts of fraudulent NGOs through an individual named Ms N. The funds were withdrawn by Ms N’s employees and eventually split among Ms N, the lawmaker, officials of the implementing government agencies responsible for facilitating the transfer of funds and, in some instances, the local mayor or governor.

In 2013, the NBI and OMB requested AMLC conduct a financial investigation on the PDAF scam. Following AMLCs investigations, 525 bank accounts were identified and frozen involving approximately PHP 98 million (approx. USD 1.8 million) and USD 593,000. Thereafter, an additional 384 accounts found in 26 financial institutions were frozen in various currencies, amounting to PHP 135 million (approx. USD 2.4 million), USD163,000 and EUR 1400. In addition, AMLC discovered the purchase of life insurance policies valued at PHP 22.5 million (approx. USD 0.4 million) and USD140,000 and documents relating to 47 titles of real property and 16 motor vehicles were also identified.

Ms. N laundered the funds using two money changers to remit more than USD 5.26 million in favour of two companies owned by her daughter and brother. AMLC sought the assistance of the FIU in the foreign jurisdiction through ESW. The information gathered established that the money changers were acting as conduits for Ms. N in the transfer of funds. AMLC, NBI and OMB acted on the MLA request from that jurisdiction for the production of documents in relation to the seizure and eventual forfeiture of the properties of Ms N and members of her immediate family. Close coordination with that jurisdiction resulted in the filing of a civil forfeiture case against the assets of Ms. N found there, amounting to approximately USD 12.5 million, and the indictment of Ms. N and her cohorts in the Philippines for benefiting about USD 20 million PDAF by purchasing real estate properties and shares in two businesses in the overseas jurisdiction. Ms. N and her cohorts were also indicted in the overseas jurisdiction referred to above for conspiring to funnel in and out of the foreign jurisdiction some USD 20 million of Philippine public funds obtained through this multi-year bribery and fraud scheme.

In 2014, AMLC filed petitions for civil forfeiture before the courts in Manila. The petitions led to the issuance of APOs to cover the following: peso funds and investments totalling more than PHP155 million (approx. USD 2.8 million); USD bank accounts totalling approximately USD 697,000; 47 real properties; and 16 motor vehicles. This trial is ongoing. In 2018, four ML complaints, involving 32 counts of ML, were filed by AMLC before OMB.

227. Estimates of the full amount of defrauded funds in the PDAF scam are as high as PHP ten billion (approx. USD185 million). The civil forfeiture actions were filed in respect of PHP155 million (approx. USD 2.8 million), USD bank accounts totaling approximately USD 697,000, 47 real properties and 16 motor vehicles. However, no information was made available as to whether action was taken in pursuit of the application of property of equivalent value to cover the shortfall. Further, civil forfeiture action was filed in 2014 amounting to approximately USD12.5 million in respect of assets transferred to foreign jurisdiction (as yet unfinalised). The Philippine authorities are closely following the developments in the relevant jurisdiction and actions for eventual repatriation to the Philippines.

228. AMLC and other LEAs have procedures in place for asset management, however there are some concerns with effectiveness given that finalisation of court actions generally takes several years. The forfeited assets are handed over to the Bureau of Treasury. The assessment team is concerned

about the implementation of the process to realise the value of confiscated assets. The new AMLC structure will assist as additional staff have been allocated to enhance asset management.

229. Most of the issues discussed above have been identified as priority actions in the NACS, by proposing a new law to create an Asset Management Office which will provide mechanisms for the preservation and management of assets. AMLC advised that in July 2018 it established a unit within the Litigation and Evaluation Group (LEG) known as the Special Services Staff (SSS) with three officials, to manage and monitor frozen assets, those under a preservation order and under a judgment of forfeiture under the existing legal framework. The unit has been tasked with developing an inventory and remedies to preserve assets. AMLC has also developed a financial investigation training program focusing on 'follow the money' techniques.

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

230. Confiscation regarding falsely / not declared cross-border movements of currency and bearer negotiable instruments is not being applied as an effective, proportionate and dissuasive sanction by border/custom. Implementation of the cross-border cash/BNI declaration system produces very few declarations and even fewer interdictions, seizures, sanctions or confiscations for smuggled cash and BNI. The weak implementation of the system is not in keeping with the significant TF and ML risks for cash smuggling.

231. Despite being an archipelago nation with several entry/exit points and sea/air ports, the assessment team was only provided with statistics of confiscations at the Ninoy Aquino International Airport (which does account for approximately 65% of all visitor arrivals). No information was provided on the mechanism in place to detect cross border transportation of currency and BNI in the other entry/exit points or sea/air ports.

232. BOC is the responsible agency for confiscation of falsely or undeclared cross border transaction of currency and BNIs. There were 15 instances of currency confiscations (limited to Yen, Pesos, USD, Dinar and HKD) reported during 2013 to 2017, with no information on BNIs or on confiscations in 2018. Despite movement of cross border currency and BNI posing a high risk, the level of confiscations is very low.

Table 3.21: Seized Foreign and Local Currencies

Year	Total Seizures	Forfeited cases	Settlement	Forfeited Amounts
2013	9	6	3	Yen 87,009,000, USD 54,000
2014	7	4	3	Yen 51,980,000; PHP 4,355,000; USD 119,000; HKD 5,930,000
2015	4	3	1	Yen 3,100,000; PHP 880,000; USD 11,000; Dinar ⁶⁷ 413,000
2016	1	1	-	PHP 50,000
2017	1	1	-	PHP 2,528,000
Total	22	15	7	USD 2,424,465 equivalent

233. BOC's investigative actions in relation to currency detections were limited to identifying ownership and the purpose of money movement.

⁶⁷ No specific information

234. BOC and AMLC have an MOA based cooperation arrangement, and as a part of the MOA, BOC refers cross border currency declarations to AMLC. For the period of 2013- 2018, there were 7,000 inbound/outbound declarations. In the context of these declarations being one of the main sources of intelligence of AMLC (in relation to cross border currency and BNIs), the number received is low. LEAs did not demonstrate that financial investigations have been initiated based on the declarations specifically targeting ML/TF offences.

3

235. BOC has referred only four cases (detections of currency, drugs and precious stones/metals) to AMLC for smuggling charges. Two cases out of these are pending in courts and two are pending with the DOJ.

236. It is noted that BOC's capability may be limited due to the lack of clear policy priorities on the detection of false declarations or non-declaration of currency, and smuggling. During the onsite it was discussed that the shortage of human resources may be one of the contributing factors leading to the low level of detections. In response, BOC has commenced a number of enhancements to human and technical resources.

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

237. There were only eight confiscations during the review period, related to fraud (5), drugs (1), corruption (1) and e commerce violations (1), which is exceptionally low. As outlined above, conviction-based confiscation of proceeds and instruments of crime is not pursued. There are very few restraints of proceeds or instruments of crime and final orders for confiscation face very serious delays. The consistency of the confiscation results is not aligned with the Philippines' risk profile or the new national AML/CFT policies and priorities.

238. During the period of 2013 to 2018, cases filed for civil forfeiture related mainly to drugs, fraud, corruption, hacking (cybercrime) and human trafficking. Overall, the risks identified in the NRA and the articulated priorities of the government in relation to drugs appear to be reflected in confiscation activities. However, proceeds generating high-risk crimes such as smuggling, intellectual property violations and environmental crimes did not have asset recovery actions attached to law enforcement activity. Despite corruption being a high level threat for ML, there were limited confiscations during the review period. This could be the result of OMB's inability to access bank records limited by a judicial pronouncement.

239. It is noteworthy that during the review period there were no confiscations in relation to terrorism and TF offences, including those involving instrumentalities and equivalent value. There is a pending civil forfeiture action filed in 2018 with a substantial value of approximately USD 1 million. As a jurisdiction with high terrorism and TF risks, this does not reflect effective TF risks mitigation.

240. The confiscations in the newly emerging areas of cybercrime have not been effective. Confiscation of USD 15 million in the Bangladesh Bank Heist case is the first success in this area, although it represents only a fraction of the laundered funds. This is likely a consequence of limited criminality attached to web-related offences (limited to e-commerce).

241. It is likely that foreign predicate crimes related confiscations are a missed opportunity other than the two cases referred to earlier. Further, not having direct access to bank records is likely limiting LEAs' ability to trace assets associated with ML and predicate crimes.

242. Provisional measures, especially the number of freezing orders applied to high risk crimes were inconsistent with the country risk profile (drug trafficking – 27, fraud – 10, graft and corruption – 5, human trafficking – 4, kidnapping – 2 and e-commerce - 2). However, considering the limited validation duration (six months) of the freeze orders, AMLC files cases for civil forfeiture before the time limit expires. This may have negatively impacted the tracing of other connected properties related to organised criminality, including its transnational elements.

243. The assessment team noted the demand and need for targeted proceeds of crime confiscation training of all LEAs, prosecutors and judiciary. Furthermore, there is a need to have proper systems to gather statistics relating to confiscation of proceeds of crime, especially conviction based confiscations (art.45 of the Revised Penal Code).

Overall conclusion on Immediate Outcome 8

244. The NACS includes confiscation of criminal proceeds, instrumentalities and property of equivalent value as a policy objective, however this policy has not yet been effectively implemented. Prosecutors and LEAs do not seek and obtain confiscation of proceeds of crime at the point of conviction and there are only limited cases of confiscation of instruments of crime. The overall confiscation results (less than USD 15.75 million over six years) is very low and is not in keeping with the Philippines' risk profile. USD 117 million has been restrained in the same period, which is also very low. Filing of cases for civil forfeiture has increased since 2013, with focus on high risk crimes including confiscation of instrumentalities of crime and property of equivalent value. LEAs have limited their actions of seizures mostly to evidentiary purposes. Confiscations mostly relate to proceeds located in the Philippines, and those arising from predicate crimes that took place in the Philippines. Proceeds moved to other countries were pursued only in one instance. Confiscation of falsely/not declared or disclosed cross-border movements of currency and BNIs are at low levels. The confiscation activities in relation to drugs appear aligned with the country risk profile. In the context of high risks associated with TF, there has been no incidence of confiscation in relation to TF offences and only one TF civil forfeiture action was filed.

245. **The Philippines has a low level of effectiveness for Immediate Outcome 8.**

CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

*Key Findings and Recommended Actions***Key Findings**

10.9

- 1) The Philippines has an appropriate legal framework to prosecute TF offences under the Terrorism Financing Prevention and Suppression Act of 2012. LEAs and intelligence agencies demonstrate a good understanding of the risk and context of TF in the Philippines for domestic terrorism matters, but less well-developed understanding of trans-national TF risks. The main source of TF is believed to be self-funding through kidnap for ransom, extortion and drug trafficking and funding from foreign terror groups.
- 2) LEAs do not effectively identify TF arising out of counter-terrorism actions, investigations and financial intelligence in keeping with the risk profile, although there has been a slight increase in TF referrals made to the AMLC in the 2016-18 period. Competent authorities focus is on pursuing these predicate offences involved in TF and rely on the disruption of financing activity as an alternative measure.
- 3) TF investigations may follow an arrest or conviction on a predicate offence, however authorities have rarely allocated resources in part because of the limitations on consecutive sentencing.
- 4) In the six and a half years since the introduction of the standalone TF offence, the Philippines has not conducted any TF prosecutions, which is not consistent with the Philippines' risk profile.
- 5) AMLC's recent designation as the lead investigation agency for TF is a positive development. However FCIG staffing levels remain too low and additional appropriately skilled investigators for TF and financial investigations are required.
- 6) Although AMLC provided case studies that show it has exercised comprehensive investigative powers such as search, seize, taking witness statements and use of special investigative techniques when conducting TF investigations, it is not empowered to do so under legislation. AMLC cooperates with PNP and other LEAs to overcome these gaps in powers.
- 7) Competent authorities raised the evidentiary threshold as a reason for why no TF prosecutions have been undertaken, citing a lack of financial trails in the cash-based economy. However the use of MSBs in TF shows that there have been instances where terrorist financiers have interacted with regulated entities.
- 8) Sanctions applying to individuals who commit the TF offence (maximum imprisonment of 40 years and maximum fine of P1,000,000) are likely to be effective, proportionate and dissuasive. However due to a lack of TF convictions, it is impossible to assess the application or efficacy of sanctions in practice.
- 9) Prosecutors cannot be actively involved in assisting LEAs (including FCIG) during investigations to support successful TF evidence collection.

IO.10

- 1) The lack of UNSCR 1373 designations or proposals for UNSCR 1267 designation, and a low number of freezes of assets and instrumentalities, is not in line with the high risk of TF in the Philippines, including the known exposure to sanctioned entities. Factors affecting the use of domestic designations have included: the required evidentiary standard of 'probable cause' for proposing/making designations; procedural requirements of the HSA; and to a lesser extent, the inability to designate an individual as a terrorist under s.17.
- 2) In relation to TFS, funds owned or controlled by a sanctioned entity have only been identified and frozen in four instances in the last five years, and services denied on one occasion. One of these freezes was initiated by a FI following its TFS screening. Some FIs, including higher risk FIs, were unaware of the requirement to immediately freeze property or funds of persons or entities designated under the UN Sanctions regime. Instead, these FIs stated they may refund or release funds and file an STR.
- 3) The Philippines NPO sector is large and diverse, comprising both registered and unregistered NPOs. Some registered NPOs in the Philippines may have regulatory obligations with up to three regulatory bodies, including SEC, DSWD and PCNC. Unregistered NPOs are small community based operations which predominantly operate using cash.
- 4) The Philippines has recently completed an assessment of its NPO sector to identify the features and types of NPO likely to be at risk of TF abuse. However, there are still considerable knowledge gaps regarding the composition of the NPO sector. This includes the TF risks associated with unregistered NPOs, which were not examined in the assessment. Targeted risk-based supervision or monitoring of the types of NPO most at risk of TF abuse has not fully commenced.
- 5) Following the assessment of the NPO sector, all 101,843 registered NPOs are required to submit a mandatory disclosure to SEC so that their risk rating can be determined. All 101,843 NPOs are also required to establish a system to know where their funds are coming from, who their beneficiaries are and to ensure funds are used for the purpose intended. There are additional requirements imposed on those NPOs that are determined of medium or high risk.

IO.11

- 1) The Philippines does not have a framework for the implementation of targeted TFS related to proliferation financing (PF) without delay.
- 2) The Philippines has diplomatic and business relationships with DPRK and Iran, and in recent years has taken some steps to monitor business activity related to WMD through the issuance of circulars. Despite these actions there is limited awareness of TFS related to PF.
- 3) Some larger FIs and integrated casinos conduct screening of customers against third-party databases which include the relevant UN sanction lists. Covered persons lack knowledge of TFS related to PF.
- 4) Competent authorities do not currently have adequate skills or resources to implement TFS on PF.

Recommendations**IO.9**

- a) Amend legislation to empower AMLC to exercise comprehensive investigative powers such as search, seize, taking witness statements and use of special investigative techniques when conducting TF investigations.
- b) Enhance the identification, investigation and prosecution, of TF in keeping with the risk profile (domestic and transnational TF risks). This should include using the findings of updated TF risk assessments to target stand-alone TF and financing terror networks as well as TF arising out of counter terrorism actions and investigations.
- c) Increase the numbers of dedicated TF investigators and enhance TF investigation and prosecution capacity amongst competent authorities on TF investigations, including regular specific financial investigation training to enhance the identification of TF and supporting evidence.
- d) Increase FCIG staffing to add appropriately skilled investigators for TF and financial investigations. Ensure dedicated staff, with specialised knowledge on financial crimes, within LEAs with financial investigation units.
- e) LEAs should regularly request AMLC to pursue parallel TF investigations with the LEAs' terrorism investigations or predicate investigations that may have TF elements (e.g. kidnap for ransom matters).
- f) The Philippines should consider allowing early coordination between LEAs and prosecutors on the TF offence to improve evidence collection and other investigation actions.
- g) AMLC should conduct ongoing outreach and guidance to regulated entities on terrorism and TF red flag indicators, and the obligation to file STRs related to TF.

IO.10

- a) Amend the legal framework, including: to be able to take *ex parte* action against persons or entities proposed for designation pursuant to UNSCR 1373; to introduce the preliminary asset preservation orders; to allow individuals to be designated as terrorists under s.17 of the HSA; to allow for an evidentiary standard of 'reasonable grounds/basis' for proposing designations under UNSCR 1267 and deciding whether or not to make a designation under UNSCR 1373.
- b) Once the legal framework is fixed, enhance the use of the designation framework to more effectively deny funds to domestic terror groups operating in the Philippines.
- c) Continue to improve understanding and implementation of TFS requirements to ensure all covered persons are aware of obligations to identify and freeze terrorist assets without delay.
- d) Authorities should continue outreach and targeted information sharing to assist FI/DNFBPs to screen for TFS. This should include identifying persons acting on behalf of designated persons or entities, noting the prevalence of affiliates of TF organisations in the Philippines.
- e) Enhance risk-based supervision of TFS by FI/DNFBPs.

- f) Complete the initial risk rating of registered NPOs introduced under the SEC 2018 NPO Guidelines. Review whether the requirements imposed across the entire registered NPO sector are necessary. Increase targeted risk-based supervision and monitoring of the NPO sector, including enhanced outreach to those NPOs most at risk of TF.
- g) Examine whether increased coordination among SEC, DSWD and PCNC (and reducing the repetition of requirements for those registered NPOs with regulatory obligations to each) would improve the Philippines' overall supervision or monitoring and understanding of its NPOs at risk to TF abuse.
- h) Undertake further analysis in relation to the unregistered NPO sector to determine the level of associated TF risk.

10.11

- a) Implement a legal framework to implement TFS on PF without delay and develop regulatory and operational mechanisms for implementing, monitoring compliance and applying sanctions for breaches.
- b) The skills and resources of relevant competent authorities should be strengthened to implement TFS related to PF.
- c) Conduct awareness raising and capacity building activities for government agencies, covered persons and the general public to inform them of their obligations relating to TFS against PF.
- d) Commence supervision of TFS relating to PF, including identifying the vulnerable sectors for PF and understanding the risk of UN sanctions evasion.

246. 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.5-8.

Immediate Outcome 9 (TF investigation and prosecution)

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

247. Terrorism financing has been an offence in the Philippines since 2012. The Philippines is exposed to significant TF risk, due to mature support networks that sustain terrorist groups through the funding of material support and ongoing recruitment of followers within the Philippines as well as internationally. The southern parts of the Philippines is a recognised destination and transit point for foreign fighters linked to ISIL.⁶⁸

248. Competent authorities recognise that TF is occurring within the Philippines, but identify difficulties with investigations. LEAs prefer to disrupt the activity by removing those responsible from the community through other charges with similar terms of imprisonment (discussed further below).

⁶⁸See para 39-40, 'Seventh report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat', S/2018/770 (16 August 2018), accessible at <https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2018_770.pdf> (last accessed 14 May 2019)

249. In the six and a half years since the TF law was enacted, there has been no prosecution of TF activity and therefore no convictions for the TF offence. This is against a high risk of TF and despite authorities asserting that they investigate a possible TF aspect in every terrorism investigation carried out. Since October 2018, AMLC has filed two cases with the DOJ but, at the time of the on-site, these had not been accepted for prosecution.

4

250. The DOJ is the authority tasked with terrorism and TF prosecutions through the National Prosecution Service (NPS). The NPS currently has around 2,100 prosecutors, although there are approximately 3,100 positions that handle prosecutions across various crime types. This capacity is not dedicated to TF or even terrorist related cases. When asked about the lack of TF prosecutions, although the DOJ noted that an increase in resources, including prosecutors, would help, it noted that it is dependent on evidence brought forward by LEAs for prosecutions. Therefore, if LEAs do not bring forward evidence supporting TF, the DOJ is unable to establish a strong enough prima facie case to consider prosecution of TF. The DOJ does not play a role in investigations.

251. LEAs highlighted challenges contributing to the lack of TF prosecutions related to meeting the evidentiary threshold for trial. There are, however, no specific legal requirements on TF cases as compared to all other crimes. LEAs other than AMLC focus on the predicate crimes which are viewed by competent authorities as easier to prove and prosecute, the prosecution of which can have the effect of disrupting TF activity.

252. The DOJ noted that under the human trafficking law, early coordination between LEAs and the prosecutors is allowed, meaning that prosecutors can provide legal knowledge to assist the LEAs on evidence needed. This is not in place for TF. Similar early coordination on TF may help to improve the quality of investigations, briefs of evidence and ultimately the number of cases that can be accepted for prosecution.

TF identification and investigation

253. Regional environmental scanning⁶⁹, undertaken by the South East Asian CTF Working Group, confirmed that ISIL is conducting financing activities in South-East Asia. The Philippines authorities identified self-funding as the main source of TF in the country, with funds raised through kidnap for ransom, extortion and drug trafficking as outlined in the 2017 NRA. The 2016 Regional Risk Assessment on Terrorism Financing, led by Australia and Indonesia, confirms that the risk of TF through criminal activity is high and the main TF income stream in the Philippines.

254. The role of the terrorist financier, and the possible offence of TF, is reported by LEAs to be considered as part of every terrorism investigation undertaken in the Philippines. From 2014 to June 2017 there were 18 specific cases of TF investigated by the FCIG. No other LEAs reported investigating a possible TF offence, despite the very significant levels of terrorism offending. It is not evident that possible TF offences are, in practice, considered as part of every terrorism investigation.

⁶⁹ The regional study conducted by the SEACTFWG, led by member-countries produced four separate reports: (a) ISIL's Financing in SEA: The Regional Environment – Australia; (b) External Funding to ISIL SEA – Indonesia; (c) Hawala Dealers Financing of ISIL and Other High Threat Terrorist Organisations in SEA – Malaysia; and (d) Self-Funding of ISIL SEA - Philippines. All members of the SEACTFWG contributed to these studies

Case Example 4.1- JMJ

In 2016, crew members of a tugboat from country A were kidnapped off the coast of the Philippines and a ransom demand made. Ransom money was to be deposited in a bank located in the Philippines.

An investigation was triggered by a request from the AFP to AMLC for a financial investigation into the bank account allegedly being used by kidnapers for the deposit of ransom money. This request was followed by further requests by the PNP Anti-Kidnapping Group, the PNP Criminal Investigation Group, and NICA, as well as a request for assistance from a neighbouring FIU.

The FCIG investigation revealed significant remittances from country A were deposited into the Philippines bank account and several withdrawals made. AMLC directed the bank to closely monitor the account and defer freezing action in order to identify the ultimate recipient of the funds. Once the recipient was identified, AMLC issued a resolution to freeze the account.

On 13 May 2016, the bank account was frozen due to TF links and suspicion it is linked to, or controlled by, a UN designated terrorist organisation. A total of PHP 498,653.68 (approx. USD 9,500) remaining in the account is now subject to a civil forfeiture case. Further, a TF case against JMJ, one of the individuals who owned the account and made withdrawals following the remittance from country A, was filed with the DOJ in October 2018 and is pending a decision regarding prosecution.

255. LEAs responsible for terrorism investigations were not able to demonstrate that TF is pursued systematically in parallel with terrorism investigations. It is not clear that those LEAs regularly develop TF related intelligence to ensure that TF activity is systematically identified and investigated. However, it is observed that in the 2016-18 period there was a slight increase in TF referrals to the AMLC, with some referrals including seized financial documents.

256. The 2017 NRA notes that intelligence and military agencies focus only on the terrorism-related aspects of a case, overlooking the role of the financier. There is an acknowledgment that this results in limited evidence of TF. In meetings with the assessment team some agencies disagreed with this finding in the NRA. Although approximately 10% of the PNP are qualified to undertake financial investigations, the PNP specifically focuses its financial investigations on dangerous drugs.

257. Cooperation occurs between AMLC, security intelligence and defence agencies to enhance information exchange and to seek enhanced collection of intelligence and evidence related to TF. Real time information on terrorism and TF suspects has been shared between the Armed Forces of the Philippines and AMLC during critical events to support TF-related intelligence development. NICA indicated that it treats TF as equally important to terrorism. The Intelligence Service of the Armed Forces of the Philippines has cooperated with AMLC in workshops with the armed forces on identifying and collecting financial information/evidence while in the field (giving financial documents similar standing to cash, drugs, firearms etc.). A small number of AMLC staff have directly travelled to conflict zones to assist with confiscation of cash seized during the Marawi siege. Further actions are being pursued to support enhanced operational cooperation and CFT capacity building amongst defence agencies operating in conflict zones.

258. AMLC (FCIG) has primary responsibility for conducting TF investigations. TF is jointly coordinated with terrorism through the JTFIG, of which most LEAs are members. During the weekly JTFIG meetings, information gathered by investigators or through exchanges with other jurisdictions, is referred to AMLC. This coordination has resulted in a small number of TF investigation outcomes, being the freezing of bank accounts related to a UN designated terrorist organisation and the filing of a

TF case against the identified financier (pending at the time of the on-site), and the validation of information on FTF who travelled to the Philippines.

4 259. LEAs indicated that they often investigate possible TF after an individual/s have been arrested on, or even convicted of, other offences. The primary focus is to disrupt the activities, which can be achieved through arrest for predicate crimes. However, if an individual is convicted of a predicate offence and sentenced to extended imprisonment, the authorities are unlikely to pursue a further TF investigation and prosecution. In the Philippines, an individual can only serve consecutive terms of imprisonment up to a total of 40 years. If an individual is convicted of kidnapping for ransom, for example, and is subject to the maximum penalty of 40 years, the DOJ sees no benefit to the filing of a further case for TF. The reasoning is that the financier has already been removed from the community for the longest possible term of imprisonment and the financial flow has been disrupted. Given this is the position of the prosecuting body, LEAs therefore have no incentive to allocate resources to a TF investigation following a predicate conviction or likely conviction.

260. There are very low numbers of STRs regarding both terrorism and TF, with the exception of a spike in reports filed in 2017. This is despite increasing terror and threat incidents within the Philippines. Terrorism and TF related STRs account for only 0.06% of STRs filed during the period 2014-2016. This low level of STR filing is recognised in the NRA. The agencies were of the view that the cash based economy of the Philippines and preference for cash by terrorist groups, meant covered persons were not frequently exposed to terrorism related activity and thus weren't filing STRs. The issue of the cash-based economy was identified as a road-block to identifying the financial transaction. While this would make the investigation of some TF cases more challenging, this issue is not unique to the Philippines. Further, the known use of MSBs in relation to TF highlights that there are instances where terrorists have interacted with regulated entities even in their use of cash. While some regulated entities (MSBs) have had their registrations cancelled in response to these interactions, TF charges have not followed. However, the assessment team was alerted to an ongoing investigation involving owners of an MSB involved in the 2017 Marawi siege.

261. There is a legislative provision that, while not an impediment, was observed to potentially discourage the pursuit of terrorism and TF cases. S.50 of the Human Security Act of 2007 requires a payment of PHP500,000 (approx. USD 9,500) per day of detainment be made by the government to a person charged with, but ultimately acquitted of, terrorism. Although this payment does not extend to acquittals from TF charges, this is likely to have an impact on the level of TF related investigative activity, which largely occurs in conjunction with terrorism investigations.⁷⁰

262. The Philippines is not identifying or investigating TF activity in line with its identified risks.

TF investigation integrated with -and supportive of national strategies

263. Until mid-2018 there was no clear policy priority given to TF investigation and prosecution.

264. National level coordination meetings are held regularly between competent authorities, considering terrorism and TF issues jointly. These coordinating mechanisms include the JTFIG, the AML/CFT Sub-Committee of the NALECC and the ATC. As outlined above, this coordination has only led to a small number of TF outcomes.

265. As noted in IO.1, in 2018 the Philippines released the NACS to provide a whole of government response to address risks identified in the NRA. Strategic Objective 5 aims to 'develop and strengthen

⁷⁰ House Bill 7141 proposes to remove this provision from the Human Security Act of 2007

mechanisms to prevent, disrupt and combat terrorism, terrorism financing and proliferation financing.’ The action plan related to this strategic objective encompasses the inclusion of TF in the focus of the NIC; capacity building on terrorism and TF tactics and trends using cybersecurity; and interagency collaboration for monitoring and prevention of travel of local and FTF. NICA has been designated as lead of the Terrorism Financing and Proliferation Financing Sub-Committee for the implementation of this action plan. Other members of the sub-committee include AMLC, ATC, NSC, NBI and PNP. Given the recent adoption of the NAC, it is yet to be seen how the strategic objectives and supporting action plans are implemented by the NACC.

Effectiveness, proportionality and dissuasiveness of sanctions

266. Under the TFPSA, both imprisonment and fines are available sanctions for TF activity. The maximum term of imprisonment for TF is 40 years, with a minimum of 12 years and one day. A maximum fine of PHP1,000,000 (USD 19,000) can also be imposed. These sanctions are dissuasive for the natural person when compared with those applicable for predicate crimes and are likely to be dissuasive. As there have been no convictions for the offence of TF, it is not possible to assess the efficacy of sanctions in practice. There has been no application of the sanctions available for TF.

267. The same sanctions are available to any natural person who deals with the property or funds of a designated person, including by providing financial services.

268. Where the activity under the TFPSA is undertaken by a legal person, the only additional sanction available to the authorities is suspension or revocation of their licence. There are no financial penalties specific to the legal person under the TF Law, rather the sanctions (imprisonment and/or fines) are to be imposed on the responsible officers (natural persons). Given the involvement of MVTS services in TF in the Philippines, the lack of available punitive sanctions is concerning. Under Philippines’ case law (*Alfredo Ching vs Secretary of Justice*, G.R. No. 164317, 6 February 2006) a legal person can be charged and prosecuted for a crime if the imposable penalty is a fine. However the financial penalties available under the TF Law are not proportionate or dissuasive when considered in the context of a legal person.

269. In reflecting on proportionality, as noted above, the relatively high sanctions associated with predicate offences, as compared to TF, is a key factor in the negligible prosecutorial activity in the Philippines. It is unlikely that a prison term greater than 40 years will contribute any great efficacy or dissuasiveness.

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

270. In the absence of any TF prosecutions and convictions, the Philippines raised its prosecution of predicate offences and freezing orders to disrupt financing activities. The Philippines’ position is that it will charge a person based on the best available evidence to secure a conviction, ensuring the individual is removed from the community and their activities are disrupted. However, the Philippines did not provide any justifiable reason why achieving a TF conviction is not practicable, i.e. there is no legal impediment in the legal framework. It seems that the challenge for LEAs is identifying and gathering evidence to support a TF charge and conviction.

271. In relation to TF, the Philippines pursues assets through the freezing of funds and assets of terrorists (discussed in IO. 10 below). This has occurred, however, in only limited circumstances. In 2015-2017 approximately USD 117,000 was seized and frozen by the Philippines and PHP 52 Million

(USD 996,235) seized by the military in June 2017 from an abandoned house linked to the Maute Group. The June 2017 seizures also included vehicles and a 120 hectare parcel of land.

272. These measures however are not taken as alternatives to TF convictions due to any justifiable obstacles in prosecuting TF.

Overall conclusion on Immediate Outcome 9

4

273. AMLC's recent designation as the lead agency for TF investigations and the conduct of some TF-related financial investigations is a welcome development. LEAs responsible for terrorism cases do not effectively investigate TF, despite a clear legal basis to do so. Considerable weight must be placed on the Philippines lack of TF prosecutions and convictions, which is not consistent with its risk. Sanctions available for legal persons are not proportionate or dissuasive, which is a concern given the involvement of MVTs in TF activity the country. Efforts have been made by the Philippines to integrate CFT with its national efforts to counter terrorism. Government agencies understand the TF risk, however largely limit their focus to the predicate crime (i.e. kidnap for ransom) or terrorism.

274. **The Philippines has a low level of effectiveness for Immediate Outcome 9.**

*Immediate Outcome 10 (TF preventive measures and financial sanctions)**Implementation of targeted financial sanctions for TF without delay*

275. The 2017 NRA assessed the risk for TF as high in the Philippines. Specifically, the southern province of Mindanao, under martial law at the time of the on-site visit, is a conflict zone where terrorism and TF issues are significant. Various terrorist groups such as Abu Sayyaf, which are Al Qaeda and ISIL affiliates, are operating. Foreign fighters from various countries are also known to have travelled to the southern Philippines. In addition, there are approximately 15 Filipinos currently designated as terrorists under UNSCR 1267, all of whom are associated with terrorist groups.

Legal and regulatory framework

276. The Philippines' legal and regulatory framework for implementing TFS is established by the TF Law and its IRR and the Human Security Act 2007 (HSA) (see R.6).

UNSCR 1267

277. The Philippines has not proposed any designations to the 1267/1989 Committee since the 2008 proposal of the Rajah Solaiman Movement. Targets for designation are identified by NICA through a technical working group comprising agencies within the intelligence community. Proposals for designation are made by NICA. The threshold for proposing a designation is a criminal evidentiary standard, i.e. a court case must have commenced. This requires an evidentiary standard of 'probable cause' rather than 'reasonable grounds' or 'reasonable basis'. This high threshold has blocked further potential proposals for designation, although NICA advised that some proposals are in the pipeline.

278. The freezing mechanism for implementing UNSCR 1267 obligations is set out in the TF law. A standing freeze order is provided by AMLC Resolutions TF-01 and TF-02 of 2012. These direct all covered persons and relevant government agencies to freeze without delay the property or funds, including related accounts, of UNSCR 1267 designated persons or entities. A broad prohibition on dealing with property or funds of designated persons is set out in s.8 of the TF law, which is a de facto freeze applying to all natural and legal persons. Updates and changes to the list of UNSCR 1267 designations must be immediately transmitted from DFA to AMLC. In practice, AMLC receives updated lists directly from the UN and updates its website and its portal for covered persons within one business day. This means that in some circumstances, such as over a weekend, the requirement to freeze may not take effect without delay.

UNSCR 1373

279. The legal framework for UNSCR 1373 designations is established by the HSA. Upon application of the Department of Justice before a Regional Trial Court, an organisation, association or group of persons may be proscribed as a terrorist entity pursuant to s.17 of the HSA. The HSA does not allow the Philippines to operate ex parte against an entity that has been identified and proposed for UNSCR 1373 designation. Instead, due notice must be given and the entity have the opportunity to be heard. Similar to UNSCR 1267 proposals, the threshold for proscription is a criminal evidentiary standard of 'probable cause' rather than 'reasonable grounds' or 'reasonable basis'.

280. The Philippines has designated one terrorist entity, the Abu Sayyaf Group, pursuant to UNSCR 1373, in 2015. This entity is also a UNSCR 1267 designee. However, as the principal terrorist group in the country, the Philippines chose to also list it domestically. Having UNSCR 1373 designation allows technical and financial surveillance to be conducted and assists with the freezing of assets. This

included the action taken in relation to the Maute Group (see Table below), who were associated with Abu Sayyaf.

281. In addition to Abu Sayyaf, NICA advised that there are other potential proposals of terrorist entities in the pipeline for designation under UNSCR 1373. Notably, one proposal for designation has been pending since February 2018; however this cannot currently be progressed because the group cannot be served notice. The assessment team considers an inability to progress designation because notice cannot be served to be a significant deficiency. This impacts on the Philippines' effective use of UNSCR 1373 designation.

282. There is no mechanism in s.17 of the HSA for an individual person to be proscribed as a terrorist. An individual (or an entity) may only be designated a terrorist under the TF Law if their property or funds are subject to seizure or sequestration under s.39 of the HSA. This has not occurred. The Philippines advised that a terrorist in the Philippines is very unlikely to be acting as an individual on their own, and that there have been no reported instances of an individual not associated with a terrorist group perpetrating a terrorist act.

283. The Philippines has received requests from foreign jurisdictions for UNSCR 1373 designations; however these have not eventuated into designations. As with domestically identified targets for UNSCR 1373 designation, requests from foreign jurisdictions require an application to a Regional Trial Court, due notice must be given and the entity must have the opportunity to be heard. Again, s.17 of the HSA only enables an organisation, association or group of persons to be declared as a terrorist entity upon request for a foreign jurisdiction. It is only possible for a designated individual in another jurisdiction to be designated as a terrorist in the Philippines if their property or funds are subject to seizure and sequestration under s.39 of the HSA. This has not occurred.

284. The assessment team's view is that the current procedural requirements of the HSA, and to a lesser extent its inability to designate an individual as a terrorist, have significantly impacted its use. The assessment team notes that there is currently a Bill before Congress to amend the HSA. This amendment enables an individual to be designated as a terrorist. The Bill also amends the requirement that the entity (or an individual) be given due notice and opportunity to be heard. This would enable the Philippines to operate *ex parte* against a person or entity proposed for UNSCR 1373 designation. Further, the Bill introduces timeframes for proscription. It states that where 'probable cause' is established, a preliminary order of proscription must be made within 24 hours of application, with a further substantive hearing within six months.

Implementation of TFS screening

285. In relation to the obligation to implement TFS without delay, the rules and guidelines of BSP, SEC, IC and for DNFBPs include requirements to identify designated persons or entities at customer onboarding and as part of ongoing monitoring. However, as identified above, in some circumstances for a new UNSCR 1267 designation, the requirement to freeze may not take effect without delay.

286. Universal banks, commercial banks and some larger MSBs, are conducting automated TFS screening against relevant UN Sanctions lists. The BSP has identified deficiencies in the screening systems being applied by some banks, although overall BSP assess TFS screening in banks to be functional. A recent survey of universal and commercial banks conducted by BSP identified that from 2014 to 2018, there were 170,000 'alerts' generated from their TFS screening (which includes US OFAC, Bank of England and other sanctions lists, in addition to UNSCR listings). Upon examination of these alerts, there were no matches to persons on UNSCR listings, but 823 positive matches to other sanctions lists (for which STRs were submitted). From examination of the 823 positive matches, links to UNSCR

1267 sanctioned entities were made in four cases, from which funds were available for freezing in one case (see Table below).

287. Screening by other types of FI, including thrift and rural banks, is mixed and often involves manual systems and open source checks. Most DNFBPs are yet to implement the requirements, although integrated resort casinos are in the process of implementing automated screening solutions.

Understanding of freeze requirements

288. Some FIs, including higher risk FIs, appear unaware of the requirement to immediately freeze property or funds of persons or entities designated under the UN Sanctions regime. These FIs stated they had no legal power to freeze funds and were unclear that the standing freeze order provided by AMLC Resolutions TF-01 and TF-02 of 2012 authorised them to do so. Instead, these FIs stated they may refund or release funds and file a STR. FIs appear aware of procedures to be followed in case AMLC issues a preventative freeze order for specific funds or property.

Freezes of funds, assets and instrumentalities

Table 4.1: Freezes of funds, assets and instrumentalities or services denied

Year	Details	Frozen funds or services denied
2014	Freeze orders relating to bank account identified in a false name linked to person associated to TF.	Bank account (PHP150,980 / USD2,870)
2015	Bank denied services to a UNSCR 1267 listed person for possible violation of US OFAC sanctions.	Purchase of cheque denied
2016	Freeze orders issued by AMLC on bank account following kidnap for ransom of tug boat crew (see IO.9 case study above)	Bank account (PHP498,653 / USD9,484)
2017	Freeze orders issued against property and funds of members of the Maute Group following the Marawi Siege	Land (120 hectares); Vehicles; Cash (PHP52 million / USD996,235); Bank accounts (59 totalling PHP28,500 / USD547)
2017	Bank account identified and frozen, and STR submitted, of a person because of his membership/affiliation to Abu Sayyaf (designated entity under UNSCR 1267). The person was subsequently designated under UNSCR 1267.	Bank account (PHP217,165 / USD4,182)
2018	Triggered by US OFAC list scrubbing, another bank identified an account and filed an STR for the same person (referred to in the 2017 case above). The STR was filed prior to his UNSCR 1267 designation. Account had no transactions since 2011 and a remaining balance of less than PHP200.	Nil
2018	Bank identified a closed account of a person known for affiliation with Abu Sayyaf. Account was closed in 2015 and had been inactive since 2011. STR was lodged nine days after US OFAC listing, and prior to the person's designation under UNSCR 1267.	Nil

289. In 2015 a bank denied a service to an individual due to possible violation of US OFAC sanctions. The person was listed on the UNSCR 1267 list.

290. In 2017 funds in a bank account of a person that was a member/associate of the Abu Sayyaf Group (a designated entity under UNSCR 1267) were identified following the bank's TFS screening.

While the funds were frozen when the account was identified, no return was filed informing AMLC that funds had been frozen under Resolutions TF-01 and TF-02 of 2012. Instead, the bank submitted an STR. This further indicates that not all banks fully understand their TFS obligations. In 2018, another bank identified an account for the same person and also submitted an STR. The account had been inactive since 2011 and had a balance of less than PHP200.

4

291. In 2018 a bank identified it was holding a closed account of an individual affiliated with Abu Sayyaf. This account was closed in 2015 and been inactive since 2011.

292. In the last five years, there have been three other instances of funds, assets and instrumentalities of sanctioned entities being frozen. These freezes were initiated by AMLC after funds, assets or instrumentalities were found to be owned or controlled by parties associated with Abu Sayyaf, including the Maute Group. No other funds have been identified for freezing. The Philippines advised that this is because of the prevalence of cash, specifically cash from criminal activity, being the preferred method of TF. Notwithstanding this, the assessment team notes that the TF Regional Risk Assessment 2016 identifies a medium risk of both the banking system and MSBs being used for TF in the Philippines.

293. Overall, there have been limited instances where funds or assets have been frozen, or services denied pursuant to UNSCR 1267 or 1373. Of these, only two have stemmed from identification by FIs. The assessment team considers this to be highly unusual considering the risk profile and population of the Philippines. This brings into question the implementation of TFS given the common occurrence of names on the UNSCR 1267 list and recent BSP survey which identified there to have been 170,000 alerts and 823 positive matches to other sanctions lists. The assessment team considers the low number of freezes in the Philippines not in line with its TF risk profile, given the known presence and operation of sanctioned entities.

294. There is no legislated mechanism for de-listing of UNSCR 1373 designations or unfreezing funds or assets. The Philippines advised that there has been no challenge to proscription or the freeze of funds or assets, but if there were, this could occur through the courts. There are provisions for humanitarian access to funds for basic expenses, but no requests have been received.

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

295. The Philippine NPO sector is large and diverse. It comprises of both NPOs registered with SEC and unregistered organisations that can be characterised as NPOs (unregistered NPOs).

296. The Philippines defines a NPO as “an SEC-registered Non-Stock Corporation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for carrying out of other types of good works”. These activities align with the activities in the FATF definition of NPO.

297. While registration with SEC is not required to operate, it is required to obtain a legal personality as a NPO, open a bank account, enter into contracts and to raise funds. There are complementary provisions under the Solicitation Permit Law, as well as other local government ordinances, that also restrict fund raising activities without prior registration as a NPO. Consequently, unregistered NPOs in the Philippines are small informal community operations, predominantly operating using cash. There is no accurate picture of how many unregistered NPOs are operating in the Philippines.⁷¹

⁷¹ Page 10, the Philippines’ assessment of the NPO sector, October 2018.

298. As at 31 December 2017, there were 101,843 NPOs that were registered with SEC (see Chapter 1). Of these, 19,511 (19.2%) were classified as religious organisations and 13,139 (12.9%) were classified as Education NPOs. Both are service type NPOs (as opposed to expressive type NPOs).⁷²

299. A further 11,734 (11.5%) of the 101,843 registered NPOs in the Philippines (as at 31 December 2017) were classified as 'Foundations'. Of the registered Foundations, 92% are service type NPOs, comprising 42% engaged in charitable and 30% in social development activities. A 'Foundation' is defined as 'a non-stock, non-profit corporation established for the purpose of extending grants or endowments to support its goals or raising funds to accomplish charitable, religious, educational, athletic, cultural, literary, scientific, social welfare or other similar objectives'. Only registered Foundations may use the word 'Foundation' in their corporate name and when describing their NPO activities. An NPO is only able to register as a Foundation if it has initial capital of at least PHP1million (USD19,250). Since 2006, Foundations have had stricter registration requirements with SEC when compared to other types of registered NPO. This included a requirement to submit a sworn statement relating to the NPO's source and amount of funds, programs and activities planned, both ongoing and accomplished, and the application of funds. However, these requirements were not strictly enforced and were relaxed in 2016 to make operating a Foundation easier.

300. A further 52,917 (52%) of the 101,843 registered NPOs in the Philippines (as at 31 December 2017) had no clear classification at all. There was no clear data available on what type of activities they undertook, whether they were still operating and whether they were expressive or service type NPOs. While action is now being taken to address this (see below), this suggests knowledge gaps as at the date of the on-site visit in the Philippines' understanding of the composition of its registered NPO sector.

301. In addition to SEC requirements, regulatory functions in the NPO sector are also undertaken by other regulatory bodies, including the Department of Social Welfare and Development (DSWD) and the Philippine Council for NGO Certification (PCNC). For a NPO to be able to provide social welfare and development programs funded by the government, or from fund drives or endowments, there are specific registration, licensing and/or accreditation requirements with DSWD. As at 31 December 2017, there were 2,252 NPOs registered or licensed with DSWD, all of which were service type NPOs. PCNC is a self-regulatory body designated to prescribe rules and standards and certify NPOs as charitable "donee" institution status, which has tax incentives. There are less than 500 NPOs that are certified by PCNC. Of these, the overwhelming majority are also service type NPOs.

302. The three bodies of SEC, DSWD and PCNC each fulfil separate functions and have regulatory requirements determined according to their own mandates. All serve to promote accountability, integrity, and public confidence in the administration and management of the registered NPO sector.

303. During 2018, the Philippines completed an assessment of its NPO sector to identify the features and types of NPO likely to be at risk of TF abuse. This primarily considered those NPOs that are registered with SEC rather than unregistered NPOs.⁷³ The assessment of the NPO sector identified that there have been thirty-two NPOs of which there has been possible involvement in terrorism or TF, though their actual involvement is not substantiated by LEAs. Of the thirty-two NPOs, five (16%) were registered NPOs that were not clearly classified by SEC. A further thirteen (41%) were unregistered NPOs. This is noted as a possible source of vulnerability for the NPO sector but no further analysis of

⁷² Service type NPOs are predominantly involved in service activities, which include programmes focused on housing, social services, humanitarian aid, education, health care, religious education and affiliated social services. Expressive type NPOs are predominantly involved in expressive activities, which include programmes focused on sports and recreation, arts and culture, interest representation, and advocacy.

⁷³ Page 10, the Philippines' assessment of its NPO sector, October 2018.

unregistered NPOs has been conducted.⁷⁴ The assessment team considers the lack of analysis of unregistered NPOs in the Philippines' assessment of its NPO sector to be a deficiency.

304. In summary, the Philippines' assessment of its NPO sector identified the nature of the threats posed to higher risk registered NPOs as (a) the diversion of funds to support terrorist entities and (b) affiliations, whether knowingly or unwittingly resulting, in logistical support to terrorist/threat groups. Overall, the Philippines assessed the risk rating of its registered NPO sector to TF abuse as low-medium. As identified in the 2017 NRA (and discussed in IO.1 above), criminal activity, including kidnap for ransom and extortion by terrorist groups, are considered the preferred methods for TF (rather than using NPOs).

305. Of the registered NPOs, the types most at risk of TF abuse are assessed to be service type NPOs that provide charitable, social development, humanitarian disaster relief or educational activities. This includes any Foundations that engage in these activities (although Foundations are not otherwise identified specifically as a higher risk type of NPO). Notably, the registered NPOs that have obligations to DSWD include service type NPOs providing social welfare and development programs, which is a type of NPO at higher risk of TF abuse. Similarly, over 90% of NPOs that are certified by and have regulatory obligations to PCNC are also service type NPOs (see R.8).

306. AMLC has regular meetings with SEC, DSWD and PCNC and other stakeholders such as CODE-NGO, a coalition that represents 1,435 NPOs. AMLC has also conducted outreach and provided briefings to NPOs on the self-regulatory initiatives that can be implemented to prevent ML/TF. Much of this has been directed at service type NPOs that are assessed as the type of NPO at higher risk of TF abuse. This included Area Based Network (ABSNET) meetings in April and June 2018, which were organised by DSWD and attended by representatives of the NPOs it regulates. AMLC also conducted a briefing at the PCNC Annual Assembly in June 2018. This was attended by 253 mostly service type NPOs, engaged in social welfare/development, education and humanitarian disaster relief. Most recently, AMLC conducted a briefing in October 2018 to 529 NPOs at an outreach event organised by SEC. Approximately 41% of attendees were involved in charitable, educational or social welfare activities. Some of the content of these briefings was specific to the risk of TF abuse.

307. In November 2018, SEC published new guidelines for the protection of registered NPOs from ML/TF. The intention is to promote accountability, integrity and public confidence in the administration and management of registered NPOs. All registered NPOs (not just Foundations) are now required to establish a system that will enable them to know where their funds are coming from, who their beneficiaries are and where they are located. All NPOs must also ensure funds reach their target beneficiaries or that they are used for the purpose intended. NPOs must also report to SEC any fact that gives rise to a suspicion that it is being exploited for ML/TF. While the 2018 NPO Guidelines do not direct what type of system must be adopted, the assessment team's view is that these requirements may involve considerable administrative resource across the NPO sector.

308. The SEC 2018 NPO Guidelines are also intended to close the current knowledge gaps regarding the composition of the registered NPO sector. The 2018 NPO Guidelines require that within six months, all 101,843 registered NPOs must submit mandatory disclosures regarding their purpose, activities, source of funds, beneficiaries and the geographical areas in which they operate. SEC stated that it intends to use this information for administrative purposes, as well as to rate the ML/TF risk associated with each NPO. Those of medium through to higher risk will be subject to increasing levels of

⁷⁴ Page 42, the Philippines' assessment of its NPO sector, October 2018.

monitoring and supervision, including additional disclosure, audit and background checking requirements.

309. Some risk-based supervision or monitoring of the types of NPOs most at risk of TF abuse has been undertaken prior to the assessment of the NPO sector. With the newly completed assessment of its NPO sector, the Philippines is now better placed to target its supervision and monitoring to those NPOs most 'at risk'. Once the Philippines has completed its wider ML/TF risk rating procedures across the NPO sector, it will then be able to determine whether there are additional 'at risk' NPOs which also require targeted supervision or monitoring.

310. As noted above, the SEC 2018 NPO Guidelines impose some requirements across all registered NPOs, rather than specifically targeting NPOs vulnerable to TF abuse.⁷⁵ This may discourage or disrupt legitimate NPO activities. The assessment team also notes that for those NPOs overseen by SEC, DSWD and PCNC, there is some repetition of regulatory requirements. Some NPOs reported this as burdensome.

Deprivation of TF assets and instrumentalities

311. The Philippines has taken limited action to ensure deprivation of assets and instrumentalities related to TF. In the last five years, there have been only four instances of funds, assets and instrumentalities related to TF activities being frozen and one instance of services being denied.

312. In one instance, funds of a person designated under UNSCR 1267 were frozen by a bank following its TFS screening. In the three other instances, the freezes occurred where funds, assets and instrumentalities were found to be owned or controlled by parties associated with the Abu Sayyaf Group. One of these instances (refer Table 26 above) related to the Maute Group following the Marawi Siege. Freeze orders were issued by AMLC in relation to real property, cash and vehicles found in the course of raids and 59 bank accounts. The assessment team acknowledges that this is a large freeze of assets, instrumentalities and funds.

Consistency of measures with overall TF risk profile

313. The assessment team notes the NRA's observations that TF risk has increased between 2014 and 2016 from medium-high to high, with terrorist organisations now enjoying 'a systematic and established method of raising funds for their operations'.

314. The design and implementation of TFS show weaknesses. The results of the TFS framework are negligible when compared with the flow of funds to designated entities active in the Philippines.

315. The assessment team considers that the current procedural requirements of the HSA, and, to a lesser extent, its inability to designate an individual as a terrorist under s.17, have significantly impacted its use. The lack of designations under UNSCR 1373 and proposals for designation under UNSCR 1267, and only four freezes of funds, assets or instrumentalities are not in line with the high risk of TF in the Philippines.

316. In the NPO sector, there have been some valuable initiatives to mitigate TF risks. The Philippines has recently completed an assessment to identify the features and types of NPO likely to be at risk of TF abuse. This provides the Philippines with a basis to increasingly target outreach to its 'at

⁷⁵ Subsequently to the on-site visit, the Philippines advised that the requirements imposed by the 2018 NPO Guidelines are to be reviewed following feedback from the NPO sector.

risk' NPOs. However, as at the date of the on-site visit, there are still considerable knowledge gaps regarding the composition of the NPO sector (see above) which impact on the Philippines' ability to address TF risk in the NPO sector.

Overall conclusion on Immediate Outcome 10

4

317. There are major gaps with the legal framework and procedural requirements of the TFS framework for UNSCR 1373, which have impacted its use. Implementation of TFS is not strong amongst FIs and weak amongst DNFBPs. Considering the high risk of TF in the Philippines, this is a significant shortcoming. The Philippines has recently completed an assessment of its NPO sector to identify the features and types of NPO likely to be at risk of TF abuse. Some outreach to these types of NPO has also been undertaken. However, current knowledge gaps remain regarding the composition of the NPO sector. Targeted risk-based supervision and monitoring of those NPOs most at risk of TF abuse has not fully commenced.

318. **The Philippines has a low level of effectiveness on Immediate Outcome 10.**

Immediate Outcome 11 (PF financial sanctions)*Implementation of targeted financial sanctions related to proliferation financing without delay*

319. The Philippines does not have a legal framework for implementing TFS related to WMD proliferation (PF). In November 2018 the 2018 IRR was amended to require covered persons to secure the consent of their customers to be bound by obligations set out in the relevant UNSRCs. Since November 2018 BSP requires its covered persons to adopt policies and procedures to implement WMD-related TFS without delay and to report to AMLC the actions taken in compliance with the prohibition requirements of the relevant UNSCRs (BSP Circular No. 706 (via circular 1022)). These new measures do not implement a legal framework, nor do they apply to all covered persons. The Strategic Trade Management Act (STMA) has provisions to regulate business related to WMD and the financing of such business, but it does not include measures relating to the implementation TFS on WMD proliferation.

320. Due to the lack of a domestic framework, TFS relating to WMD proliferation is not implemented without delay in the Philippines. The Philippines does not have a mechanism to systematically disseminate relevant UN list updates, nor does it have mechanisms or procedures relating to designation, listing, delisting, freezing/unfreezing or access to funds.

321. The Philippines has taken some measures to seek to monitor possible business with sanctioned entities. In relation to DPRK, in May 2017 BSP issued circular letter No. CL-2017-035 which noted BSPs support of UNSCR 2321 and ‘within the bounds of banking laws, rules and regulations’, advised BSP-supervised entities to monitor and exercise vigilance on any financial transactions with the individuals and entities referred to in UNSCR 2321. The UNSCR was attached to the circular letter. The circular also advised BSP-supervised entities to report any known information regarding the individuals referred to in UNSCR 2321 to AMLC and appropriate supervision department of the BSP. No circular was issued by BSP following the issuance of UNSCR 2356 in 2017. A similar circular was issued in August 2009 relating to UNSCR 1874 and 1718.

322. In relation to Iran, in September 2015 BSP issued circular letter CL-2015-058 which directed FIs to monitor developments related to UNSC 2231 and informing FIs about the FATF’s 26 June 2015 public statement. The circulate notes “for implementation and guidance”, however it is not clear what is required to be implemented. In November 2010 BSP issued circular CL-2010-084, informing FIs of UNSCR 1929 and advising banks and non-bank FIs to monitor and exercise vigilant on transactions with listed entities. It also advises FIs to report any known information on listed entities to the BSP.

323. While these circulars demonstrate that BSP has some awareness of the UNSCRs and obligations related to PF, they do not provide a basis for asset freezing and other requirements set out in R.7. Further, their distribution and applicability is limited to BSP supervised entities.

324. The Philippines has national coordination structures focused on combating WMD, but these do not extend to TFS on or other elements of PF. The August 2018 NACS includes consideration of PF and the action plan includes the development of a regulatory framework for TFS related to PF. NACS also includes the establishment of a sub-committee on TF and PF, however this is not yet operational. The Strategic Trade Management Office (STMO) has been identified as the lead agency for implementing TFS related to PF and it is currently receiving capacity building to strengthen its understanding ahead of the development of a legal framework for implementation.

325. The Philippines’ exposure to PF is notable due to its diplomatic and business relationships with DPRK and Iran. Authorities may not be fully aware of the level of exposure that the Philippines has

to vulnerabilities related to PF. In 2017 the Philippines exported USD1.2 million in goods to DPRK. Also in 2017 the Philippines exported goods valued at USD102.6 million to, and exported USD99.8 million from, Iran⁷⁶. In 2016 the Philippines government impounded a North Korean cargo ship which was subject to UN sanctions, which illustrates awareness of the UN sanctions obligations.

4 326. While there is no requirement in the FATF standards to assess risks related to PF, authorities should enhance their understanding of the vulnerable sectors for PF and the risk of UN sanctions evasion in order to effectively implement an appropriate framework.

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

327. There is no legal requirement to identify assets or funds held by designated persons or entities. Authorities are not aware of any assets or funds held by designated persons or entities within the Philippines. The banking and MBS sectors appear to refuse customers from both DPRK and Iran.

328. Despite the lack of obligation, some larger FIs and casinos are utilising third party screening databases to check for sanctioned entities. No cases were reported of a private sector entities having a match with a UN sanction listed persons or entity, including a false positive.

FIs and DNFBPs' understanding of and compliance with obligations

329. There appears to be little awareness amongst FIs/DNFBPs of the relevant UNSCRs. The limited obligations imposed by the 2018 IRR and BSP circular only came into effect in November 2018. Some larger FIs and casinos are conducting TFS screening checks through third party screening providers. AML/CFT policies of covered persons do not include provisions for TFS relating to PF.

330. While there is no requirement for covered persons to submit STRs on TFS relating to PF, a number of covered persons indicated that if they had a name match they would report this via STR to the FIU. There have however been no STRs submitted relating to TFS related to PF.

Competent authorities ensuring and monitoring compliance

331. In the absence of a legal framework for TFS related to WMD proliferation, there is no authority mandated to ensure and monitor compliance with TFS related to PF obligations. While there is no requirement for doing so, BSP, has a general provision in its revised Examination Manual requiring examiners to validate if customers are matched with the "UN Sanctions List". BSP claims that this includes all applicable UNSCRs, but this has no practical bearing as there is no obligation for FIs to freeze the funds and/or assets of designees.

Overall conclusions on effectiveness with IO.11

332. Philippines does not have a framework for implementing TFS relating to PF.

333. **The Philippines has a low level of effectiveness for Immediate Outcome 11.**

⁷⁶ UN Comtrade Database <https://comtrade.un.org/data/>

CHAPTER 5. PREVENTIVE MEASURES

*Key Findings and Recommended Actions***Key Findings**

- 1) Overall, bank, and their subsidiaries, in the Philippines have a sound understanding of their ML/TF risks and AML/CFT obligations, are implementing a risk-based approach (RBA) and have functioning money laundering prevention programs (MLPPs).
- 2) However, banks continue to face significant challenges with some CDD obligations. These include ongoing CDD and account monitoring, understanding customer source of funds, identifying and verifying beneficial owners and establishing ultimate beneficial ownership. Some banks have been reluctant to apply reduced due diligence measures, although this is now being used more widely (where ML/TF risks are lower).
- 3) Following an extensive re-registration process, the MSB sector has been consolidated. The overall level of understanding of ML/TF risks and AML/CFT obligations by the re-registered MSBs is developing. There are controls in place intended to detect and prevent unregistered MSBs from operating. However, these are not sufficient to detect MSBs such as small hawala operators that may not rely on bank accounts to transact and/or do not have a significant physical presence.
- 4) For the SEC and IC supervised FIs, the level of understanding of ML/TF risks, AML/CFT obligations and levels of AML/CFT compliance are mixed. Some larger and internationally affiliated FIs have comprehensive MLPPs in place, which include a RBA. However, for other SEC and IC supervised FIs, understanding of and adherence to these requirements is less developed. In part, this is due to the lower level of AML/CFT specific supervision conducted by SEC and IC prior to 2018.
- 5) The overwhelming majority of CTRs and STRs in the Philippines are made by universal and commercial banks. The volume of reports is increasing, along with quality and timeliness. In the newly consolidated MSB sector, there has also been an increase in the volume and quality of CTR/STR reporting. For other types of FIs, the levels of registration with AMLC to enable CTRs/STRs to be reported, and the number of FIs that are now actively reporting, has also increased steadily. This is positive, particularly for SEC and IC supervised FIs, where registrations with AMLC were previously low.
- 6) The requirements for enhanced CDD and account monitoring, particularly relating to high risk customers such as PEPs, MSBs and NPOs are understood by FIs, particularly by the banks. This is also the case for other enhanced measures, such as wire transfer rules and requirements relating to higher risk countries identified by FATF. However, some FIs face challenges in implementing enhanced or specific measures comprehensively.
- 7) In relation to TFS obligations, some FIs, including higher risk FIs, were unaware of the requirement to immediately freeze property or funds of persons or entities designated under the relevant UN Sanctions regimes. These FIs stated they had no legal power to freeze funds and were unclear that the standing freeze order provided by AMLC Resolutions TF-01 and TF-02 of 2012 authorised them to do so. Instead, some FIs stated they may refund or release funds and file an STR.
- 8) For DNFBPs, the requirements to comply with AML/CFT obligations are currently being implemented. Large or internationally affiliated DNFBPs, particularly in the casino sector, have

made considerable progress towards readiness to comply with AML/CFT obligations, although understanding of ML/TF risks is still developing. For the many other DNFBPs, including smaller or regional DNFBPs, their readiness is in its infancy. The integrated resort casinos and the PAGCOR operated land-based casino have registered with AMLC. Overall however, only a very low number of DNFBPs had registered with AMLC as at the time of the on-site visit.

- 9) There are concerns regarding casinos outsourcing of CDD obligations to junket operators, given the identified major risks posed by junkets and the fact junket operators are not regulated.
- 10) Real estate agents are not covered persons under the AMLA.

Recommended Actions

- a) Extend AML/CFT controls directly to casino junket operators, or strictly enforce agency requirements to ensure appropriate agreements are in place, and are subject to adequate supervision.
- b) The Philippines should include real estate agents as covered persons under the AMLA.
- c) Implement measures to ensure:
 - i. Universal and commercial banks should continue to implement a RBA and further improve AML/CFT measures in relation to ongoing CDD and monitoring, understanding source of funds and beneficial ownership.
 - ii. MSBs should maintain a RBA as they embed their newly established MLPPs. Competent authorities should continue to take steps to ensure that previously registered MSBs are no longer operating and apply appropriate sanctions to any found to be doing so. Competent authorities should also take steps to identify and apply appropriate sanctions to any MSBs, such as smaller hawala operators, that have never been registered.
 - iii. Other FIs should ensure that they understand their ML/TF risks, implement a RBA and their AML/CFT obligations, including the requirement to report CTRs/STRs.
 - iv. FIs should apply reduced due diligence (where lower ML/TF risks are identified) to promote financial inclusion.
 - v. FIs should continue to improve their understanding and implementation of TFS obligations.
- d) Review legal framework to determine whether scope of capture of DNFBPs as covered persons meets FATF standards and is fit for purpose in the Philippines. Conduct further outreach to DNFBPs (other than the integrated resort casinos and trust entities) to clarify which are captured as covered persons, the extent to which their activities are captured by AMLA, and to promote registration with AMLC. This should be prioritised to 1) casinos, 2) jewellery dealers and dealers in precious metals or stones, 3) company service providers (CSPs), and then 4) law and accounting sectors. This outreach should leverage relationships with other regulatory and self-regulatory bodies, as well as industry associations.
- e) Provide further education and assistance to enable DNFBPs (other than to trust entities) to identify, understand and assess their ML/TF risks, implement their AML/CFT obligations on the basis of risk; and to report CTRs/STRs. This should also be prioritised to 1) casinos, 2) jewellery dealers and dealers in precious metals or stones, 3) CSPs, and then 4) law and accounting sectors.

334. 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 R9-23.

Immediate Outcome 4 (Preventive Measures)

Background and context

335. ***Banks*** - The Philippines' financial system is dominated by the banking sector. There are 42 universal and commercial banks and 103 subsidiaries of banks that offer securities products. There are also 545 rural and thrift banks comprising the remainder of the banking sector. The 2017 NRA assessed the banking sector as highly vulnerable to ML/TF. However, after considering existing AML/CFT controls, its net vulnerability to ML/TF was assessed as medium.

336. ***MSBs*** - The Philippines MSB sector is large and is also supervised by BSP. In 2017, new registration and fit and proper requirements were introduced to increase the level of AML/CFT competency and compliance. This required all MVTS providers, foreign exchange dealers, money changers and virtual currency exchanges to register, or re-register, with BSP. MVTS providers are now referred to as Remittance Transfer Companies (RTCs) and include e-money issuers (EMIs) and any remittance agent with more than one office. Smaller agents (i.e. with only one office) are considered an extension of the RTC that they are an agent for. Of 1,621 potential re-registrants in the MSB sector, approximately 1,000 had re-registered as at the time of the on-site visit. This represents a significant restructure, and consolidation, of the MSB sector. The 2017 NRA (which was completed before the restructure) assessed the MSB sector as highly vulnerable to ML/TF due to the common use of cash, high exposure to overseas customers and low levels of AML/CFT compliance. The MSB sector's net vulnerability to ML/TF was assessed as medium-high. The net vulnerability to ML/TF of the restructured MSB sector has not been assessed.

337. ***Other FIs supervised by BSP*** - This comprises 65 Non-Stock Saving and Loan Associations (NSSLAs) and six e-money issuers (EMIs). NSSLAs provide services to military or government employees. After considering existing AML/CFT controls and supervision by BSP, the 2017 NRA assessed the net vulnerability of both NSSLAs and EMIs to ML/TF as medium. In 2017 EMIs were re-classified as RTCs under the new MSB registration provisions.

338. ***SEC supervised FIs*** - The FIs in the securities sector that are supervised by SEC for AML/CFT requirements comprise 142 brokers/dealers, 38 investment houses/securities underwriters, 26 government securities dealers and 85 investment companies/mutual funds. 98% of these FIs, by total asset size, are also subject to BSP's consolidated supervision. The 2017 NRA assessed the net vulnerability to ML/TF of the securities sector as medium. Also supervised by SEC are those financing and lending companies that have more than 40% foreign equity or with a paid-up capital of PHP10 million or more. Of 681 financing companies and 2,535 lending companies in total, there are 426 financing⁷⁷ and 76 lending companies supervised by SEC and required to comply with AML/CFT obligations. The 2017 NRA assessed their vulnerability to ML/TF as medium-low. However, due to a lack of active AML/CFT supervision by SEC, their overall net vulnerability to ML/TF was assessed as medium.

339. ***IC supervised FIs*** - The insurance sector comprises insurance companies (26 life, 54 non-life, five composite, one reinsurer), 35 mutual benefit associations and 18 pre-need companies. These FIs

⁷⁷ There are a further 5 financing companies that are under BSP supervision.

are supervised by IC for AML/CFT requirements. The 2017 NRA assessed the net vulnerability of the insurance sector to ML/TF as medium.

5 340. *Casinos* – The Philippines casino sector is very large and growing at a rapid rate. Casino related tourism and junket operators, including the international movement of funds in relation to junket operations, is significant. The Philippines advised that there are 94 casinos that are covered persons under AMLA. This includes the nine integrated resort casinos which account for 70% of the casino market, the PAGCOR branded land-based casino and online casinos. There are a further 931 entities (252 e-games, 565 e-bingo, 108 sports betting and six poker houses) that are technically classified as casinos. Consideration is currently being undertaken by PAGCOR to determine whether, and if so, the extent to which they can be exempt from AML/CFT obligations due to a low level of ML/TF risk. The casino sector is predominantly supervised for AML/CFT requirements by PAGCOR. However, 27 of the online casinos are separately supervised for AML/CFT requirements by CEZA. AMLC services as co-supervisor for all casinos. Casinos AML/CFT requirements took effect in November 2017. The 2017 NRA assessed the casino sector as highly vulnerable to ML/TF. Due to lack of AML/CFT requirements at the time of the 2017 NRA, its net vulnerability to ML/TF was assessed as high.

341. *Other DNFBPs* – These comprise of jewellery dealers and dealers in precious metals or stones, company service providers (CSPs), lawyers (or law firms) and accountants (or accounting firms). The Philippines advised that seven industry associations for jewellery, precious metal or stones dealers (representing 250 dealers) and 23 large individual dealers, 11 CSPs, 43 law firms and 28 accounting firms were prioritised for bringing in as covered persons. There are many more DNFBPs, including in smaller or regional centres around the Philippines that are likely only providing activities captured by AMLA on a lesser scale and have not yet been engaged with. In relation to jewellery dealers and dealers in precious metals or stones, there are likely to be thousands of small businesses, many of whom may never conduct transactions over the PHP1,000,000 (USD18,600) threshold. All these DNFBPs are supervised by AMLC and their AML/CFT requirements took effect in May 2018. For jewellery dealers and dealers in precious metals or stones and CSPs, the 2017 NRA assessed their net vulnerabilities to ML/TF as medium. For lawyers and accountants, their net vulnerability to ML/TF was also assessed as medium.

342. *Trust Entities* - In the Philippines, acting as a trustee or administering a trust requires a license pursuant to s79 of RA 8791. CSPs, lawyers and accountants are not able to provide trust or trustee services. There are 39 trust entities, which are licensed, considered to be FIs and supervised by BSP. Most of the trust entities are subsidiaries of banks. Due to existing AML/CFT controls and alignment with the banking sector, the 2017 NRA assessed their net vulnerability to ML/TF as medium.

Understanding of ML/TF risks and AML/CFT obligations

Financial Institutions

343. Overall, banks in the Philippines, who are supervised by BSP, appear to have a sound understanding of the NRA and an improving understanding of their ML/TF risks and AML/CFT obligations. In part, this is due to BSPs AML/CFT supervisory framework which includes a comprehensive and proactive outreach program to banks to promote understanding of risks and obligations (see IO.3). Given that the total assets of the banking sector accounts for 96% of the GDP of the Philippines, the level of understanding by banks of their ML/TF risks and AML/CFT obligations is materially significant.

344. All universal and commercial banks reported comprehension of the NRAs and that the findings of the NRAs, in conjunction with internal reviews, ongoing dialogue with other banks, BSP and AMLC, were used to create or update their own ML/TF risk assessments. The impact of the 2016 Bangladesh Bank Heist (see IO.7) on the banks was also evident. Banks acknowledged that this had prompted significant review of ML/TF risks (and MLPPs) across the banking sector.

345. BSP supervisory findings indicate that universal and commercial banks have a sound understanding of the risks associated with their products, services, delivery channels, countries or geographical areas of operation and customer base. This included awareness of their higher risk customer types such as PEPs, NPOs, other FIs, particularly MSBs, casinos and casino junkets. The banks understood the respective ML/TF risks associated with these higher risk customers and the additional AML/CFT requirements required to mitigate these risks. Overall, the universal and commercial banks presented sound understanding of the full range of AML/CFT obligations, including CDD, EDD, record keeping, CTR and STR reporting and other specific measures. This is consistent with discussions with banks during the on-site visit.

346. For rural and thrift banks, the assessment team considers the understanding of the NRAs, their ML/TF risks and AML/CFT obligations, to be basic but functioning. This is consistent with their business activity and risk profile.

347. In the newly structured MSB sector, some FIs, particularly RTCs, are large and have networks of agents. The level of understanding of the NRA, ML/TF risks and AML/CFT obligations of these MSBs is developing. This includes EDD, other specific measures, CTR and STR reporting. Many RTCs are also affiliated or partnered with banks and international remittance companies, which further assists in their understanding of ML/TF risks and management of AML/CFT policies and procedures. The BSP assess the overall level of understanding of ML/TF risks and AML/CFT obligations across the newly restructured MSB sector to be reasonable.

348. While the new MSB industry framework has only recently commenced, it provides a strong foundation for the MSB sector to understand its ML/TF risks and AML/CFT obligations as it matures. This is in contrast with the previous registration system, which was not robust and the level of understanding of ML/TF risks and AML/CFT obligations to be at best, mixed.

349. For NSSLAs and EMIs that are also supervised by BSP, the level of understanding of ML/TF risks and AML/CFT obligations is functional. This is broadly consistent with their types of product, service and risk profile, although the exposure of some NSSLAs to funds from domestic PEPs should be noted.

350. The FIs supervised by SEC have had a lower level of AML/CFT specific supervision and engagement to date (see IO.3). For example, prior to the November 2018 version, SEC's previous AML Guidelines omitted significant AML/CFT requirements that were contained in the 2016 RIRR, including important risk-based obligations. Also, the first thematic audit of AML/CFT compliance across the SEC supervised FIs was only undertaken in mid-2018. The thematic audit, which was only a basic review of the level of AML/CFT understanding and compliance, determined that there were deficiencies. Of particular concern regarding the SEC supervised FIs, there has been very limited engagement with the 426 financing companies and 76 lending companies in relation to their AML/CFT obligations.

351. Overall, for SEC supervised FIs, the assessment team considers there to be a much lower level of understanding of the NRAs, ML/TF risks and AML/CFT obligations when compared to the banking sector. The exception to this is the larger or internationally affiliated FIs, where the level of understanding of ML/TF risks and AML/CFT obligations is more developed.

352. For the FIs supervised by IC, there has also been a lower level of AML/CFT specific engagement and supervision by IC to date when compared to the banking sector (see IO3). Again, prior to the latest September 2018 version, IC's previous guidelines, including important risk-based requirements, did not comply with the 2016 RIRR. In addition, an advisory to FIs regarding the 2017 NRA was only issued in June 2018, and neither the 2015 nor 2017 NRAs were published on the IC website until May and June 2018 respectively. Further, and while a (non-anonymous) survey conducted by IC of its FIs for the 2017 NRA presented reasonable understanding (and implementation) of AML/CFT obligations, subsequent supervisory inspections by IC identified deficiencies in practice. The assessment team notes that these supervisory inspections only considered AML/CFT understanding and compliance at a basic level.

353. Overall, for IC supervised FIs, the assessment team also considers there to be a lower level of understanding of the NRA, ML/TF risks and AML/CFT obligations when compared with the banking sector. Again, the exception to this is the larger or internationally affiliated FIs, where the level of understanding of ML/TF risks and AML/CFT obligations is more developed.

DNFBPs

354. DNFBPs, as covered persons under the AMLA, are in the early stages of having to understand their ML/TF risks and AML/CFT obligations.

355. For casinos, the implementing rules and regulations (CIRR) took effect in November 2017 but casinos had until August 2018 to register as a covered person with AMLC. While the integrated resort casinos and PAGCOR operated land-based casino have done so, very few of the online casinos had as at the date of the on-site visit (further detail below). For other DNFBPs, the implementation of their requirement to comply with the AMLA and its IRR is even more recent. AML/CFT Regulatory Issuance B(1) took effect in May 2018 and DNFBPs had until 29 December 2018 to register with AMLC. Again, as at the date of the on-site visit, very few of the many other DNFBPs had done so (further detail below).

356. In the casino sector, PAGCOR, as the main gaming regulator and AML/CFT supervisor, has undertaken significant work in preparation for casinos becoming AML/CFT covered persons. The casino sector was included in the preparation of the 2015 and 2017 NRA. There has also been considerable engagement with some casinos to prepare them for having to comply with AML/CFT obligations. As at the date of the on-site visit, this has primarily and justifiably focussed on the large land-based casinos. This includes the integrated resort casinos, four of whom have conducted a casino sector risk assessment in conjunction with PAGCOR.

357. Amongst the casinos, the integrated resort casinos are shown to be investing resources and adapting existing controls and systems for AML/CFT compliance. The integrated resort casinos have undertaken training on their ML/TF risks and AML/CFT obligations. Notwithstanding this, a number of casinos understanding of their ML/TF risks was still developing. Importantly, the significant risks associated with proxy betting and junkets (as shown by the 2016 Bangladesh Bank Heist) need to be better understood so that effective AML/CFT measures can be implemented. Under the CIRR and PAGCOR's CDD Guidelines, it is possible for casinos to outsource the conduct of CDD to junket operators (as an agent of the casino, see c.22.5). The assessment team notes there are currently no AML/CFT requirements imposed directly on, or specific to, junket operators.⁷⁸

⁷⁸ The Philippines advised that it does not consider it necessary to impose AML/CFT requirements on junket operators because responsibility for compliance (when junket operators act as an agent) is on the casino. The Philippines notes that the FATF standard does not require AML/CFT requirements to be imposed directly on junket operators.

358. For the online casinos, some of whom are supervised by CEZA, the level of understanding of ML/TF risks and AML/CFT obligations is still in its infancy. This is also so for any of the 931 other entities that are classified as casinos (if they are not exempted by PAGCOR from AML/CFT obligations).

359. Notwithstanding the positive steps being taken by some casinos to understand their ML/TF risks and AML/CFT obligations, there is a lack of clarity around the extent to which the AMLA applies to their operations (see R.22). Most fundamentally, both AMLA and the CIRR define casinos to (only) be covered persons with respect to their 'cash' transactions relating to their gaming operations.⁷⁹ Contradicting this, PAGCOR's subsequently issued CDD Guidelines for land-based casinos⁸⁰ impose AML/CFT obligations for wider types of transactions and financial services in casinos. The Philippines advised the reference to 'cash' transactions in the definition of casinos as covered persons relates to CTR obligations. However, the assessment team notes this is not what the wording in the definition states. Authorities advised that because the CDD Guidelines are 'enforceable means', casinos are required to comply with AML/CFT obligations for the broader set of financial services and transactions. The assessment team acknowledges that the CDD Guidelines constitute 'enforceable means'; however the team finds that there is not persuasive evidence that the CDD Guidelines are able to extend the scope of AML/CFT obligations beyond the definition of covered person that is set out in the AMLA (and the CIRR).

360. The assessment team considers that the lack of clarity regarding the extent to which AMLA applies to casino operations affects the sector's understanding of its AML/CFT obligations. Some casinos appear aware of the differing requirements of AMLA, the CIRR and the CDD Guidelines regarding the extent to which AML/CFT obligations apply to their operations. The team notes some confusion in the casino sector regarding obligations, although casinos indicated their intention to comply with the requirements of the CDD Guidelines.

361. For other DNFBPs, there has also been outreach and awareness campaigns to prepare them for coverage as AML/CFT covered persons. As at the date of the on-site visit, this has primarily and justifiably focussed on the large and/or internationally affiliated DNFBPs. These engagements have been conducted by AMLC as the AML/CFT supervisor of DNFBPs. For jewellery dealers and dealers in precious metals or stones, there has been engagement with 23 large dealers and with seven industry associations (representing 250 dealers) regarding AML/CFT coverage. Similarly with 11 CSPs, 43 law firms and 28 accounting firms, as well as with some real estate agents who are not covered persons. So far, AMLC has reasonably focussed on education regarding the 2017 NRA, ML/TF risks and on preparing DNFBPs to meet their upcoming AML/CFT obligations.

362. For jewellery dealers and dealers in precious metals or stones, who are new to regulation, the outreach and engagement undertaken so far has been positive. However, with thousands of small businesses operating in this sector, the overall level of understanding of ML/TF risks and AML/CFT obligations is still in its infancy. There is also a complicating factor regarding the extent to which AML/CFT obligations apply, or should apply, to jewellery dealers and dealers in precious metals or stones. The AMLA states that these dealers are covered persons when they trade in transactions in excess of PHP1,000,000 (USD18,600). However, the 2018 IRR states that all jewellery dealers and dealers in precious metals or stones are covered persons (rather than only those trading in transactions over the threshold - see R.22). The inconsistency between the AMLA and its IRR is not conducive to the understanding of AML/CFT obligations within the sector. The assessment team also notes that many

⁷⁹ Cash' is defined in the CIRR as 'currency notes and coins'. For land-based casinos, this limits the scope of the AML/CFT obligations. This also excludes all online casinos from being covered persons.

⁸⁰ PAGCOR's CDD Guidelines for Offshore Casinos is not yet published.

jewellery dealers or dealers in precious metals or stones are small businesses that may never conduct in transactions in excess of PHP1,000,000 (USD18,600).

5 363. Amongst CSPs, law firms and accounting firms, the larger or internationally affiliated entities appear to have a reasonable understanding of ML/TF risks and their AML/CFT obligations.⁸¹ However, across the many smaller or regional CSPs, law and accounting firms (or sole practitioners) with whom there has been minimal AML/CFT engagement so far, the level of understanding of ML/TF risks and AML/CFT obligations is limited.

364. As with the other DNFBP sectors, there is also a complicating factor relating to the extent to which AML/CFT obligations apply to CSPs, lawyers and accountants. Under the AMLA, the 2016 and 2018 IRR, CSPs, lawyers (or law firms) and accountants (or accounting firms) are covered persons if they engage in various specified activities. When so, the 2018 IRR and Regulatory Issuance B(1) then indicate that AML/CFT obligations must be applied to all their customers (rather than requiring CDD only for customers engaging in those specified activities). This would, if correct, extend AML/CFT obligations to professional activities that may pose little or no ML/TF risk at all. The Philippines advised that CSPs, law firms or accounting firms (that are covered persons) are not required to comply with AML/CFT obligations in relation to professional services that are not specified in AMLA. However, the assessment team's view is that this is not clear in the IRR or Regulatory Issuance B(1). There are concerns that this lack of clarity has hindered CSPs, law firms and accounting firms preparation for implementing AML/CFT obligations, both within their own business and across the wider sectors. Some CSPs, law firms and accounting firms may, out of caution, comply with AML/CFT obligations in relation to all their customers, (rather than just those for whom they undertake the various specified activities).

365. Of the trust entities, which are licensed, considered as FIs in the Philippines and supervised by BSP, most are subsidiaries of banks. These trust entities leverage from their parent bank's AML/CFT capability and resource. This has resulted in sound understanding of the NRAs, their ML/TF risks (as relevant to their sector) and AML/CFT obligations.

366. Real estate agents are not covered persons under the AMLA.

Application of risk mitigating measures

Financial Institutions

367. As set out in s.X805.5 of the MORB, all banks in the Philippines are required to identify, understand and assess their ML/TF risks arising from customers, countries or geographic areas, products, services, transactions or delivery channels. Indeed, most universal and commercial banks in the Philippines conduct regular or ongoing, enterprise ML/TF risk assessments. There are also policies and procedures in place to ensure that risk assessments are regularly reviewed and updated. For those banks that have not completed an enterprise wide risk assessment, this is considered a priority. The BSP, during its examinations of banks, also emphasises the importance of doing so.

368. Universal and commercial banks have shown understanding that identifying their ML/TF risks is central to being able to implement a RBA and have an effective MLPP, which has been tested in BSP's AML/CFT supervision and demonstrated during the ME onsite. As is required by s.X806 of the MORB, risk rating systems are applied to customers, classifying them as low, medium or high risk by considering various risk factors. This informs the level of CDD and account monitoring that must be

⁸¹ Lawyers and accountants acting as legal professionals are excluded from the requirements of covered persons in relation to information subject to client confidences or attorney-client privilege.

conducted and the frequency with which reviews must be undertaken and the procedures for higher risk customers, such as PEPs, NPOs and MSBs, and the circumstances in which EDD is required.

369. Since 2013, BSP's supervision of the banking sector has incorporated an AML Risk Rating System (ARRS). Output from ARRS indicates a steady improvement in the AML/CFT frameworks that are in place at banks across the banking sector (see IO3). This is consistent with the findings of the assessment team.

370. For rural and thrift banks, the assessment team considers the implementation of risk mitigation measures and a RBA to be simple but functioning and consistent with their risk profile.

371. Most MSBs appear to have conducted an enterprise wide risk assessment and demonstrated a sound understanding of the requirements for a RBA. MSBs also implement requirements for risk rating customers, conducting account monitoring and the need for enhanced CDD for higher risk transactions and customers such as PEPs. Notwithstanding this, the wider implementation of a RBA across the MSB sector, particularly among smaller MSB, is still in its early stages. In part, this reflects the transition from the previous MSB sector where the implementation of risk mitigation measures appears to have been very mixed. The assessment team considers that the new structure of the MSB sector provides a strong framework for the implementation of ML/TF risk mitigation measures moving forwards.

372. The BSP has a framework in place with both local government units (LGUs) and banks to identify unregistered MSBs and to prevent them from operating (see R.14). Since 2017, BSP's priority has been promoting and ensuring re-registration of all operating MSBs under the new system (see IO.3), with the date for re-registration extended until 30 April 2018. At the date of the on-site visit, no fines (or terms of imprisonment) had been imposed on a previously registered MSB for continuing to operate while unregistered under the new system. Nor in relation to a MSB that has never been registered with BSP. The Philippines advised that the framework with LGUs and requirements imposed on banks relating to MSBs make it difficult for an unregistered MSB to operate. However, the assessment team's view is that small MSBs without a significant physical presence, and/or that use a hawala system without bank accounts, are unlikely to be detected by the current framework.

373. For NSSLAs and EMIs that are supervised by BSP, risk mitigation measures and the implementation of a RBA appears to be simpler. However, this is sufficient considering their narrower range of products and service and overall risk profile.

374. For SEC and IC supervised FIs however, the risk mitigation measures and implementation of a RBA appears to be much less developed. Neither SEC nor IC updated their guidelines to fully reflect the risk-based requirements until late 2018, and these requirements have not been supervised consistently (see IO.3 for information on SEC and ICs conduct of AML/CFT supervision). As a result, the implementation of risk mitigation measures and a RBA by FIs is far more variable in the SEC and IC sectors. Again, the exception to this is the larger or internationally affiliated FIs, where the risk mitigation measures and implementation of a RBA is more developed.

DNFBPs

375. For DNFBPs, the application of risk mitigating measures are in the preliminary stages of implementation.

376. In the casino sector, the large land-based casinos, particularly the integrated resort casinos, appear to have a reasonable understanding of a RBA. However, implementation of a RBA is still in its

early stages. For online and any other casinos, the level of understanding and implementation of a RBA is minimal.

377. For jewellery dealers and dealers in precious metals or stones, who are new to regulation, their level of understanding and readiness for implementing a RBA is in its infancy.

5

378. Large or internationally affiliated CSPs, law firms and accounting firms demonstrated a reasonable understanding of a RBA. Again however, the implementation of a RBA is still in its very early stages. For the many smaller or regional CSPs, law and accounting firms (or sole practitioners) the level of understanding of a RBA is minimal.

379. For trust entities that are supervised by BSP, risk mitigation measures and the implementation of a RBA appears to be simple but functioning. This is sufficient considering their narrower range of products and service and overall risk profile.

Application of CDD and record keeping requirements

Financial Institutions

380. Universal and commercial banks in the Philippines appear to have comprehensive CDD and record keeping systems based on an RBA. Most utilise technology systems for CDD, record keeping and account monitoring, although some systems are more sophisticated than others. For example, not all banks review ML/TF risks at a transactional level unless there are concerns about a customer.

381. Supervision and feedback from the sector indicate that all universal and commercial banks risk rate customers at on-boarding in accordance with their obligations. This forms the basis of their account monitoring and ongoing CDD. For higher risk customers such as MSBs and NPOs, banks appear to understand risk management and policies and procedures are in place for CDD and enhanced monitoring. Banks appear to understand the importance of charitable/humanitarian works that NPOs provide and the need for financial inclusion, and keep an awareness of balancing de-risking of MSBs and NPOs. Notwithstanding this, the assessment team notes that BSP considers that de-risking of MSBs, which is driven by foreign banks, is a significant issue that is impacting on financial inclusion in the Philippines (see Chapter 1).

382. Banks have procedures and policies to promote financial inclusion, allowing reduced due diligence on certain customers where lower ML/TF risks are identified. However, some banks have not always implemented reduced due diligence appropriately, preferring to take a conservative approach. As with the de-risking of MSBs, a reluctance by banks to allow reduced due diligence (where lower ML/TF risks are identified) has an adverse impact on financial inclusion. The BSP advised that this conservative approach was not prevalent to all banks and that in any event, an appropriate use of reduced due diligence is now widely applied.

383. Banks also have procedures in place to refuse or close accounts when CDD cannot be completed. A survey of 27 universal and commercial banks conducted by BSP determined the number of accounts refused or closed as follows:

Table 5.1: Number of accounts closed by banks due to incomplete CDD

	2013	2014	2015	2016	2017
Closed accounts due to incomplete CDD	30,187	12,838	11,666	21,769	48,391

384. Notwithstanding the comprehensive AML/CFT systems for CDD and record keeping that the banking sector has in place, some universal and commercial banks report that there are still challenges with some AML/CFT obligations.

385. Notably, many universal and commercial banks report challenges in meeting their ongoing CDD obligations. For example, BSP CL. No. 950 requires updating customer CDD records at least every three years, or more frequently if enhanced account monitoring is required. Banks advised that this is not a problem in itself and they are comfortably able to update CDD records within this timeframe, and for higher risk customers, annual updates are the norm. However, as is acknowledged by the banks, updating CDD records only constitutes part of the ongoing CDD and account monitoring obligation. The challenge, as reported by many banks, is to also understand the customer's business activity and to ensure it is consistent with their CDD records and risk profile. This includes the requirement to understand the source of customer funds, which many banks consider to be a significant issue for the effectiveness of their MLPPs. The BSP advised that banks are taking steps to address these challenges and that compliance with ongoing CDD obligations is improving.

386. Another challenge experienced by universal and commercial banks relates to identifying the beneficial owners of corporate clients, particularly establishing ultimate beneficial ownership. Many banks primarily utilise self-declarations and copies of the General Information Sheet (GIS) provided by the client (see IO.5 for deficiencies in the GIS process). Verification from other sources is used to a lesser extent. Many banks perceive that failure to understand the beneficial ownership of corporate clients is a significant AML/CFT compliance issue. The BSP acknowledge that identifying beneficial ownership can be challenging for the banking sector, particularly in relation to the ultimate beneficial owners, and/or where there are complex ownership structures involving overseas legal persons. The BSP advised that it is working with banks in relation to this, and that banks are taking steps to address these challenges.

387. Most banks utilise technology solutions, either developed in-house or by third-party providers, to comply with CDD and record keeping requirements. Manual or excel based systems are used to a far lesser extent. For transaction monitoring, automated technology solutions are used to an even greater extent than for CDD and record keeping, with only a small percentage of banks relying on manual or excel systems. The banks agree that technology solutions are an important part of being able to comply with CDD and record keeping requirements.

388. For rural and thrift banks, the CDD, record keeping and account monitoring systems are more rudimentary but functional. For example, in rural and thrift banks, manual or spreadsheet systems are more common. The importance of financial inclusion is understood by rural and thrift banks, with procedures and policies in place for reduced due diligence where lower ML/TF risks are identified. However, as with universal and commercial banks, BSP assess that reduced due diligence has not always been appropriately implemented, with some banks preferring to take a conservative approach. The BSP advised that a conservative approach was not prevalent to all rural and thrift banks and that in any event, appropriate use of reduced due diligence is now increasingly applied.

389. For the MSB sector, the new registration requirements are intended to improve the overall level of AML/CFT competency and compliance, which includes CDD and record keeping obligations. Initial findings suggest that this has occurred, with the re-registered MSBs now better equipped to comply. Some larger MSBs utilise technology-based systems for CDD and account monitoring. MSBs appear to have a sound understanding and application of the range of CDD and record keeping requirements. This contrasts with the previous registration system, where application of CDD and record keeping requirements was at best, mixed.

390. For NSSLAs and EMIs, as well as SEC and IC supervised FIs, the application of CDD and record keeping requirements varies. While some larger and internationally affiliated FIs have comprehensive systems in place, including technology-based systems, for other FIs, adherence to these requirements is less developed. For SEC and IC supervised FIs, this is in part due to the lower level of AML/CFT specific supervision prior to 2018.

DNFBPs

5

391. For DNFBPs, the requirement to comply with CDD and record keeping obligations are in the preliminary stages of implementation.

392. Casinos have existing operational processes and procedures for keeping records relating to their customers. Larger casinos are in the process of modifying these to comply with CDD and record keeping requirements. The large and integrated resort casinos have made considerable progress towards being able to meet their CDD and record keeping requirements using technology solutions. For online and any other casinos, the level of readiness to comply with CDD and record keeping obligations is minimal.

393. Under the CIRR casinos can rely on third parties which are covered persons, or FIs and DNFBPs subject to similar CDD requirements in foreign jurisdictions, or can outsource CDD to a 'counterparty, intermediary or agent'. The assessment team is concerned about casinos reliance on junket operators for the purpose of CDD, noting that they are not covered persons in the Philippines and the team was not satisfied that arrangements with junket operators fall under an agency agreement. Given the high ML/TF risk of the casino sector and that junkets were one of the identified major risks to land-based casinos in the 2017 NRA, additional measures should be implemented to either capture junket operators as covered persons or check the adequacy of the CDD arrangements in place.

394. For jewellery dealers and dealers in precious metals or stones, the existing processes and procedures for keeping records relating to customers are more limited. Their level of readiness to comply with CDD and record keeping requirements is in its infancy.

395. CSPs, law firms and accounting firms also have existing operational processes and procedures for keeping records relating to their customers. Due to international business relationships, some large or internationally affiliated law and accounting firms conduct CDD and record keeping measures to comply with AML/CFT requirements of other jurisdictions. For the many smaller or regional CSPs, law and accounting firms (or sole practitioners), the assessment team consider the level of readiness to comply with CDD and record keeping obligations to be much less developed.

396. For trust entities that are supervised by BSP, the application of CDD and record keeping requirements is functional.

Application of enhanced or specific measures by FIs and DNFBPs

Politically Exposed Persons (PEPs)

397. Universal and commercial banks appear to have a sound understanding of the enhanced measures relating to PEPs. It appears that when a PEP is identified, the enhanced CDD requirements are applied reasonably across the banking sector. This is consistent with the findings of BSP.

398. Notwithstanding this, identifying beneficial ownership, particularly ultimate beneficial owners, remains an ongoing challenge for banks (as discussed above). These challenges are likely to

extend across into the ability to identify PEPs, particularly if family members or associates are used to conceal beneficial ownership. The BSP advised that it is working with banks in relation to this, and that banks are taking steps to address these challenges.

399. To identify PEPs, most banks utilise automated screening solutions, either developed in-house or by a third-party provider. Reliance on wholly manual screening systems is much less common. Screening is usually conducted against external databases from third-party providers and internally developed databases of PEPs, which include local Philippine content. Screening solutions are often supplemented by local knowledge at a regional or branch level. While these systems are in place in the banking sector, some deficiencies have been identified by BSP with PEP databases not being updated periodically. BSP advised that these deficiencies have generally been addressed by banks.

400. The screening systems for PEPs in rural and thrift banks are simple but functioning. The use of manual screening is more common, and significant importance is placed on the regional or local knowledge by bank staff. This is consistent with their business activity and risk profile.

401. In the newly structured MSB sector, there are now reasonable systems in place to comply with enhanced measures relating to PEPs. While some of the larger MSBs subscribe to third party databases and have internally developed databases for PEP screening, others only utilise manual open source checking. MSBs appear to have a reasonable understanding of the requirements for EDD where a PEP is identified, along with the requirements to seek senior management approval and conduct ongoing monitoring. For smaller MSBs, or those using manual systems, the application of enhanced CDD measures relating to PEPs is more challenging.

402. For NSSLAs and EMIs, as well as SEC and IC supervised FIs, the application of enhanced CDD measures relating to PEPs appears reasonable. FIs appear to understand the requirements for EDD when a PEP is identified. Notwithstanding this, the assessment team notes that other than confirming that PEP checking provisions are in place, SEC and IC's testing of the effectiveness of these policies by their FIs has been minimal. As with the banks, the same challenges relating to identifying beneficial owners also impact on a NBFIs ability to identify PEPs.

Correspondent banking

403. In general, banks are implementing correspondent banking requirements that are consistent with the FATF standards. Both banks and BSP advised that there are defined policies and procedures, including the requirement to obtain senior management approval before establishing a new correspondent banking relationship. The Wolfsberg Group questionnaire is adopted as the basic document for assessing the respondent institution. Many Philippine banks are correspondent banks and as such, are subjected to stringent ongoing due diligence by correspondent banks in other jurisdictions. There have been no cases reported of correspondent banking relationships with shell banks.

New technologies

404. The BSP has taken a cautious approach to the use of new or developing technologies in the delivery of products and services. The BSP seeks a balance between ML/TF risk mitigation and its strategic goal to promote financial inclusion, including through new technologies (see Chapter 1).

405. Within the banking sector, the requirement to conduct face-to-face on-boarding was only relaxed by BSP in 2017. This opened options for technology based on-boarding in combination with technology-based delivery of products and services. However, s.X701 of the MORB still requires banks

CHAPTER 5. PREVENTATIVE MEASURES

to seek approval from BSP prior to the launch of any new or enhanced electronic banking products. There are concurrent AML/CFT requirements in the MORB for banks to assess new products and services for ML/TF risk, including new delivery mechanisms, as well as the use of new or developing technologies for either new and existing products. This risk assessment should be an integral part of the product or service development and conducted prior to launch.

5

406. In practice, these requirements result in close coordination between banks and BSP for any use of new or developing technologies that being considered. Proposals are made to BSP, presentations are held with stakeholders and any concerns are discussed. Often BSP approves new or developing technology products on an initially limited basis only, with certain restrictions placed to manage risks. These restrictions may only be lessened after a subsequent evaluation process undertaken by BSP. The banks understood their obligations relating to new or developing technologies.

407. For NSSLAs and MSBs (including EMIs), s.4701Q of the MORNBFBI applies the same provisions. Some MSBs, particularly EMIs, have implemented products and services that use new and developing technologies, which received considerable scrutiny from BSP. MSBs appear to understand their obligations relating to new and developing technologies.

408. The use of new and developing technologies is less common for FIs supervised by SEC and IC. However, there are requirements to identify and assess ML/TF risks associated with new or developing technologies, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

409. In relation to virtual assets specifically, BSP CL. No. 944 of February 2017, classifies virtual currency exchanges as RTCs. Accordingly, they are required to comply with the registration requirements in the MSB sector, including competency and fit and proper tests. As with other NBFIs supervised by BSP, the requirements of the MORNBFBI apply, including s.4701Q that requires approval for new or enhanced electronic products. Any other FIs that are involved with virtual assets as part of their products and services are required to undertake the ML/TF risk assessment in relation to this part of their business prior to launch.

Wire transfer rules

410. Notwithstanding some deficiencies in the 2016 RIRR and the MORB, which have now been corrected, the Philippines banking sector has functioning policies and procedures in place in relation to the wire transfer rules. Banks appear to have an understanding of the wire transfer rules, including the requirements when there is incomplete originator or beneficiary information. BSP on-site and off-site examinations include reviews of compliance with the wire transfer rules. The BSP advised that the implementation of the wire transfer rules by banks has been steadily improving since 2012 and is expected to improve further. BSP surveys 27 universal and commercial banks to determine the number of wire transfers rejected by banks.

Table 5.2: Number of wire transfers rejected by banks

	2013	2014	2015	2016	2017
Number of wire transfers rejected by banks	40	116	228	455	230

411. In the MSB sector, where there are networks of agents and relationships with both banks and international remittance companies, all of which utilise their own systems, complying with the wire transfer rules is often more complex. MSBs demonstrated demonstrated an understanding of the wire transfer rules and the various requirements that must be adhered to when information is incomplete.

This provides a solid foundation for compliance with the wire transfer rules as the newly structured MSB sector matures. This contrasts with the previous registration system, where the application of the wire transfer rules was at best, mixed.

412. The Philippines advised that the wire transfer rules are applicable to banks and MSBs, although SEC's latest Guidelines include these requirements. SEC advised that the wire transfer rules were only included in its latest Guidelines so that their FIs were aware of the wire transfer rules.

Targeted financial sanctions - TF

413. Universal and commercial banks are predominantly using automated solutions for TFS screening against relevant UN Sanctions lists. As with PEP screening, BSP has identified deficiencies in the screening systems being applied by some banks. Screening by rural and thrift banks is mixed, with some relying on manual systems and open source checks.

414. In the MSB sector, some of the larger entities have also implemented automated TFS screening. However, other MSBs utilise only manual systems that involve open source checks. For the other types of FI, including those supervised by SEC and IC, the systems implemented for TFS screening are also mixed. While some larger FIs subscribe to third-party databases, others conduct open source checks only. The level of compliance with TFS screening obligations across non-bank FIs, including SEC and IC sectors is assessed as variable.

415. Some FIs, including higher risk FIs, were unaware of the requirement to immediately freeze property or funds of persons or entities designated under the UN Sanctions regime. These FIs stated they had no legal power to freeze funds and were unclear that the standing freeze order provided by AMLC Resolutions TF-01 and TF-02 of 2012 authorised them to do so. Instead, these FIs stated they may refund or release funds and file an STR.

416. The overall effectiveness of TFS screening by FIs in the Philippines appears to be limited (see IO.10). Funds have been frozen by a covered person because of TFS screening on only one occasion and there have been no instances of false positive freezing actions. Links to sanctioned entities were identified by covered persons in four instances. This is not consistent with the TF risk profile. Further, the lack of false positive freezes brings into question the implementation of TFS given the common occurrence of names on the UNSCR 1267 list. That some FIs were unaware of the requirement to immediately freeze property or funds of designated persons is a further concern.

Higher risk countries identified by FATF

417. FIs appear to be aware of risks associated with certain countries identified by FATF and apply some countermeasures. However, it appears that some FIs consider that this only applies to not dealing with countries on the FATF Public Statement (who are also sanctioned countries). There appears to be a lower level of awareness of other countries that may have weaknesses in their AML/CFT systems.

418. For DNFBPs, the application of the relevant enhanced or specified measures are in the early stages of implementation.

419. In the casino sector, there are prohibitions on domestic PEPs from entering casinos and so enhanced measures will only apply to foreign PEPs. Large land-based and integrated resort casinos demonstrated an understanding of the enhanced and specific measures relating to PEPs, new technologies, TFS and those countries identified by FATF as higher risk. With the assistance of PAGCOR,

integrated casino resorts in particular have commenced modifying their existing processes and procedures to comply with the various AML requirements. This includes implementing automated screening solutions for PEPs and TFS. For online and any other casinos, the level of readiness is minimal. The application of measures required for new technologies is particularly relevant to the online casinos.

420. For jewellery dealers and dealers in precious metals or stones, the application of enhanced and specific measures relating to PEPs, new technologies, TFS and higher risk countries is in its infancy. This is compounded by their lack of familiarity with being subject to regulation.

421. CSPs, law firms and accounting firms are in the process of adapting their existing business processes and procedures to be able to comply with the various enhanced and specific measures. They appear to have an understanding of the enhanced and specific measures relating to PEPs, new technologies, TFS and countries identified by FATF as higher risk. Notwithstanding this, the overall level of readiness to comply with the various enhanced and specific measures across the many CSPs, law and accounting firms (or sole practitioners) is minimal.

422. For trust entities that are supervised by BSP, the application of the enhanced and specified measures relating to PEPs, new technologies, TFS and those countries identified by FATF as higher risk is functioning. In relation to new technologies, trust entities have the same obligations as other FIs supervised by BSP (see above) and are required to comply with s.4701Q of the MORNBF. I.

Reporting obligations and tipping off

423. Universal and commercial banks account for the overwhelming majority of CTRs and STRs submitted to AMLC. STRs arise from alerts generated from transaction monitoring systems, or from manual referrals from branches. The number of CTRs/STRs has been steadily increasing year by year.

Table 5.3: Number of STRs and CTRs reported by Universal and Commercial Banks

	2014	2015	2016	2017	Nov 2018
Number of STRs reported by UBs/KBs	72,214	112,071	93,480	215,689	305,979
CTRs filed by UBs/ KBs	38.9 million	31.6 million	32 million	34.4 million	33.3 million

424. AMLC advised that 95% of registered banks are actively reporting CTRs/STRs. The remaining 5% of banks are small rural or thrift banks operating in remote areas with a limited number of customers and minimal transactions. The level of CTR/STR reporting is consistent with the business and risk profile of the rural and thrift banks. There are very few banks (only 0.75% of the total asset size of the banking sector) that are submitting CTRs, but not STRs.

425. Between 2013 and 2018, over 80% of reported STRs related to fraud (see IO.6). STRs related to graft, corruption or drug offence were at a much lower level but increased dramatically in 2017. This sharp increase was due to intensified LEA focus on corruption and drug trafficking. For other high-risk crime types, the number of related STRs received does not align to the risk areas. There are also very low numbers of STRs regarding terrorism, TF or kidnapping for ransom, despite the context.

426. A review of STR quality conducted by AMLC in 2017 covered the 132,306 STRs received from 149 FIs in 2016 and found that 53% were of high quality. Quality was assessed based on the completeness of information about the suspicion, the details of the transaction and the suspicious activity. AMLC has sought to address areas of weakness through detailed guidelines on STR submission,

and action plans for those banks with lower levels of STR compliance. This includes content relating to range of predicate offences (rather than focus on types of fraud).

427. The recent consolidation of the MSB sector and mandatory registration requirements have seen a large increase in CTRs/STRs reported to AMLC. In 2016 only 1,488 of 5,430 MSB head offices (27.4%) were registered with AMLC and only 98 (1.8%) were actively reporting CTRs/STRs. The number of MSBs reporting and the quality have increased following requests for action plans to MSBs that had low quality and/or numbers of STRs. While this is positive, MSBs' compliance with CTR/STR requirements across the MSB sector should be an ongoing focus that requires further development.

Table 5.4: STRs and CTRs reported by MSBs

	2014	2015	2016	2017	Nov 2018
STRs	4,549	3,073	4,593	35,688	96,896
CTRs	16,376	17,648	62,304	120,629	164,734

428. For NSSLAs and EMIs (as well as trust entities) that are supervised by BSP, approximately 64% are actively submitting CTRs/STRs. The majority of these are NSSLAs. This is consistent with the business and risk profile of these FIs supervised by BSP.

429. For both SEC and IC supervised FIs, there has been a steady increase in the number of registrations with AMLC to be able to report CTRs/STRs. In 2016, only 60% of SEC broker/dealers, 16% of mutual fund/investment advisers and 14% of investment houses had registered with AMLC. By the end of 2018, the SEC and IC sectors had increased to almost 100%.

430. There has been a dramatic increase in the number of STRs/CTRs reported by SEC and IC supervised FIs. AMLC advised that there has also been an increase in quality.

Table 5.5: Number of CTRs and STRs by SEC and IC supervised FIs

	2014	2015	2016	2017	Nov 2018
STRs reported by SEC FIs	92	70	1,931	4,018	1,924
CTRs reported by SEC FIs	493,111	595,451	744,550	848,770	910,897
STRs reported by IC FIs	362	467	697	989	907
CTRs reported by IC FIs	83,072	68,861	58,907	72,329	83,588

431. FIs appear to have a good understanding of the tipping off provisions and systems needed to be in place to manage these specific measures. Larger FIs have tight controls in place to restrict access to STR information to prevent tipping off (whether intended or unintended). These controls are particularly important for FIs operating or with branches in less populated or regional centres, where FI employees may live within the same smaller community as a person that is subject of a STR. These controls appear to have been implemented comprehensively by large FIs.

432. BSP, SEC and IC all advised that there have been no reported instances of violations of the tipping off provisions by their respective supervised FIs.

433. Casinos had until August 2018 to register with AMLC to be able to commence CTR/STR reporting. Other DNFBPs had until 29 December 2018 to do so. Other than the integrated resort casinos and the PAGCOR operated land-based casino, very few DNFBPs had registered with AMLC as at the date of the on-site visit. Table 32 illustrates the registration statistics as of 28 November 2018. AMLC attribute this low number of registrations to DNFBPs having difficulties complying with all documentary requirements. While this may explain some of the shortfall, the assessment team considers the overall number of DNFBP registrations to be very low. This is particularly so considering the total number of DNFBPs in the Philippines and that the date for casinos to register has passed.

Table 5.6: DNFBPs registered with AMLC (as of 28 November 2018)

Industry Type	Prioritised for AML/CFT coverage in the sector	Approved Registration for STR /CTR reporting	Pending completion of requirements
Casinos- Integrated Resorts	9	9	
casinos - PAGCOR operated	1	1	8
casinos - POGO	57	4	
casinos - CEZA Licensees	27	0	
casinos - APECO Licenses	0	0	
Jewellery precious metals/stones	273	2	5
CSPs	11	1	3
Accounting firms	28	2	0
Law firms	43	0	0

434. As of 28 November 2018, AMLC had received 2,016 CTRs and 375 STRs from the casino sector. It had not received reports from any other DNFBP.

Internal controls and legal/regulatory requirements impending implementation

435. Universal and commercial banks have functioning internal controls and AML/CFT compliance structures. There are established governance frameworks, with reporting lines from the compliance officer to Board of Directors, as well as reporting to risk and audit committees. There is capacity building and training for bank staff. Most banks provide role specific AML training, although some banks only provide common training to all employees. For local branches and foreign owned banks that are part of an international group, controls are aligned with parent/group standards. BSP advised that during its on-site examinations, the effectiveness of the internal controls of universal, commercial and foreign banks are generally found to be robust and satisfactory, with only minor weaknesses noted which are promptly corrected.

436. For rural and thrift banks, NSSLAs and EMIs, the controls are less sophisticated but also functioning. This is appropriate considering their business and risk profiles. In the MSB sector, the re-registration requirements have provided a strong basis for internal AML/CFT controls and a developing compliance culture moving forwards. MSBs appear to have dedicated compliance teams and an understanding of the importance of having internal controls in place.

437. For SEC and IC supervised FIs, the assessment team considers the effectiveness of internal AML/CFT controls to be mixed. While SEC and IC supervised FIs are subject to other regulatory frameworks that require controls, the assessment team notes that only limited testing of AML/CFT controls has been conducted to date. As with other AML/CFT obligations, the exception to this is the larger or internationally affiliated FIs, where the internal AML/CFT controls are more developed.

438. For DNFBPs, the requirements for internal AML/CFT controls and compliance structures are in the early stages of implementation.

439. Casinos have existing operational processes and procedures for internal controls and compliance structures in relation to other casino activities. Casinos appear to be in the process of modifying these existing processes and procedures to incorporate AML/CFT controls. The integrated resort casinos have made considerable progress towards implementing AML/CFT controls and compliance structures. For online and any other casinos, the assessment team consider the application of AML/CFT controls and compliance culture to be minimal.

440. For most jewellery dealers and dealers in precious metals or stones, the requirement to apply AML/CFT controls and introduce a compliance culture has not yet commenced.

441. CSPs, law firms and accounting firms also have existing operational processes and procedures for internal controls relating to their business activities. CSPs, law firms and accounting practices are in the process of modifying these to incorporate AML/CFT controls. Due to international business relationships, some large or internationally affiliated law firms or accounting firms are already applying AML/CFT controls to comply with requirements of other jurisdictions. For the many smaller or regional CSPs, law and accounting firms (or sole practitioners), the assessment team considers the application of AML/CFT controls and a compliance culture to be minimal.

442. For trust entities that are supervised by BSP, the internal AML/CFT controls are functioning.

Overall conclusion on Immediate Outcome 4

443. Banks and other large or internationally affiliated FIs are implementing AML/CFT measures to a significant extent. Other FIs, particularly those supervised by SEC or IC, are implementing AML/CFT measures to a lesser extent. For DNFBPs, the requirements to comply with AML/CFT obligations are currently being implemented. Large or internationally affiliated DNFBPs, particularly in the casino sector, have made progress towards implementing AML/CFT measures. For the many other DNFBPs, implementation of AML/CFT measures is negligible.

444. **The Philippines has a moderate level of effectiveness on Immediate Outcome 4.**

CHAPTER 6. SUPERVISION

*Key Findings and Recommended Actions***Key Findings**

- 1) Most supervisors have a reasonable understanding of ML/TF risks, but do not receive sufficient up to date risk information to best support their risk based approach. BSP demonstrated sound understanding of individual risk profiles of banks. However, there is less understanding on a sectoral and cross sector basis. The lack of analysis in the NRA in relation to cash, cross sector and cross border transactions has impacted the understanding of particular risks relevant to high risk sector supervisors.
- 2) The adequacy of market entry procedures differ across sectors. BSP implements robust market entry requirements for banks and trust entities. Gap exists in the frameworks for other supervisors and there is a lack of identification of beneficial ownership BSP restructured the MSBs sector in 2017 with tighter market entry requirements that prevent criminal ownership and management. There are shortcomings in identifying illegal MSBs and applying sanctions.
- 3) BSP has a prudent AML/CFT supervision framework. Thematic reviews for banks have only been introduced within past two years and are not effectively utilised. Risk-based supervisions by other supervisors is still developing. PAGCOR has a supervisory gap in covering all financial transactions of casinos and has a conflict of interest given its ownership and management of its local casinos (Casinos Filipino). It is not clear whether the scope of PAGCORs first examination included casino agents (junket operators). SEC and the SRO, CMIC, duplicate AML/CFT on-site examinations of securities market participants, which is not an efficient use of resources. There is a scope deficiency in the coverage of financing and lending companies and real estate agents are not covered persons and therefore not subject to AML/CFT supervision.
- 4) BSP has applied a range of dissuasive supervisory penalties for AML/CFT breaches using its prudential powers. Breaches of the AMLA can also be sanctioned by AMLC based on findings of other supervisors upon referral. In such cases AMLC can exercise its own AML/CFT sanction for violation of AMLA, however AMLC faces resource challenges and has not systematically pursued this option. No sanction for breaches of AML/CFT compliance have been applied by SEC, casino supervisors or by AMLC on DNFBPs.
- 5) BSP demonstrated that it has had an impact on improving the compliance of banks and MSBs. Other supervisors demonstrated minimal impact of their actions on AML/CFT compliance, noting the recent implementation of AML/CFT supervision in some sectors.
- 6) BSP has a comprehensive outreach program designed to enhance its regulated entities understanding of their obligations and risks through on-going industry dialogues, trainings and on-site examinations. PAGCOR has had reasonable engagement with larger market players. IC and SEC's engagement with their sectors is less advanced. AMLC has conducted considerable outreach to DNFBPs, however this only reached a very small numbers of DNFBPs (except casinos).

Recommended Actions

- a) SEC, IC, PACGOR, CEZA and AMLC should implement risk-based AML supervision.

- b) Sectoral vulnerability analysis should be expanded to include the assessment of cash transactions, cross-border and cross sectoral linkages and a deeper assessment of risks associated with the casino sector.
- c) Supervisors, the FIU and LEAs should exchange risk information to guide priorities and to support conduct of supervision (planning and operational levels). AMLC should feed information on covered transactions into off-site surveillance processes to enhance understanding of ML/TF financial flows across sectors.
- d) Improve market entry controls across all sectors with deficiencies, and considering extending such controls to junket operators, to ensure criminals and their associates are prohibited from ownership and management.
- e) Continue its efforts to identify illegal remittance operations (e.g. hawala) and apply proportionate and dissuasive sanctions.
- f) PAGCOR should resolve its conflict of interest in its role as casino operator and AML/CFT supervisor and should ensure casino agents are captured in the scope of its examinations
- g) SEC and CMIC should work together to find a resource efficient solution to harmonise the duplication of AML/CFT supervision.
- h) AMLC should work with other supervisors to establish more efficient referral rules to prioritise application of administrative sanctions, in order to ensure supervisory actions are proportionate and dissuasive. Further, all supervisors should also apply/continue to apply appropriate sanctions for non-compliance of AML/CFT supervisory guidelines where warranted.
- i) BSP should make more efficient use of thematic examinations to address sectoral risks arising from ML/TF abuse.
- j) Further outreach should be provided to all sectors to improve understanding, in particular of the new obligations which came into effect in 2018. The confusion caused by the scoping issue in relation to lawyers and accountants should be resolved to ensure AML/CFT compliance can be enforced.
- k) The Philippines should rectify its TC deficiencies related to supervision, including:
 - i. the scope gaps in the coverage of financing and lending companies and the lack of coverage of real estate.
 - ii. PACGOR's record keeping requirements and sanctions for financial transactions not yet covered under existing guidelines, and in relation to reliance of third parties/agents (particularly junket operators).

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

Immediate Outcome 3 (Supervision)

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

Financial Institutions

6

446. Bank licensing requirements set out in the Banking Law and regulations (MORB) include integrity and competence requirements for directors, officers and shareholders of different types of banks. There are appropriate procedures to identify beneficial owners of the banks. BSP conducts comprehensive assessments to prevent criminals and associates from owning or controlling banks including criminal background checks through NBI clearances, maintaining and screening an internal watchlist of individuals with negative backgrounds in FIs, and collecting information/intelligence from open sources and AMLC. From 2013 to 2018, 10 out of 13 applications for a banking licence were for branches of foreign banks. For these, certification from home authorities is required and BSP liaises with foreign counterparts to support BSP's assessment of fitness and propriety. From 2013-2018 BSP declined 79 directors/officers due to insufficient qualifications and/or experience. There were no instances of rejection due to criminal influence, which BSP credits to banks' initial vetting.

447. BSP conducts on-going monitoring of fit and proper covering transfers/changes of shares or re-appointment of key management. From 2015 to 2018, BSP declined or returned 46 applications for transfer of shares, mostly in rural banks. One rejection was due to inadequate provision of source of funds information. Another was due to the proposed shareholding of a PEP with a history of corruption. A further was a rejection due to a failure to provide adequate evidence of eligibility (see case study 6.1).

448. There are ambiguities relating to market entry controls to protect against criminal ownership and control of banks. The requirement relates to only a subset of crimes, being crimes of 'moral turpitude'. In practice however the scope of an NBI clearance exceeds this, recording all convictions and pending criminal proceedings, and extends to principals and suspected associates in the crimes.

Case Example 6.1: BSP's review of a proposed change of shareholding in a rural bank

In July 2018 the President of a rural bank and a representative of prospective buyers requested BSP approval to transfer 75% of the bank's shares to the buyers. BSP identified several deficiencies in the application. The buyers could not provide adequate information on corporations in which they had controlling interests, disclosure and screening of related persons at the fourth degree of consanguinity/affinity. The personal histories provided by the prospective buyers also contained inaccurate information. Further, the buyers could not prove their financial capacity to buy the shares and police clearances were not provided. BSP made the decision to deny due to those deficiencies and returned the application to the bank's President and the prospective buyer's representative three weeks after the request of share transfer.

449. SEC and IC apply some fit and proper measures, but these are less stringent than those applied to banks. Measures applied by SEC and IC to determine suitability of officers or directors include review of qualifications and experience and screening of internal watchlists⁸². Criminality is checked by IC using NBI clearances, but SEC does require such checks in all instances. If adverse information, or suspicion, is received, SEC will investigate to identify whether criminals and associates are shareholders or beneficial owners, however such checks are not utilised during market entry. Unless

⁸² The watchlists include industry practitioners with adverse information recorded, for example a history of unethical practice or violation of laws. As of November 2018, there were around 1,300 persons in the SEC watchlist and 1,477 agents in 82 organisations and 566 officers or employees on the IC watchlist.

there is a reason to suspect the persons mentioned in a GIS as shareholders are not the persons who ultimately own or control a corporation, SEC presumes the persons listed as shareholders are the beneficial owners (see IO.5 for GIS deficiencies).

450. From 2013 to 2018, SEC approved 44 licenses for investment companies, 93 financing companies (head offices) and over 2,000 licenses for lending companies (head offices). In the same time period IC approved five insurance companies. IC provided one example where an insurance licence was deferred due to a shareholder's criminal linkages (see case study below).

Case Example 6.2: IC's deferral of license due to suitability issues

In 2014 a license extension of an insurance company was deferred by IC as one of the shareholders had been involved in a case of manipulation of government funds. IC examined the company and requested supporting documents (bank statements, bank certification and/or copy of passbook) related to the shareholder's capital. The capital was not accepted by the IC because the company failed to submit supporting documents from banks. This resulted in a capital deficit and caused the insurance company to be financially ineligible for renewal of its license. The license was ultimately deferred and led to IC's appointment of a conservator to take charge of the assets, liabilities and management of the company. As of November 2018, the company was still under conservatorship.

451. BSP amended its market entry requirements for MSBs as part of the 2017 MSB re-registration process. The revised fit and proper rules require submission of NBI clearances from proposed stockholders, owners, directors and principal officers of MSBs. These persons are also screened against BSP and AMLC watchlists. Since 2017 BSP has denied 45 applicants during re-registration due to inadequate documentation.

452. The increased capital and fit and proper requirements imposed by BSP on MSBs have resulted in a consolidation of the sector. By the end of the onsite visit, only 17.3% of MSBs which operated in the market prior to the implementation of the new requirements had re-registered. The composition of the market has also changed. Notably, there are 1,667 small remittance agents (with only one office) now considered an extension of the principal registered MSB. These remittance agents are subject to the principal's AML/CFT policies.

Table 6.1: Re-registered in money service business sector

Particulars	MSB head offices prior to re-registration (31 Dec 2017)	Re-registered under Circular 942 (as of Nov 2018)	Difference
Pawnshops with remittance services	751	187	564
Other MSBs	4,679	750	3,929
Total MSBs	5,430	937	4,493
% of MSBs re-registered			17.3%

453. To identify illegal MSBs that need to register or re-register, BSP has been using a mapping process with business licensing reports of local government units (LGUs). BSP's evaluation of the first set of reports provided by LGUs in December 2017 identified 335 stand-alone MSBs with LGU business permits but not BSP registration and another 353 BSP-registered pawnshops were operating as MSBs but without specific MSB registration. In 2018, BSP issued 1,634 letters to LGUs to advise of MSBs

operating without BSP licenses. With over 1,600 LGUs⁸³ in the Philippines, the mapping of LGU and BSP records in order to identify unregistered MSBs is ongoing.

454. To further combat unregistered MSBs, both the MORB and BSP guidelines require banks to only deal with registered MSBs (see c.14.2). Banks must undertake monitoring to detect suspicious transactions of any customers or accounts being used to facilitate MSB activities. BSP advised that three banks had terminated a total of 2,291 accounts of 1,444 MSBs. The requirements on banks may inhibit the ability of unregistered MSBs to use banking facilities, however, the assessment team notes it does not assist to combat operators of illegal MVTS.

Casinos

455. PAGCOR licenses all casinos, except those which operate in special economic zones. In addition to its role as supervisor, PAGCOR owns and operates its own casinos, branded “Casino Filipinos”, which account for 19% of total casino gaming revenue. There is a conflict of interest with PAGCOR acting as both regulator and market participant, and also substantially overseeing its market competitors. All employees of PAGCOR-owned casinos are classified as public servants and are subject to Government screening processes that include criminal background checks.

456. PAGCOR utilized Personal Disclosure Statements (PDS) to assess the suitability of individuals to be directors, sole proprietors or partners. PAGCOR provided two examples demonstrating its conduct of fit and proper checks for land-based casinos (see case study). There has been one instance of the suspension of a casino licence when the casino owner was involved in a bribery case. The fit and proper checks for integrated resort casino licensees rely on the reputation of the parent companies and gaming experience of the shareholders and key management in other jurisdictions. PAGCOR does not inquire into the underlying beneficial ownership of casinos in other instances. While not required under the FATF methodology, junket operators lack of market entry requirements presents a high risk given junkets management of financial transactions with patrons. This was demonstrated by the Bangladesh Bank Heist, when junket operators acted as agents and received illicit proceeds.

Case Example 6.3: Rejection of director and licence by PAGCOR following criminal background checks

Case 1: In 2017 a hotel corporation applied for a land-based casino license. PAGCOR identified that a proposed director (who was also the Chairman of the Board) was subject to criminal charges abroad. The company removed the individual and resubmitted its proposed directors/officers. PAGCOR conducted further background checks, utilising information obtained from LEAs and INTERPOL to verify the overseas criminal history of those individuals. The license was issued to the applicant after the completion of the verification process and compliance with other requirements.

Case 2: In 2016 PAGCOR received an application for an off-shore internet casino license. Preliminary research revealed that the applicant was involved in an illegal gaming operation in the Philippines and had links to a well-known person who was wanted by LEA in a foreign country. PAGCOR sent an information request to that country and subsequently denied the application due to the applicant’s linkage with illegal gaming operations.

457. As at the time of the on-site visit, APECO had not issued any gaming licenses within the Aurora Special Economic Zone and had therefore not commenced AML/CFT supervision.

458. CEZA’s fit and proper requirements are set out in the Interactive Gaming Rules and Regulations. License applicants are subject to probity checks on finances, integrity, competence and

⁸³ As of September 30, 2018, the LGUs in the Philippines comprised of 81 provinces, 145 cities and 1,489 municipalities.

their criminal records. CEZA outsources these checks to a third party (an independent probity checker), with the results, and any adverse findings, considered by the CEZA legal department. It was not demonstrated that prevention of criminal associates is considered. There is also no indication that CEZA enquires into the underlying beneficial ownership of a casino.

459. In 2017 the number of CEZA licensees decreased from 151 to 28, in response to an Executive Order issued in February 2017 to control on-line gaming within the Philippines and restrict the proliferation of illegal gaming. As a result, CEZA revoked over a hundred licenses where the licensees had failed to transfer their operation to within the Cagayan Zone.

Lawyers and Accountants

460. Market entry for lawyers and accountants is undertaken by the Supreme Court and Professional Board of Accountancy respectively. The requirements include professional qualification exams, testimonials from existing members (for lawyers) and criminal background checks. Prior to professional qualification exams, the Supreme Court screens applicants against criminal records held, while the Professional Board of Accountancy relies on NBI clearances. The two authorities have revoked licenses in the past five years (an average of seven lawyers per year and only one case for accountants). There are cases where the Supreme Court has suspended or disqualified existing lawyers due to criminal convictions (e.g. fraud). On-going criminal checks are not undertaken by either authority; checks only commence following the receipt of a complaint filed.

Real estate agents

461. Real estate agents, although not covered persons under the AMLA, are subject to some fit and proper checks during registration. Market entry requirements include professional qualification exams and NBI clearances. Licenses are subject to renewal every two years, however there is no criminality check during license renewal unless there is a complaint file against the covered person.

Trustee services providers

462. As of 2018, over 90% of trust entities are bank affiliates and are supervised by BSP. The fit and proper rules applied to banks are also applied to the management and shareholders of trust entities. Three stand-alone trust entity licenses were issued between 2016 and 2017. There are no market entry requirements for other TCSPs.

Jewellery dealers, dealers in precious stones or metals and company service providers

463. There is no licensing framework or fit and proper checks conducted for jewellery dealers, dealers in precious stones or metals or company service providers (CSPs). AMLC undertakes some fit and proper however it was not further demonstrated that those measures have prevented criminals or their associates owning or controlling actors in those sectors. As indicated in the NRA, these businesses are fragmented and unregulated.

Supervisors' understanding and identification of ML/TF risks

Financial Institutions

464. BSP is an experienced banking sector regulator and has a good understanding of the ML/TF risk profile of individual FIs, obtained through its examinations and documented in its AML/CFT risk rating system (ARRS). Off-site surveillance also feeds into risk information at an institutional level, with

BSP collecting information on emerging risks and updating institutional risk profiles following prudential supervision. BSP also receives information from AMLC (such as condensed CTR data) which is used to inform AML/CFT risks of individual banks prior on-site examination.

465. Externally, BSP participated and received risk information from the NRA processes and NALECC meetings (see c.1.2), which provides BSP with inputs from LEAs and AMLC on predicate offence typologies to support the identification of higher risk FIs. BSP however does not have timely access to comprehensive CTRs information (due to bank secrecy) and sectoral risk information. This impedes the ability of BSP and other supervisors to effectively assess emerging risks at a sectoral level, in particular cross sector risks, cross border transactions and the abuse of cash.

466. With respect to the MSB sector, BSP maintains a wide range of information which supports its understanding of the risk profile of MSBs, mainly collected in its off-site surveillance. Since 2015, BSP has applied a network-based supervision model on the sector, requiring BSP to maintain its understanding of MSB ownership and controlling interest. This model, combined with negative intelligence collected during supervision (e.g. customer complaints and media news) and information received from other authorities such as LGUs and AMLC, inform BSP of higher risks or potential involvement to ML/TF predicate offences. In assessing materiality and geographic risks, BSP relies on the quarterly reports submitted by MSBs on their financial activities, distributions of branches/networks and CTR information obtained during examinations.

467. SEC and IC demonstrated a basic understanding of ML/TF risks, derived primarily from the NRA processes and some engagements with industry to understand sectoral risks. SEC has knowledge gaps with respect to the risks posed by smaller financing and lending companies, noting the scope deficiency in the coverage of these entities (see c.26.1).

DNFBPs

468. The NRAs identified the major risks to land-based casinos to be junkets and proxy betting. Information on the risks of other national-owned casinos was limited. The NRAs did not include an assessment of on-line casinos. PAGCOR has a reasonable understanding of the risks in the casino sector, particularly at the transaction level and has prohibited casinos from conducting specific high risk transactions. PAGCOR's understanding of risk was developed through the NRA processes and the conduct of a sector risk assessment on integrated resorts in 2018. However, in meeting with supervisory authorities, the assessment team found a lack of recognition of the vulnerabilities related to junkets role in the international movement of funds. Authorities did not demonstrate to the assessment team that supervisors have an understanding of the risks posed by offshore illegal activities facilitated from proxy betting in land-based casinos. CEZA displayed a lower level of understanding of ML/TF risk, which is still in its infancy.

469. AMLC has a reasonable understanding of the risks of the sectors it supervises (jewellery dealers, dealers in precious metals and stones, accountants, lawyers, and CSPs), due to its roles as supervisor, FIU, lead of the NRA processes, and through the conduct of meetings with industry. It is noted however that the risks associated with smaller and regional DNFBPs, especially dealers in precious metals and stones and CSPs, have not been identified and currently unknown.

470. The real estate sector is not captured as covered persons under the AMLA. The Philippines demonstrated understanding of the risks posed by the link between banks and real estate developers (e.g. large property developers are often banking group conglomerates) in the NRA however has not assessed the risk context of the secondary real estate market and transactions using cash or those which

circumvent the banking sector. In-depth analysis of the risk context of this sector would be beneficial, given the 2017 NRA indicated that properties have been subject to forfeiture from individuals charged with ML or predicate offences.

471. Most trust entities are affiliates of banks and the BSP has a reasonable understanding of ML/TF risks relating to trusts formed by trust enterprises. However, supervisors lack understanding of the risks relating to trust that are not formed by trust entities (see IO.5).

Risk-based supervision of compliance with AML/CFT requirements

Financial Institutions

472. BSP commenced AML/CFT supervision in 2007 and conducts supervision in accordance with its AML/CFT supervision manual (approved in 2013) and its ARRS (adopted in 2012).

473. Regular AML/CFT on-site examinations are conducted as part of BSP's prudential examinations of banks. Prudential examinations are required to be conducted annually, but BSP can exercise its discretion on the frequency of AML/CFT examinations, largely proportionate to the risk profile of banks. Despite this, BSP has a high coverage of AML/CFT examinations of banks in the past five years. ARRS, which provides a rating from 1 to 4, is used to inform the frequency and intensity of bank examination cycles. A bank's ARRS rating is based on various risk factors, namely adequacy of management oversight, AML/CFT internal controls, and the effectiveness of risk-based measures relating to its clients, products and services. BSP conducts less frequent on-site AML/CFT examinations (every three years) to banks with an ARRS rating of 4 (sound AML/CFT system), and less intense examinations (follow-up only) on banks with a rating of 3. Banks with lower ARRS ratings are subject to full-scope annual AML/CFT examinations or focused examinations targeting select components based on ARRS identified risks. For example, the scope of examination of rural banks is limited to customer identification and verification and reporting of covered and suspicious transactions, given their size and simple operations.

474. BSP's has 742 officers (as of November 2018) who conduct AML/CFT supervision on almost 600 banks. BSP has a specialised unit, the Financial System Integrity Department (FSID), which comprises 36 experienced staff who conduct AML/CFT supervision on the top 20 banks (all universal and commercial banks, accounting for 70% of banking sector assets) or smaller banks with significant weaknesses (e.g. a rating at 1 in ARRS). When undertaking group-wide supervision, BSP includes overseas branch offices and local branches, based on materiality. Rural banks are assessed as lower risk and only one BSP officer is assigned to their AML/CFT on-site examinations.

475. BSP utilises off-site surveillance to identify higher risk areas to be focused on during on-site examination of each bank (e.g. higher customer, product or transaction risk). In 2017, BSP commenced thematic reviews in response to specific sectoral risks and unusual transactions BSP observed in corporate bank accounts of on-line gaming business (OGBs) and MSBs. Undertaking these thematic reviews demonstrates a proactive risk-based approach. However, these reviews were embedded in regular examinations, which is not a timely and efficient use of supervisory tools when tackling specific sectoral risks.

Table 6.2: AML/CFT regular on-site examinations 2013- November 2018

	2013	2014	2015	2016	2017	2018	Total
BSP-regulated FIs							
Banks:	585	564	555	498	488	479	3,169
Universal banks (UB) and commercial banks, including foreign banks	25	29	21	26	25	25	151
Thrift banks	56	57	62	58	39	44	316
Rural and cooperative banks	504	478	472	414	424	410	2,702
<i>Among which conducted by FSID (for large/higher risk FIs):</i>	55	69	52	55	50	60	341
Universal banks and commercial banks, including foreign banks, and overseas branches of UB	25	29	21	26	25	25	151
Thrift banks	21	28	21	19	16	18	123
Rural and cooperative banks	9	12	10	10	9	17	67
Pawnshops and MSBs	366	392	154	180	101	74	1,267
<i>Among which conducted by FSID</i>	1	1	10	15	1	2	30
Bank subsidiaries & affiliates (non-bank FIs)	23	32	32	32	23	25	167
<i>Among which conducted by FSID</i>	15	23	9	1	9	4	61
NSSLAs (Non-bank FIs)	40	39	38	39	35	28	219
<i>Among which conducted by FSID</i>	1	2	3	-	1	1	8
Securities sector							
Securities brokers				132*	132*	132	396
Investment houses and underwriters of securities	-	-	-	-	-	11	11
Investment company advisor and mutual fund distributors	-	-	-	15	17	11	43
Insurance companies	54	84	65	109	40	42	394
DNFBPs							
Casinos (PAGCOR-regulated)	-	-	-	-	-	1	1
Trust entities	23	31	26	29	32	27	168
Examinations conducted by FSID	22	30	26	29	31	27	165

* Conducted by CMIC on behalf of SEC.

476. BSP also conducts special examination and overseeing examinations. These are remedial supervisory tools requiring approval by management. Between 2013 and November 2018 BSP conducted three special examinations (two in 2013 on a total of 45 banks and one in 2016 on five banks related to the Bangladesh Bank Heist) to resolve significant control weaknesses of banks. Two overseeing examinations were conducted in 2016-2018 to review the progress of action plan items for banks where significant deficiencies were identified in previous regular examinations.

477. BSP applies a risk-based approach to prioritise its supervision of non-bank sectors. This is based on the FI's risk profile (size, complexity of operations, customer profile and delivery channels) and off-site surveillance (e.g. major business/operational developments) to determine the frequency and focus of examination. BSP showed examples of prioritising NBFIs with risk exposures to PEPs. Examination of higher risk NBFIs are conducted by FSID.

478. BSPs on-site examination framework applied to banks is also applied to the MSB sector. In 2015 BSP commenced on-site examination of stand-alone MSBs. Prior to this, only MSBs linked with pawnshop businesses were regulated and examined. BSP implemented a network based supervision approach in 2015 which groups MSBs by networks (head office, branch offices and those systematically linked are counted as one registered MSB). This has improved the efficiency supervision.

479. BSP utilises a broad range of off-site surveillance information to prioritise its on-site supervision to cover large MSBs with wide network or branches, those with material transactions and those previously identified with illicit proceeds. This approach also seeks to address the resource challenges in covering over 5,000 MSBs with 280 examinations on MSBs conducted by BSP between 2016 and 2017. On-site examination conducted on MSBs are full-scope, with checks of specific MSB obligations. For example BSP Circular 942 in 2017 prohibited transactions exceeding P500,000 to be paid in cash in order to impede the abuse of cash without audit trails.

480. AML/CFT supervision of the securities sector is carried out by SEC and a SRO, the Capital Market Integrity Corporation (CMIC). CMIC's on-site examination program commenced in 2014 and covers SEC-regulated security brokers and dealers. CMIC's on-site AML/CFT examinations are embedded in its prudential examinations. CMIC applies a rule-based approach and only covers basic AML/CFT elements. CMIC shares its inspection findings with SEC, however SEC has not used these reports for any purpose.

481. SEC has not commenced a risk-based approach to supervision, despite the establishment of an AML Unit and a risk-based on-site examination manual in 2018. SEC conducted its first round of on-site examinations between May and October 2018 covering all securities broker dealers, investment houses and investment companies. The examinations predominately focused on legal compliance with key obligations. It is noted that CMIC is still conducting its AML/CFT compliance checks on broker dealers which is a duplication. SEC has not yet engaged financing and lending companies for AML/CFT supervision. The 2017 NRA included financing companies in an assessment of financial inclusion (micro financing), however this finding has not been utilised to apply simplified measures. As noted in c.26.1 there is a scope deficiency in the coverage of financing and lending companies.

482. AML/CFT supervision was conducted by IC as part of prudential supervision until a dedicated AML Division was established in 2015. In 2017 IC moved to a risk-based approach to AML/CFT supervision and began conducting thematic examinations focused on insurance products with investment elements. This focus is in response to the 2017 NRA finding that such procedures posed a high level of ML/TF risk, rather than a supervisory risk assessment. Insurance is a lower risk sector among FIs and is dominated by foreign insurance groups. There is a need to focus more on group supervision to enhance effectiveness. This will require the IC to extend its ability to cooperate with foreign counterparts (see c.40.12).

DNFBPs

483. Non-casino DNFBPs, including jewellery dealers, dealers of precious stones and metals, lawyers, accountants and CSPs (except trust entities supervised by BSP) have been included as covered persons under the AMLA since 2013. However, AMLC's AML/CFT supervision of DNFBPs only

commenced with the issuance of the DNFBS AML/CFT Guidelines in May 2018. AMLC has prepared an AML/CFT supervision manual and on-site supervisions commenced in mid-2018, with the examination of one casino in conjunction with PAGCOR. No further examinations had been conducted as at the time of the on-site.

6 484. The PAGCOR/AMLC joint inspection, conducted in July 2018, was targeted at a higher-risk, large integrated resort casino. The scope of examination focussed on validating AML/CFT policies and procedures. As at the time of the onsite PAGCOR and AMLC had issued the report and were waiting for a remedial action plan from the casino. PAGCOR is in the process of establishing a risk-based supervisory model based on its first examination and its recent first sectoral risk assessment. CEZA has not conducted any AML/CFT supervisory activity.

485. It was not evident that the inspection of the casino included examination of the casino's agents, noting that the Philippines claims that junket operators conduct CDD on behalf of casinos as casino agents. Supervision of casinos should include coverage of their agents, which is particularly important noting the high risk of junket operators.

486. BSP applies a risk-based approach to the supervision of trust entities, as per its approach to NBFIs. This is based on size, complexity of operations, customer profile and delivery channels. As most trust entity licensees are part of universal and commercial banks, most of the onsite examination are conducted by FSID as part of AML/CFT examination of the bank. BSP also extend the same on-site examination model to stand-alone trust entities.

Remedial actions and effective, proportionate, and dissuasive sanctions

Financial Institutions

487. AMLC is the primary authority for the imposition of administrative sanctions for non-compliance with the AMLA. Supervisors are also able to apply their own powers to sanction non-compliance with their respective AML/CFT guidelines/regulations. AMLC relies on MOAs with the three FIs supervisors and reviews examination reports submitted by them to determine sanctions. From 2013 to 2017, BSP sent 2,494 examination reports to AMLC. AMLC took action on only 33 of those reports and the sanctions applied were not dissuasive or proportionate, with only one fine penalty applied. AMLC issued new rules of sanctions to improve the process and imposed a penalty fine of PHP6.75 million (approx. USD 128,587) on a bank for a delayed reporting of 30 CTRs in 2018. While the implementation of the new process is positive, it requires supervisors to submit all examination reports to AMLC for review, which is misaligned with AMLC's available resources. A more effective sanctioning referral mechanism is required to effectively apply sanctions stemming from supervisors examinations.

488. BSP has made use of different supervisory actions to improve AML/CFT compliance in the banking sector. A total of PHP1.021 billion was imposed in penalties by BSP for serious AML violations, with a PHP1 billion (approx. USD 19 million) fine imposed on the bank which handled the illicit funds in the Bangladesh Bank Heist case in 2016, after a special examination was conducted. Other than these severe cases, remedial action is the most common supervisory action taken by BSP, which are applied proportionately to the ARRS rating resulting from an onsite examination. The severity of the corrective actions is aligned with the level of commitment expected from BSP, i.e. more serious deficiencies require board commitment to rectify. Warnings, monetary penalties and restrictions on the scope of operations have been applied to those banks which made minimal progress, or to those with significant deficiencies (e.g. absence of effective customer profiling mechanism).

489. BSP has imposed prudential sanctions on MSBs, with six MSB licenses revoked (in 2016 and 2018). Three of the revocations related to the Bangladesh Bank Heist case, and the other three were as a result of serious AML/CFT non-compliance. Remedial actions are the most common supervisory action imposed on MSBs since the risk-based on-site examination model was implemented in 2015. BSP has not applied any sanctions on unregistered MSB operations. However, it has advised LGUs to terminate, or not issue, local business licenses to MSB that have not re-registered with BSP. There is a notable disparity between the administrative sanction and the criminal sanction available to BSP to sanction illegal MSB operations, with the administrative sanction (penalty fine of PHP200,000, approx. USD 3,800) not dissuasive. More proactive measures should be undertaken to sanctions illegal MSBs.

490. IC has used its prudential powers to take supervisory actions for AML/CFT non-compliance. Between 2015 and 2018 it imposed 11 fine penalties, and three examination reports were referred to AMLC for further action (all in 2018).

491. No sanctions related to AML/CFT violations have been issued by SEC. A number of deficiencies were identified in the SEC's first round of AML/CFT examinations. SEC advised that it will conduct a second round of examinations in 2019 before considering what supervisory action should be taken for AML/CFT non-compliance.

Table 6.3: AML/CFT supervisory actions applied in regular on-site examinations

	2013	2014	2015	2016	2017	2018	Total
BSP-regulated FIs							
Banks - Universal banks and commercial banks:							
Request for remedial actions	22	23	22	33	29	15	144
Written warnings	-	3	-	4	2	1	10
Restrictive actions/operations	-	1	-	2	2	2	7
Monetary penalties	11	1	1	3	2	2	20
Banks - Thrift banks:							
Request for remedial actions	36	41	46	45	47	24	239
Written warnings	1	7	7	2	3	-	20
Restrictive actions/operations	-	-	1	1	1	-	3
Monetary penalties	2	2	1	-	2	-	7
Banks - Rural banks:							
Request for remedial actions	462	457	460	400	407	398	2,584
Written warnings	-	-	-	-	-	-	-
Restrictive actions/operations	-	-	-	-	-	-	-
Monetary penalties	-	-	-	-	1	-	1
MSBs (including pawnshops with remittance services):							
Request for remedial actions	-	1	61	66	86	72	286
Written warning	-	-	-	-	-	-	-
Restrictive actions/operations	-	-	-	-	1	-	1
Monetary penalties	-	-	-	-	-	-	-
Revocation of licenses	-	-	-	3	-	3	6
NSSLAs:							
Request for remedial actions	40	39	38	39	35	28	219
Insurance sector							

Request for remedial actions	17	3	12	8	23	2	65
Written warnings	-	-	1	-	8	1	10
Restrictive actions/operations	-	-	-	-	-	-	-
Monetary penalties	-	-	5	4	1	1	11
Revocation of licenses	-	-	-	-	-	-	-
DNFBPs - trust entities (BSP-regulated)							
Request for remedial actions	-	1	1	-	2	3	7

DNFBPs

492. No sanctions have been imposed on DNFBPs for AML/CFT non-compliance. AML/CFT supervision of DNFBPs (other than trust entities supervised by BSP) only commenced in mid-2018.

Impact of supervisory actions on compliance

493. The high volume of BSP's supervisory activity over past five years has positively impacted the AML/CFT compliance of banks. BSP demonstrated that ARRS ratings of 42 banks (16 universal banks and 26 thrift banks, accounting for 58% of asset size in 2017) increased between 2013 and 2018. This improvement is attributable to the BSPs on-site examination process. BSP data illustrated that 30 banks with "vulnerable" ratings (ARRS score of 2) had attained improvement to an "adequate" level (ARRS score of 3). These improvements relate to key AML/CFT measures, including the implementation of CDD, CTR and STR reporting, monitoring systems, internal audit and compliance officer competency. Banks provided positive feedback on the ARRS system and noted that it and the examination report process drove them to improve. BSP's impact on compliance to rural banks is less noticeable. Over 90% of rural banks require remedial actions in past five years.

Table 6.4: Progress of improvement of 42 banks (16 UB/KB, 26 TB) in ARRS 2013 – 2017

ARRS Composite rating improved progress	Length of time for improvement of grading				Total
	1 year	2 years	3 years	4 years	
Upgraded from 1 to 3 (twice upgrading)	-	-	2	-	2
Upgraded from 3 to 4	-	1	-	-	1
Upgraded from 2 to 3	15	7	6	2	30
Upgraded from 1 to 2	7	1	1	-	9
	22	9	9	2	42
Rating: 4 = sound; 3 = adequate sound ; 2: vulnerable ; 1: grossly inadequate (A FIs with an overall rating of 1 or 2 are subject to prioritised supervisory actions)					

494. The re-registration process of MSBs has resulted in an improvement in compliance, notably in the increased lodgement of CTRs and STRs. This difference is attributed to the sectors' increased awareness and the implementation of enhanced monitoring processes and red flags automation. Further, one of the MSBs interviewed by the assessment team noted that the re-registration process re-structured smaller MSBs with limited resources to become remittance agents associated with larger, well-resourced MSBs, which are now supervised as one entity under centralised policies.

495. IC and SEC demonstrated limited impact on compliance, noting their sectoral guidelines were out of date until 2018. IC demonstrated it had enforced all IC-supervised covered persons to designate compliance officers following sanctions, and noted an increase in CTRs and STRs from the insurance sector. SEC's 2018 examinations identified that out of the 132 securities brokers assessed, 86 (65%) had AML/CFT policies updated in line with the 2016 RIRR and 107 (81%) did not have adequate risk-based CDD policies. The issuance of 2018 IRR and revisions on guidelines by IC and SEC in November 2018 mean that more supervisory attention is required to enhance compliance in these sectors.

496. Integrated resort casinos (the highest risk sector) have taken some steps towards compliance, however this has not formally been assessed. Following explanatory meetings, NRA involvement and the consultation process on the AML/CFT guideline, most of the integrated resort casinos have submitted copies of their AML/CFT programmes to PAGCOR, and all have registered with AMLC for reporting CTRs and STRs. As at the end of on-site visit, AMLC had received 2,016 CTRs and 375 STRs from the casino sector, within a few months of their registration. However, this impact on compliance has not yet reached the smaller market participants, including PAGCOR-owned casinos and CEZA on-line casinos.

497. Trust entities have enhanced their compliance culture and AML/CFT policies and have been submitting CTRs/STRs since the commencement of BSP's full-scope examinations in 2017. Limited impact of supervisory actions on compliance was demonstrated for other DNFBPs. Onsite examinations have not yet commenced on other DNFBPs, so their level of compliance is unknown.

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

498. BSP has a comprehensive program designed to enhance FI's understanding of their obligations and risks, including on-going capacity building and issuance of circulars on AML/CFT obligations. Between 2013 and 2017, BSP delivered over 120 seminars/training sessions to bank associations, officers and/or employees, promoting their AML/CFT obligations. BSP and AMLC work together with various industry associations to clarify, formulate and revise the AML/CFT rules and regulations. BSPs on-site examination process is another mechanism used by BSP to communicate with covered persons, with exit meetings and examination reports used to enhance understanding of AML/CFT obligations.

499. BSP conducted 151 seminars for MSBs between 2013 and 2017, which were attended by over 18,000 participants. Mutual dialogue is conducted between BSP and MSBs, for example during the consultation process for the BSP Guideline in relation to the restructuring of the sector.

500. IC provides regular AML/CFT training for its regulated sector. From 2014 to 2017 it conducted seven AML/CFT workshops. IC's increased focus on AML/CFT on-site examinations and enforcement actions since 2017 have also improved understanding within the sector.

501. SEC has conducted limited outreach on AML/CFT to its sector, with 25 seminars for broker dealers conducted between 2014 and 2018. These seminars focused on AMLA requirements, STR reporting and risk profiling.

502. PAGCOR has delivered outreach program in the last two years on the new AML/CFT guidelines for casinos. BSP has held meetings with the industry association for trust entities on the updated AML/CFT requirements. Gaps in the legal requirements in the AMLA and supervisory guidelines have impacted the development of a clear understanding by affected sectors. For example, casinos are a lack of clarity on the requirement for all financial transactions in casinos to be subject to AML/CFT monitoring. AMLC delivered a sizeable outreach program to DNFBPs to promote the implementation of AML/CFT requirements, however only 19 DNFBPs (mostly casinos) out of 93 that received outreach

have registered with AMLC as of the onsite (see Table in IO.4). Further outreach is required to enhance the understanding of legal professionals (given the scope deficiencies in R.22) and the recently issued 2018 IRR. CEZA has not conducted any outreach, however issued its first guidance paper (for on-line casinos) in November 2018.

Overall conclusions on Immediate Outcome 3

6

503. Supervisors of large and higher risk sectors demonstrated a reasonable level understanding of risks, however lack some information to enhance their understanding of sectoral risks. BSP demonstrated that it is preventing criminal influence to a large extent, notably for banks, however other supervisors do not consistently apply market entry for shareholders and beneficial owners. BSP's restructure of the MSB sector in 2017 identified unregistered MSBs, however no sanctions have been applied for illegal operations. The lack of coverage of all financial transactions conducted by casinos is a deficiency in the AML/CFT supervision of casinos related to junket-to-player transactions. There is an operational independence issue with PAGCOR given its dual role as supervisor and market participant.

504. BSP has a prudent framework for risk-based supervision, however thematic reviews were only recently implemented and are not effectively utilised. Risk-based supervision frameworks for other supervisors are in their infancy. BSP has applied dissuasive sanctions to large banks and MSBs. The process for AMLC to deal with sanctions of non-compliance referred by FI supervisions requires enhancement in light of resourcing challenges. Outreach has been conducted to most sectors, however further is require to improve the understanding of specific sectors.

505. **The Philippines has a moderate level of effectiveness with Immediate Outcome 3.**

CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS

*Key Findings and Recommended Actions***Key Findings**

- 1) The Philippines has not undertaken a ML/TF risk assessment of the different types of legal persons that can be created within the country. Public and private sectors have a limited understanding of those risks as well as the risks associated with legal arrangements.
- 2) The Philippines primary measures to prevent the misuse of legal persons and arrangement are the public access to information on legal persons as contained within the GIS, the Articles of Partnership, and CDD documents; regulation and supervision of trustee entities by the BSP; and measures to prevent the misuse of bearer shares.
- 3) Trustees to private trusts, charitable trusts or foreign trusts are not subject to transparency obligations, however CDD conducted by an FI or DNFBP on those trustees would capture beneficial ownership and control information which would be available to competent authorities.
- 4) Business trusts are formed by trust entities which are covered persons under the AMLA, and are supervised by the BSP.
- 5) The Philippines relies on the use of CDD information obtained by FIs and DNFBPs to obtain information on legal persons and arrangements. Bank secrecy laws affect the timely access to this information, when held by banks, by competent authorities other than AMLC.
- 6) The sanctions imposed by competent authorities on legal persons for failure to comply with information requirements include the suspension or revocation of the certificate of incorporation and fines. However, suspension and revocation only occur after an extended period of non-compliance (five years or more). Fines in the interim five year period are not effective, proportionate or dissuasive.

Recommended Actions

- a) Undertake a comprehensive ML/TF risk assessment of all types of legal persons operating in the Philippines, including characteristics of particular types of legal person or arrangement, or features of their establishment or ongoing management and control that would contribute to or mitigate ML/TF risk followed by targeted awareness raising of the ML/TF vulnerabilities posed by legal persons and arrangements.
- b) Introduce measures to ensure bearer share warrants, nominee directors and nominee shareholders are not misused for ML/TF in line with the FATF requirements.
- c) Ensure certain competent authorities seek expedient access to bank records (with appropriate integrity controls) and that mechanisms operate to ensure that information on the beneficial ownership of a company can be determined in a timely manner
- d) Following the release of the Guideline on Beneficial Ownership, conduct outreach to competent authorities, financial institutions and other covered persons on beneficial owner requirements.

506. 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 and R.25.

Immediate Outcome 5 (Legal Persons and Arrangements)

7

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

507. Information on the creation and types of legal persons in the Philippines is available from SEC (for corporations and partnerships) and CDA (for cooperatives). There is however limited information available to the public on the creation and types of trust arrangements in the Philippines. While the Civil Code (the framework within which trusts may be settled) is publically available there is no information on the various types of trusts that may be settled within that legal framework.

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

508. As mentioned in Chapter 1, as at 31 December 2017 there were 634,109 registered domestic legal persons in the Philippines and 4,319 registered foreign legal persons. In addition, according to the CDA there were 17, 866 registered cooperatives.

509. No ML and TF risk assessment has been undertaken on the types of legal persons that can be created in the Philippines. Assessments of risk did not identify the characteristics of particular types of legal person or arrangement, or features of their establishment or ongoing management and control, that would contribute to or mitigate ML/TF risk. There is a limited understanding of the risk of ML/TF with respect to those legal persons across a broad range of agencies and entities within the public and private sectors. The SEC (company registrar) acknowledged the ease with which companies can be established in the Philippines and provided several case studies to the assessment team identifying misuse and SEC action taken. However, the SEC lacked a depth of ML and TF risk understanding.

510. A case of graft and corruption involving the PDAF funding stream to NGOs was repeatedly mentioned as the only instance where abuse had taken place as far as most agencies were aware (see IO.8 for relevant case study). However, that example did not appear to lead to a broader understanding of the potential for misuse of legal persons, particularly within LEAs.

Mitigating measures to prevent the misuse of legal persons and arrangements

511. The Philippines' primary measures to prevent misuse of legal persons and arrangements are as follows: a) access to information on legal persons in the General Information Sheet (GIS); b) regulation and supervision of trustee entities by the BSP; and c) prohibition on bearer shares.

512. The GIS is required to be submitted by all corporations (including foreign corporations) and cooperatives on an ongoing annual basis. The GIS must be resubmitted within seven days of any changes to the information contained within it. However, the GIS contains only basic information on corporations, including shareholder and director information, which is also publicly available; it does not contain beneficial ownership information. The information contained within the GIS is not routinely verified by the SEC, with authorities instead relying on the GIS being submitted under oath.

513. Trustee entities (for business trusts) must be authorised by the Monetary Board before they can provide trust services. The BSP is responsible for the regulation and supervision of trustee entities

(and therefore business trusts), and conducts onsite and offsite supervision. However, as noted in R.25, neither BSP nor any other agency supervises directly or indirectly private trust arrangements including foreign trust arrangements. Philippines authorities could not provide an estimation of the number of total number of trust arrangements in the Philippines. Neither could the tax authority provide an indication of the number of trusts in the Philippines that file tax returns.

514. While bearer shares cannot be issued in the Philippines, bearer share warrants can be issued and there are no measures in place to address the risk posed by those instruments. Neither are there any arrangements in place to address the risks posed by nominee directors or nominee shareholders. Notably, the use of nominee shareholders is common in the Philippines in order to circumvent the incorporation requirement of five incorporators. Authorities are aware of the use of nominee shareholders for this purpose.

515. In conclusion, there are few measures in place to mitigate the risks associated with legal persons and trusts (apart from business trusts) in the Philippines.

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

Basic Information

516. As discussed in the TC annex, access to basic information on corporations and partnerships is available from the SEC.

517. Some basic information is updated yearly in the GIS, while the Articles of Incorporation must be resubmitted following any changes. This information is available publicly through several means, including an online database that can be accessed for a fee and through direct requests to SEC. However the SEC online database is able to provide information only for documents filed between 1998 and 2016. Documentation prior to this time period is still available, however in microfilm rolls. Requests for these documents can be made but take longer to produce.

518. Competent authorities appear to mostly use SEC's database to confirm if a company is registered or not. The preferred method of obtaining basic information is through a formal request to the SEC or subpoena as the documents obtained through the online database have no evidentiary value. Information contained in the database was not regularly utilised for investigations. Formal requests for information take approximately five business days to complete when a record is required for evidence in court.

519. The CDA maintains a publicly available list of all registered cooperatives. Authorities did not demonstrate to the assessment team that basic information contained in registration documents (Articles of Cooperation and by-laws) are publicly available or available upon request by competent authorities, except under a freedom of information request.

520. If the trustee of the legal arrangement has engaged a broker dealer in the stock market, the SEC is able to access information through the records maintained by the broker dealer. However, it is not clear that competent authorities are aware of this source of information, particularly as the SEC is not otherwise involved in the supervision or regulation of legal arrangements.

Beneficial ownership information

7 521. Competent authorities have access to CDD BO information on legal persons from FIs and covered persons in keeping with the AMLA and IRRs. Due to banking secrecy laws, competent authorities, other than AMLC and the BSP (as regulator of authorised trustee entities), are not able to seek this information directly from FIs. This inhibits competent authorities' timely access to both basic and beneficial information as AMLC needs to request information from the financial institution (if not already contained in the database)), while the BSP is unable to share information it holds without the prior approval of the Monetary Board. AMLC estimated that accessing and releasing this information takes approximately five business days.

522. The Philippines did not demonstrate that LEAs request access to beneficial ownership information. During discussions with competent authorities, the banking secrecy law and the steps needed to obtain account information were raised as hindering investigations.

523. The SEC can obtain beneficial ownership information on legal persons that hold accounts in the Philippines stock market. In order to open an account a Customer Account Information Form (CAIF) must be completed. Broker dealers are required to maintain these forms and ensure they are current and accurate. The basic and beneficial ownership information of clients must be maintained by each broker dealer in an electronic database and made available to the SEC when requested. The SEC advised it has utilised this method of obtaining beneficial ownership information for its own investigations into securities offences as well as at the request of other competent authorities.

524. Competent authorities are able to request beneficial ownership information in relation to regulated trustee entities from AMLC. However, AMLC has not received any requests to date. Generally, the number of requests for beneficial ownership information among competent authorities has been low. Authorised trustee entities have information requirements under s.X806.2.a(3) of the MORB, whereby the trustee must obtain specific information including the names of the settlor, trustee, trustor, protector, beneficiaries and any other natural person exercising ultimate control over the legal arrangement.

525. As supervisor, BSP assesses compliance with this information requirement on authorised trustee entities during onsite examinations. However, BSP is prohibited under legislation from releasing information to other competent authorities unless approval has been obtained from the Monetary Board. The assessment team was made aware of the time frame such a request would involve through a request made by the OMB, in May 2018, for both basic and beneficial ownership information on a financial institution. It took three months for the BSP to evaluate the request and retrieve the requested information prior to taking the request to the Monetary Board. Although Monetary Board approval only took one week, OMB did not receive the requested information until 24 August 2018, almost four months after the request was submitted. It is not clear whether the OMB was aware that the information could also be accessed through AMLC.

526. Trustees of private trusts (charitable, foreign trusts or otherwise) operate without any requirements to collect beneficial ownership and control information. AMLC and other LEAs can obtain beneficial ownership information from FI/DNFBPs that may have trustees of private trusts as customers. Competent authorities did not demonstrate that they have sought information on legal arrangements other than those formed by trust entities (business trusts).

527. The assessment team noted some cases of confusion in the private and public sectors regarding mechanisms to obtain information on beneficial ownership, with some stakeholders apparently confusing legal ownership and beneficial ownership and control. The assessment team had

some concerns about the accuracy of beneficial ownership collected by covered persons in particular, as there appears to be an over-reliance on the legal ownership information contained within the GIS.⁸⁴ Some covered persons demonstrated a good understanding of beneficial ownership and the complexities involved, and including work undertaken by them to understand the multiple layers of ownership involved in ascertaining ultimate beneficial ownership.

528. To address the concerns AMLC issued AMLC Regulatory Issuance A, B, and C No. 3 Series of 2018 – Guideline on Identifying Beneficial Ownership on 27 November 2018. The purpose of the guideline is to assist FIs and DFNBPs to identify the ultimate beneficial owner of clients. This is the first guideline issued in the Philippines on beneficial ownership. However the assessment team was unable to assess its impact given that it was issued just prior to the end of on-site visit.

Effectiveness, proportionality and dissuasiveness of sanctions

529. Sanctions for non-compliance with information requirements, including annual reporting and information updates, consist of administrative penalties under the SRC and Corporation Code (for corporations and partnerships) and the MORB for regulated legal arrangements. Trustee entities (as regulated) are also subject to sanctions under that Act for identification, verification and record-keeping obligations.

530. Failure to submit the GIS for legal persons to the SEC can result in varying degrees of actions, culminating in suspension of registration. Table 37 shows the number of corporations that have had their registration revoked or suspended between 2015 and September 2018.

Table 7.1: Number of registrations revoked or suspended for failure to meet annual reporting requirements

	2015	2016	2017	2018 (as at September)
Domestic non-stock	9,884	9,370	5,896	18,775
Domestic stock	10,552	7,174	4,949	17,365
Foreign non-stock	10	8	-	8
Foreign stock	55	29	23	57
Total	20,471	16,581	10,868	36,205

531. Under the SRC, the SEC may impose suspension or revocation of any registration for the offering of securities; fines of between PHP10,000 (approx. USD 190) and PHP1,000,000 (approx. USD 19,000) with an additional PHP2,000 (approx. USD 38) for each day of continuing violation; suspension or revocation of the Certificate of Incorporation; and other penalties within the power of the Commission to impose. Under s.54.1, these sanctions are available for any violation of the code, and also in the case of providing false information or omitting a material fact in required reports. This then leads to the sanctions for violations of the Corporation Code. Under s.144, violation of the Code, including of information requirements, incurs penalties which include fines of between PHP1,000 (approx. USD 19) and PHP10,000 (approx. USD 190), imprisonment for 30 days to five years and dissolution of the corporation.

⁸⁴ During the onsite visit, the Philippines amended the GIS to require submission, within 30 days of the corporation's annual meeting, of beneficial ownership information for all domestic legal persons. However these amendments did not come into force until 1 January 2019, one month after the onsite.

532. Although Table 37 shows a large number of suspensions and revocations, it is not clear whether this action was only taken after sustained failure to meet reporting requirements. Philippines authorities only take significant action against corporations after at least five consecutive years of failing to submit annual report, including the GIS. During the onsite, the SEC advised that they have a variety of sanctions, on an increasing scale, which they can take against corporations for failing to meet reporting requirements, however monitoring reports did not demonstrate this. SEC monitoring reports provided to the assessment team showed minor fines for failure to submit the GIS. In one case, a corporation failed to submit a GIS in 2013-2015. On each occasion the corporation was fined PHP 2,500 (approx. USD 48). The fines handed out each year did not increase, rather the SEC applied a further penalty of 10% of the total fines handed out over the six year period (2013-2018) for repeated violations. This further penalty amounted to PHP 2,000 (USD 38) for six years of either failing to file or late filing of the GIS as well as financial statements. Other corporations were subject to fines of between PHP 7,000 and 10,000 for failure to submit the GIS (approx. USD 133 and USD 190). Other fines handed out included for corporations that failed to file a petition to substitute the corporation's resident agent. These fines were between PHP 7000 and 30,000 (approx. USD 133 and 572).

Table 7.2: Scale of fines for non-submission of GIS (and financial reports)

Income of corporation	Penalties for domestic and foreign stock corporations	Penalties for domestic and foreign non-stock corporations
PHP 0 - 100,000 (USD 1905)	PHP 1,000 (USD 19)	PHP 500 (USD 10)
PHP 100,001 – 500,000 (USD 1,905 – 9,525)	PHP 3,000 (USD 57)	PHP 1,500 (USD 29)
PHP 500,001 – 5,000,000 (USD 9,525 – 96,250)	PHP 5,000 (USD 95)	PHP 2,500 (USD 48)
PHP 5,000,001 – 10,000,000 (USD 96,250 – 195,500)	PHP 7,000 (USD 133)	PHP 3,500 (USD 67)
Above PHP 10,000,000 (USD 195,500)	PHP 10,000 (USD 191)	PHP 5,000 (USD 95)

533. In addition to the monitoring sheets, the SEC provided statistics on fines issued over the period 2015 to 2018 (Table 38). However, these figures are for violations of any laws and rules and regulations of the SEC, not just for failure to meet reporting obligations relevant to AML/CFT. It is unclear how many fines have actually been issued for non-submission of required reports, outside of the four relevant monitoring reports provided to the team. Based on these reports, the actual fines imposed are not dissuasive and proportionate. The repeated failure to submit, or late submission, without a proportionate increase in penalty demonstrates that the fines imposed are not dissuasive.

Table 7.3: Fines imposed by the SEC on legal persons

Year	2015	2016	2017	2018 (as at September)
Legal persons	12,839	11,101	18,411	9,740
Average fine per legal person	USD 158	USD 200	USD 122	USD 151
Total fines	PHP106,819,781 (USD2,034,917)	PHP116,599,281 (USD2,221,216)	PHP117,873,637 (USD2,245,492)	PHP77,487,841 (USD1,476,143)

534. The assessment team was also provided with cases where Certificates of Incorporation have been suspended or revoked, mostly for continued failure to submit required reports over at least a five-

year period, and in instances where a number of the corporations had already ceased to continue operations. This sanctioning activity is not assessed as proportionate or dissuasive.

535. BSP can impose written reprimands, restriction on certain licenses, suspension and disqualification under Part 8 of the MORB. However, there is a significant gap in the regulation of trustees in private, charitable and foreign trusts.

536. The BSP can also impose monetary penalties, in coordination with AMLC, for violation of CDD requirements. Record-keeping obligations are left to the discretion of AMLC.

537. The authorities have not applied any sanctions against trustees of private trusts and BSP has not sanctioned any covered trustee entities in relation to information requirements placed on covered trustee entities. Instead, the BSP has issued directives to FIs who fail to perform the appropriate CDD on trustors and the beneficial owners of a trust. This is in the context that majority of trustee entities are managed or owned by financial institutions.

Overall conclusion on Immediate Outcome 5

538. Across the public and private sectors there is a low level of understanding of ML and TF risks relating to legal persons and arrangements. Moreover there is a low level of compliance among competent authorities to collect or enforce the collection of beneficial ownership information. Sanctions are not dissuasive and proportionate, and there is a lack of sanctions being applied.

539. **The Philippines has a low level of effectiveness for Immediate Outcome 5.**

CHAPTER 8. INTERNATIONAL COOPERATION

*Key Findings and Recommended Actions***Key Findings**

- 1) The Philippines has a reasonable legal framework for seeking and responding to MLA and extradition, and assessments of risk have considered transnational risks, however the framework has not been fully applied to respond to the transnational risk profile.
- 2) While AMLC and BSP proactively pursue international cooperation, however other competent authorities, and LEAs, in particular, do not proactively pursue international cooperation in keeping with the ML/TF risk profile.
- 3) The level and of outgoing requests for MLA and extradition is low compared to incoming requests and the risk profile overall. Timeliness of responding to requests remains a concern with respect to MLA and extradition requests to the Philippines.
- 4) LEAs utilise informal international cooperation rather than MLA and extradition mechanisms, in part due to the delays associated with these mechanisms.
- 5) The Philippines takes advantage of a wide range of mechanisms including regular bilateral or multi-jurisdictional operation meetings, international organisations and officer level contacts.
- 6) Counterparts noted that the Philippines usually provides constructive international cooperation with respect to exchange of financial information. AML/CFT supervisors cooperate with foreign counterparts when conducting fit and proper assessments and on the conduct and results of AML/CFT supervision efforts.
- 7) The volume of outgoing international cooperation requests related to AML/CFT issues, especially outgoing requests are low in the context of the Philippines. The strength of the Philippines informal networks is a positive, but is used largely in response to requests from other jurisdiction, and/or in relation to predicate offences.
- 8) Foreign partners can access basic information on legal persons through the GIS database. Sharing basic and beneficial ownership information with foreign partners has been limited to AMLC.

Recommended Actions

- a) Enhance the capability of LEAs to identify and investigate transnational elements of cases with the cooperation of relevant counterparts, including by actively seeking MLA and extradition in their ML, TF and predicate offences investigations in keeping with the trans-national risk profile.
- b) Consider at a joint agency and agency level, the priority jurisdictions for international cooperation based on findings of risk assessments.
- c) Based on this process develop a priority international cooperation plan to guide FIU, LEAs, supervisors and others in their proactive international cooperation.

- d) Implement an improved and better resourced case management system in the DOJ central authority, supported by enhanced inter-agency cooperation on MLA, to better manage the Central Authority's workload of incoming requests
- e) Further enhance supervisors' regular engagement in international cooperation for AML/CFT including risk sharing, fit and proper checking and the conduct and results of supervision.
- f) Enhance support mechanisms and joint agency cooperation to reduce delays with international cooperation. This should include monitoring the timeliness of responding to requests as part of the Philippines' broader efforts to reduce delays.
- g) Adopt a more proactive approach and better utilise existing arrangements to seek informal international cooperation, and not only to respond to requests from foreign counterparts.
- h) Create better awareness amongst competent authorities and international counterparts on the mechanisms to access basic and beneficial ownership information.

540. The relevant Immediate Outcome considered and assessed in this chapter is IO2. The recommendations relevant for the assessment of effectiveness under this section are R.36-40.

Immediate Outcome 2 (International Cooperation)

Providing constructive and timely MLA and extradition

541. The Philippines has a reasonable legal framework for responding to MLA and extradition. MLA is available through MLATs, under various international conventions or diplomatically through the principle of reciprocity.

542. Risk assessments have consideration of many of the geographic and trans-national risks, but there are a number of gaps and the assessments only form a partial basis to inform priorities for international cooperation. AMLC and BSP prioritise their international cooperation, taking into account risks, but implementation of national and agency level policies, particularly amongst criminal justice agencies, does not sufficiently focus on priority threats and shared risks with foreign counterparts.

543. All MLA requests are handled by the DOJ, as the Philippines central authority on all MLA matters. Requests for assistance made on the basis of reciprocity are submitted through diplomatic channels and then transmitted to the DOJ. The DOJ has a manual case management system, and takes responsibility for prioritisation and timely response. As required under the 2018 IRR, AMLC has a supplementary system for tracking MLA requests. AMLC utilises an electronic document management system for monitoring MLA cases on a per request basis, and an excel spreadsheet for macro-level monitoring of all MLA requests.

544. In the period 2013-2018, the Philippines received 299 MLA requests, 43 of which are related to ML (14%), but none related to TF. The relatively high numbers of incoming ML requests reflects the strong informal international cooperation on AML/CFT pursued by AMLC. Authorities have been supporting agency to agency international cooperation on TF-related matters, but none of these have been reported as involving incoming MLA requests.

545. Fraud-related offences accounted for 101 (33%) of all incoming MLA requests. The next most common categories of MLA requests received by the Philippines were 47 related to child

pornography/sexual abuse/exploitation of children (16%), 46 related to murder (15%), 14 related to drug trafficking (5%) and 13 related to corruption/embezzlement (4%). The figures for fraud reflect the risks, but other high risk crime types receive very few requests. The number of murder cases involving profit or payment is not clear.

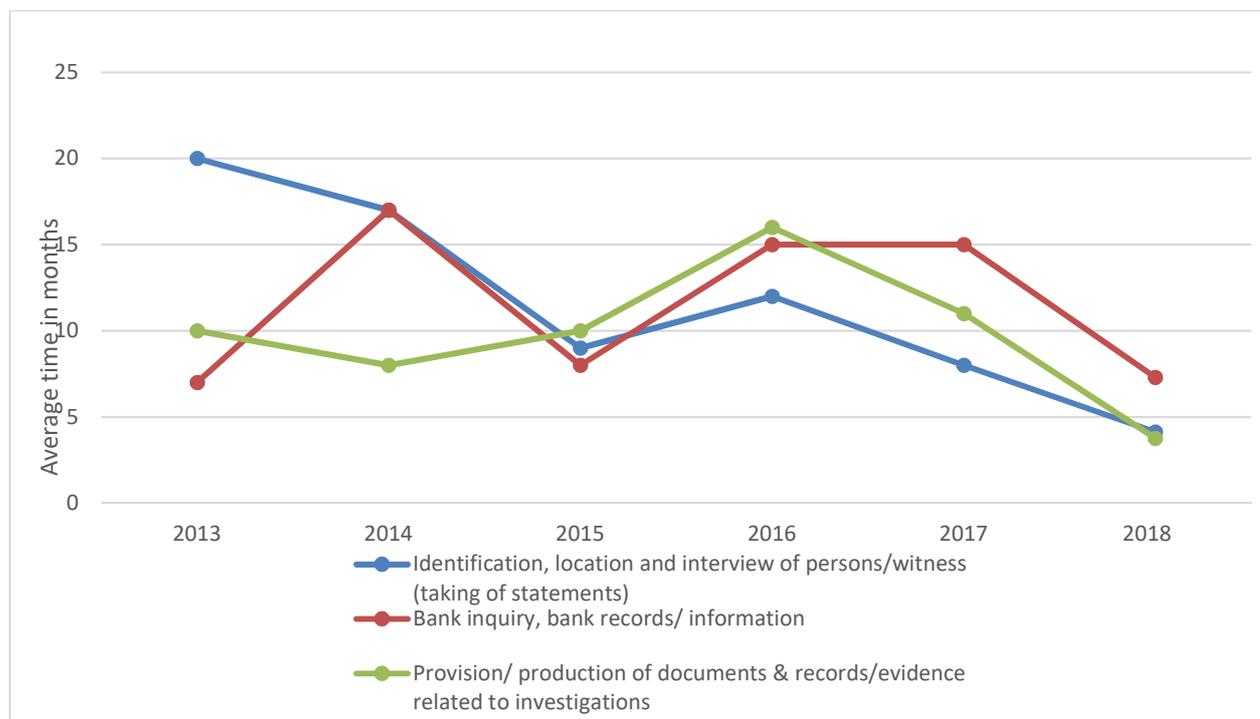
Table 8.1: Number of Incoming MLA requests (per predicate offence / ML)

Offences	2013	2014	2015	2016	2017	2018	Total
Money Laundering	8	5	3	11	10	6	43
Terrorist Financing	-	-	-	-	-	-	
Fraud/Investment Scam / Swindling	12	17	15	22	17	18	101
Trafficking in Persons/Child Pornography/Sexual Abuse	3	11	7	7	9	10	47
Murder/Homicide/Assault	4	6	5	15	9	7	46
Drug Trafficking	1	1	1	2	1	8	14
Corruption-related	3	1	-	3	2	4	13
Forgery/Falsification	2	2	-	2	2	2	10
Theft	-	1	-	4	-	2	7
Terrorism-related	-	-	-	-	3	2	5
Copyright Infringement/IPR	1	1	-	1	-	-	3
Environmental Crimes	-	-	2	-	-	-	2
Kidnapping	1	-	-	-	1	-	2
Smuggling	-	1	-	1	-	1	3
Manufacture/ possess firearms & explosives (illegal exportation & arms smuggling)	-	-	-	-	1	-	1
Illegal Gambling	-	-	-	1	1	-	
Totals	35	46	33	69	56	60	299

546. The timeliness of the Philippines' response to MLA requests shows some delays, albeit the response time is improving with some increasing support (see below) from AMLC to help to overcome delays. Information on the DOJ manual case management system reveals the average completion time of one year. While this timeframe may be reasonable in the context of specific cases, the concerns over a lack of timeliness is supported by international cooperation feedback received from two foreign counterparts on MLA requests. Even for bank inquiries, bank records/information, the average completion time took over a year in the period 2014 and 2016. Improvements in responsiveness were noted in the feedback in the period following AMLC's commencement of a staffing restructure and their closer involvement in helping to ensure MLA requests are met without undue delay. In an effort to improve timeliness, AMLC provides documents which are easy to gather (e.g. CDD documents) while it is completing its bank inquiry to get transaction documents.

Case Example 8.1 – MLA in relation to prosecution of a child sex offender in Norway

In February 2016, Norway made a request for assistance regarding offenses relating to the sexual abuse of minors, including the production of media of the sexual abuse of children. In November 2016 the Philippines provided requested items of evidence, including sworn statements of the victims and results of the search warrant conducted by Philippine LEAs. One of the suspects was convicted in Norway in December 2016 for sexual abuse of children and sentenced to eight years of imprisonment.

Table 8.2: The average time to complete MLA requests

547. The Philippines received 14 extradition requests in the period 2013-2018 covering a range of offences. One of these matters involved three separate requests. Three of the requests have been completed (of which one waived the right to an extradition hearing). The numbers of requests was relatively low, but it is notable that a small number related to ML and TF.

548. While extradition processes may necessarily be lengthy, the assessment team has concerns regarding some undue delays in these extradition matters, contributed by challenges of policy and practice. Concerns with undue delays with extradition proceedings included: abuse of motions regarding judges being 'inhibited' by questionable impartiality; complex and confusing application of Philippines' evidence law, rather than the treaty. While the work of the DOJ and OSG was acknowledged, responding jurisdictions flagged implementation of court procedures during extradition proceedings as problematic overall.

549. In one instance a request for extradition was made in April 2016 on murder charges, and the Philippines only responded in April 2018 with further questions / requests for clarification. The request is not yet completed. Another incomplete request relates to an extradition request lodged on embezzlement grounds in June 2014. In yet another case, a request for extradition was made in November 2013 in relation to importation of a commercial quantity of a border-controlled drugs and conspiracy to deal with proceeds of crime. The petition for extradition was granted by the courts three years later in October 2016.

550. LEAs coordinate with foreign counterparts in relation to deporting persons or receiving persons being repatriated from other jurisdictions having been accused of convicting serious crimes.

551. Outside of general feedback that related primarily to the timeliness of response, the assessment team was provided information by the Philippines of cases where its cooperation through response to MLA and extradition requests led to arrests and convictions in other jurisdictions. Some

feedback received from foreign counterparts is relevant to the issue of quality and indicates that where assistance is provided it is generally of reasonable or good quality.

Table 8.3: Incoming extradition requests to the Philippines

Requesting Party	Offence	Current Status
2018		
Korea Apr 2018	Murder with robbery	<i>In process</i>
Korea Sept 2018	Murder by robbery	<i>In process</i> : provisionally arrested Apr. 2019
2017		
Australia Aug 2017	Conspiracy to import a commercial quantity of a border controlled drug, conspiracy to traffic a commercial quantity of a controlled drug, attempt to prevent justice.	<i>In process</i> : proceedings ongoing: 5 Jun. 2018: DOJ filed Petition for Extradition 17 Sept 2017: date of provisional arrest 4 Sept. 2017: Application for Provisional Arrest filed;
Spain – Feb 2017	Membership in a criminal organization; money laundering	<i>In process</i>
US January 2017	A range of offences including terrorism, TF (including material support to terrorists) and conspiracy to use WMD	<i>In process</i> : Pending appeal 27 July. 2018: Order granting the Petition for Extradition 7 Apr. 2017: Subject’s provisional arrest
2016		
Canada April 2016	Murder	<i>In process</i> : Apr. 2018, DOJ requested clarification/additional information
US March 2016	Murder	<i>Complete</i> : Extradited 18 Nov. 2016; accused pleaded guilty and sentenced to 20 years-to-life imprisonment in the US. 20 Jun. 2016: Subject arrested
2015		
UK Nov 2015	Rape; attempted rape; attempting to pervert the course of justice	<i>In process</i> - Nov. 2016 DOJ requested clarification/additional information.
UK Dec 2015	Assault to severe injury and danger to life, attempting to pervert the course of justice	<i>Request withdrawn</i> - Subject returned to UK in Jan. 2016; arrested/convicted in UK and served sentence
UK Dec 2015	Child abduction	Requesting Party informed in 2017 that the offense is not extraditable under the PH-UK Extradition Treaty
2014		
Thailand July 2014	Making false report; embezzlement	<i>In process</i>
UK June 2014	Drugs offences – The person had fled UK after he was convicted in the UK for the subject offenses	<i>Complete</i> - Extradited to UK in Feb 2015 - Subject waived extradition proceedings 23 Jan. 2015: Date of provisional arrest
2013		
Australia Nov 2013	Conspiracy to traffic a commercial quantity of a controlled drug, conspiracy to import a commercial quantity of a border controlled drug and conspiracy to deal with proceeds of crime	<i>In process</i> : appeals pending with the Court of Appeals 6 Oct. 2016: petition for extradition granted 14 Nov. 2013: date of provisional arrest
Korea Feb. 2013,	Murder, “murder by robbery”, 4 separate cases of “special robbery”,	<i>Complete</i> - 2018 – convicted in Korea and sentenced to life imprisonment

updated in 2015 & 2017 (temp surrender)	“special robbery, etc.”, and “bodily injury resulting from robbery”	2015 - temporarily surrendered to be jointly tried in Korea 2013 –tried and convicted in the Philippines for illegal possession of firearms
---	---	--

Case Example 8.2 – Extradition request

In 2013, the Republic of Korea requested the extradition of an accused to face charges including murder and robbery. However, the accused was being prosecuted in the Philippines for illegal possession of firearms. He was later convicted and sentenced to 4-5 years imprisonment.

In December 2014, the Philippines received a further request from Korea for the temporary surrender of the accused on the same grounds. The temporary surrender request identified that his co-accused in a murder-by-robbery, was temporarily surrendered to Korea by Thailand in October 2013. The co-accused was raising the defence in his trial that he did not participate in the commission of the said crime and that the subject crime was committed by the accused and another co-accused, who died before the trial began. Korea sought to try both co-accused together. In May 2015 the Philippines granted the request for the temporary surrender which was renewed in 2016 and in May 2018.

The accused was prosecuted in Korea for the offenses and was ultimately sentenced to life imprisonment, made final by a decision of the Korean Supreme Court on 17 September 2018.

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

552. In the period 2013 to 2018, the Philippines made 36 MLA requests. Of these, 28 were successfully completed, two remain pending and one was denied due to the foreign court not accepting a request to give effect to a Provisional Asset Preservation Order (PAPO) issued by the Philippine court, as the PAPO was not considered to be equivalent to its domestic forfeiture order. The high completion rate of outgoing MLA requests reflects good agency to agency support of requests made. It is notable that 25 of the 32 MLA requests went to jurisdictions making more than one request.

553. The level of outgoing MLA requests is low compared to scope of transnational crime and the level of incoming MLA requests. While there is a high level of investigative activity by LEAs on predicate crimes, there is a lack of focus on obtaining foreign evidence of transnational elements of the criminal activity for inclusion in prosecutions. Limited capacity and resources in the DOJ for MLA and extradition issues have led to delays for LEAs in receiving assistance through those formal channels, thereby dissuading LEAs from utilising them. There is also a preference amongst LEAs to utilise information mechanism of cooperation due to perceived efficiencies.

Table 8.4: Philippines’ outgoing MLA requests – by crime type

Offense	2013	2014	2015	2016	2017	2018	Totals
Money Laundering		1	1	-	-	-	2
Terrorism-related (including elements of TF)		-	-	-	-	1	1
Trafficking in Persons / Child Pornography / Sexual Abuse		5	3	1	-	2	11
Fraud /Investment Scam		2	2	1	1	-	6
Murder/ Homicide/ Assault		1	1	2	2	-	6
Corruption-related		1	2	-	-	-	3
Illegal recruitment		-	1	1	-	-	2
Kidnapping		1	-	-	-	-	1
Totals	4	11	10	5	3	3	36

Table 8.5: Outgoing MLA Requests – Jurisdictions receiving more than one request

Requested Parties	2013	2014	2015	2016	2017	2018	Total
US	1	4	2	1	-	2	10
Chinese Taipei		1	1	2	1	-	5
Malaysia	3	1	1	-	-	-	5
UK		2	-	-	-	1	3
Indonesia		-	1	1	-	-	2

554. In terms of predicate offences that pose a higher threat to the Philippines, the utilisation of MLA is very low and not proportionate to the risk profile. Although the geographical landscape and vast maritime borders and sea ports make the Philippines susceptible to the smuggling and corruption has been detected among customs officials, there are only three MLA requests for smuggling and nine for corruption-related crimes.

555. The limited number of outgoing requests relating to ML is inconsistent with Philippines' ML risk profile, given that Philippines main proceeds-generating crimes are largely transnational in nature. In the context of ML, the limited use of international cooperation appears to be a product of concerns amongst investigators about delays caused by courts; a limited awareness of formal channels of international cooperation; the absence of mechanisms amongst Philippines authorities to select, prioritise and make requests for assistance; and the lack of a proactive approach to combating ML and pursuing criminal assets outside the Philippines, as outlined in the analysis of IO.7.

Case Example 8.3 - Outgoing MLA - Request to UK authorities regarding a TF case

In 2018 the NBI conducted investigations to identify a suspected ISIL extremist based in the Philippines, known as adz Abdusalam. Abdusalam, who had contacted US-based ISIL extremists via social media regarding his provisions of medical supplies to ISIL fighters in Marawi City and later in relation to purchasing bombing equipment. Abdusalam's wife was also a person of interest for acting as a money courier for ISIL fighters in Marawi City.

Investigation was conducted in coordination with NICA, PNP and other local authorities and with US and UK authorities. Search warrants were executed in the Philippines. NBI submitted an MLA to the DOJ, which was then transmitted to UK authorities, for evidence pursuant to a TF case against Abdusalam and his associates.

556. With respect to TF, the few TF investigations overall correlates with the limited TF-related MLA requests despite the high risks associated with TF in the Philippines. However, it is notable that the low level of outgoing requests from the Philippines is matched by a lack of incoming MLA (zero) or extradition (one) requests linked to TF (see case study).

557. In the period 2013 to 2018, the Philippines made a total of five extradition requests, three of which are related to murder prosecutions with one related to TF. None were related to ML. Two were successful, one was denied and three are ongoing. The incoming extradition request in relation to TF in a case connected to significant police to police and outgoing MLA cooperation is notable. Even with these positive developments, given the risks in the Philippines, and its size and geopolitical status, six extradition requests is a notably small number over six years. Similar to MLA the primary reason for the lower number of outgoing extradition cases seems to be a lack of focus on transnational elements of the criminal activity being investigated.

Table 8.6: Philippines' outgoing Extradition requests

No.	Requested Party	Requesting Agency - Offense & Request	Outcome
2013			
1	US	NBI - Provisional arrest request for Double Murder	Subject extradited in 2014 (died in 2015 while case was being heard)
2014			
1	Malaysia	National Prosecution Service - Provisional arrest request for Syndicated Fraud	Request denied in Oct. 2014 (basis: lack of an extradition treaty between the Philippines and the requested Party; inability of the Philippines to guarantee the subject if extradited)
2015			
1	US	National Prosecution Service -Provisional arrest request for Murder	Extradited in May 2016 ; trial ongoing; subject is detained
2016			
2	Australia	NBI & private complainant - Murder	Ongoing
	India	National Prosecution Service - arrested pursuant to INTERPOL Red Notice – human trafficking / child pornography / sexual abuse	Ongoing
Total requests		5	

Seeking and providing other forms of international cooperation for AML/CFT purposes

558. For other forms of international cooperation, the Philippines utilises a wide range of mechanisms. This includes regular bilateral or multi-jurisdictional operation meetings on predicate offences, engagement with relevant regional and international organisations and regular officer level contact with foreign counterparts.

559. Competent authorities are responsive to incoming requests received through these channels and generally provide assistance of satisfactory quality in a timely manner, in particular AMLC facilitated requests. However, outgoing requests for assistance by Philippines agencies are less frequent and not generally in keeping with the risk profile.

FIU

560. AMLC, through Egmont and other networks, actively supports international cooperation for its own use and on behalf of other domestic competent authorities. However, the volume of requests made by the FIU AMLC is low. From 2013 to 2018, AMLC made 82 requests on ESW (on per predicate offense basis) or 128 ESW requests (on per country basis). These requests have been in line with the Philippines' identified higher risks (ML, corruption, fraud, drugs, TF).

Table 8.7: AMLC Egmont Secure Web Outgoing Requests

ESW requests made by crime type	2013	2014	2015	2016	2017	2018	Total
Money Laundering	3	2	5	5	2	2	19
Terrorist Financing		-	-	1	1	5	7
Corruption	3	4	5	-	-	4	16
Fraud	4	2	1	1	-	3	11

Drugs	1	-	1	3	1	2	8
Others		-	1	2	-	8	11
Electronic Commerce Act violations		-	-	3	-	1	4
Violation of Banking Law		-	-	-	1	-	1
Child Abuse		-	1	-	-	-	1
Qualified Theft	1	-	-	-	-	-	1
Murder		1	-	-	-	-	1
Human Trafficking						2	
Grand Total	12	9	14	15	5	27	82

561. AMLC monitors the timeframes for foreign FIUs responding to ESW requests and engages with foreign partners to increase the quality and timeliness of responses. A majority of responses are received from foreign partners in a timely period.

562. The Philippines FIU is responsive to incoming requests. From 2013 to 2018, AMLC received 462 foreign requests. 14% of incoming requests related to ML while 6% related to TF. 33% of incoming requests related to fraud, while corruption accounted for 7% and drugs, human trafficking and tax evasion accounted for approximately 3% each. The majority of which have been responded to within a period of six months or less. Feedback from foreign counterparts confirmed that international cooperation from AMLC was generally responsive and helpful, particularly on ESW.

563. In addition to the bilateral exchange of financial intelligence, AMLC also engages with the regional FIUs, namely AUSTRAC, PPATK and Bank Negara Malaysia through iterations of Multilateral Analyst Exchange Programme (MAEP). MAEP programmes have resulted in exchange of financial intelligence between the FIUs on TF, including assessing the flow of funds, fighters and material support to the MAUTE Group and associated groups in the Philippines prior to and during the Marawi Siege in 2017. AMLC shared the findings of the MAEP with domestic partner agencies.

LEAs

564. LEAs actively interact with international counterparts on predicate offences. However, the number of cases including informal international cooperation does not reflect the scale of transnational criminal risks in the Philippines, or the level of interest from international counterparts. Cooperation by LEAs other than AMLC is mostly limited to responding to the specific predicate offence that is the subject of the investigation or referral.

565. With the exception of the AMLC, most LEAs do not prioritise international cooperation with foreign counterparts on ML/TF or broader financial investigations including asset tracing. However it is noted that AMLC is the primary ML/TF investigator in the Philippines.

566. Various LEAs have a range of agreements in place with foreign partners and participate in a number of regional and global initiatives to support police-to-police cooperation. The PNP provided several examples of cooperation with investigators from foreign counterparts in relation to particular cases, or through the foreign LEAs with a representative in the Philippines (34 jurisdictions have a presence in the Philippines). The PNP has also established offices in the United States, China, Pakistan, Malaysia and Saudi Arabia for its Police Attaches. This allows ease of cooperation ranging from human trafficking to TF. NBI has a link with many countries, including the United States, China and other

INTERPOL members and utilises various communication channels to cooperate with counterparts in relation to predicate offences, including drug offences and terrorism.

567. *AMLC*: As an investigative agency, AMLC pursues international cooperation through coordination meetings and case conferences with foreign partners. This occurred for three cases dealing with predicate offences (corruption, hacking and smuggling) between 2013 and 2018. For example the Bangladesh Heist case (see IO.7) resulted in 34 meetings and the PDAF case for example (see IO.6 & 8) led to over 20 meetings and regular information exchange through other means.

Case Example 8.4 – International LEA cooperation

Coordinated efforts between NBI, PNP and U.S. Homeland Security Investigations (HSI) culminated in an arrest and rescue of five children in Bulacan, Philippines in March 2018. The accused was arrested for violations of the Expanded Trafficking in Persons Act of 2012, Cybercrime Prevention Act of 2012, Anti-Child Pornography Act of 2009, and Anti-Trafficking in Persons Act of 2003.

568. *PDEA*: In the period 2015-2018, PDEA made 59 requests to foreign counterparts (through official letters) in relation to drug cases. In the same period, PDEA received 141 requests from foreign counterparts. PDEA also conducted informal cooperation with foreign counterparts. PDEA demonstrated active cooperation with investigators of foreign counterparts on particular cases.

569. *OMB*: OMB demonstrated cooperation with foreign counterparts on particular predicate investigations. In some instances AMLC was involved for exchanging financial information.

Financial / Supervisory

570. *BSP*: is proactive in providing or requesting information, including information for fit and proper assessments. BSP is responsive to requests for information from various foreign counterparts and from non-counterparts. Depending on the nature of request, the BSP may directly act on it, or refer it to the appropriate government agency, such as AMLC, for appropriate action. Typical information exchanges conducted by BSP with counterpart regulators relate to fit and proper assessment of proposed stockholders, directors or officers of BSFIs. Coordination and information exchange takes place with host supervisors for onsite examination of branches abroad of Philippine banks and there are instances that the host supervisor meets with the BSP team to discuss the scope/coverage of the examination.

571. *SEC*: SEC pursues international cooperation with foreign counterparts for AML/CFT on market entry fit and proper issues. The SEC is a member of the IOSCO, and has existing Memoranda of Understanding with Indonesia, Hong Kong, China and Iran.

572. *IC*: To date, the international cooperation extended between IC and its foreign counterparts/international organizations has related mostly to prudential regulation or insurance matters and has not extended to AML/CFT, with the exception of its response to one request in relation to market entry controls by a foreign counterpart.

573. *Tax*: The BIR shares information, including tax records and bank deposit information, with counterparts under its international tax treaties. It received 163 separate requests over the period 2013-2018 from 20 jurisdictions; and sent 23 requests out to 13 jurisdictions over that period. While BIR clearly has a well utilised network of tax treaty partners, it is not clear whether these related to ML/TF.

International exchange of basic and beneficial ownership information of legal persons and arrangements

574. AMLC has experience of exchanging basic and beneficial ownership information on legal persons, largely based on ESW requests. BSP, SEC and IC have not received any request for information on beneficial ownership. Registered information on basic ownership of legal persons is publicly available to foreign counterparts through the GIS. AMLC does not maintain statistics on the inclusion of beneficial ownership in incoming or outgoing requests, however provided one example of it requesting beneficial ownership information via ESW.

Case Example 8.5 - Beneficial Ownership

In September 2017 AMLC received a request via ESW from a foreign FIU in relation to an investigation on a business entity engaged in trading arms and military equipment. The FIU requested information in relation to four companies; A, B, C and D, three of which had received outward remittance from the business entity being investigated by the FIU. The request also sought information on the beneficial owners, authorised persons, business or financial activities and any criminal records that AMLC could access on the entities and beneficial owners.

In March 2018 AMLC responded to the report, providing the following information, which the Philippines notes includes beneficial ownership information:

- Company A – names, addresses, nationality, number of shares subscribed, amount of shares subscribed as a percentage of stock ownership; and names, addresses, nationality, tax identification number and position of its key corporate officers and executives.
- Company B (registered partnership) – names, addresses, nationality and capital contribution of its partner.
- Company C (trading company) – names and key executive positions of the owners.
- Company D – names, addresses, nationality, number of shares subscribed, amount of shares subscribed as a percentage of stock ownership; and names, addresses, nationality, tax identification number and positions of its key corporate officers and executives.

Overall conclusion on Immediate Outcome 2

575. The Philippines has a sound basic framework for international cooperation, and overall AMLC and BSP are the most active in responding to and seeking international cooperation in response to the risk profile. Overall it is not evident that LEAs use formal channels to actively pursue transnational activities of criminals in line with the national risk profile. Timeliness of response to MLA and extradition requests is a concern, however there has been an improvement in timeliness in recent years. With respect to other forms of international cooperation, the Philippines benefits from a wide range of mechanisms at varying degrees of formality. The strength of the Philippines informal networks is a positive, however there is a need for greater proactive use of these channels focusing on key risks. Cooperation is shown to be strongest in response to requests.

576. **The Philippines has a moderate level of effectiveness for Immediate Outcome 2.**

TECHNICAL COMPLIANCE ANNEX

1. This annex provides detailed analysis of the level of compliance with the FATF 40 Recommendations of the Philippines 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.

2. 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 [date]. This report is available from www.apgml.org.

Recommendation 1 - Assessing Risks and applying a Risk-Based Approach

3. This is a new Recommendation, which was not assessed in the 2009 MER.

4. *Criterion 1.1* - Philippines has identified and assessed its ML/TF risks through various exercises over a number of years. Serious Organised Crimes Threat Assessments (SOCTAs) were undertaken in 2013, 2014 and 2016, which took a reasonable approach to assess the Philippines context, main threats and vulnerabilities As well as some elements of sectoral vulnerabilities. The 2016 SOCTA analysed the nexus between emerging trends and organised crimes and other serious crimes. The Philippines has undertaken two National Risk Assessments, the First National Risk Assessment on ML/TF (2011-2014) and the Second National Risk Assessment Report on ML/TF (2015-2016) published in 2017. The 2017 NRA included three stages process, i.e. coordinated methodology building, analyses and review of findings and initial mitigation action plan. Both quantitative and qualitative data drawn from periodical reports and submissions from LEAs and other agencies as well as private sector's input were also utilised in the NRA. In addition, the Philippines also undertook a NPO Sector Assessment (November 2018). The Philippines assessment of TF risks does not sufficiently take into account the threat posed by presence and movement of foreign fighters in, into and out of the Philippines, or the significant terrorism related events since 2016, while some understanding of money trail in relation of TF is undertaken at the regional level by AMLC in relation to Marawi Siege. Less comprehensive risk assessments of legal persons in the context of accessibility of beneficial ownership by the different sectors were also undertaken as part of the NRA. The understanding of the vulnerabilities of legal persons/ legal arrangements in posing ML/TF risk, inter- linkages between covered persons and crimes, external threats/ foreign proceeds is weak and vulnerabilities arising from the cash economy are not well understood.

5. *Criterion 1.2* - AMLC is the lead agency for coordinating risk assessment exercises NRAs (Office of the President Memorandum Circular No. 64 dated 20 June 2014) in which the authority is sourced from Rule 13(1) of the 2018 Implementation Rules and Regulation of AMLA (2018 IRRs) (for NRA). While for the purpose of sectoral risk assessment, Rule 7(3) of the 2018 IRRs provides for supervisory authorities to conduct sectoral risk assessments. A broad range of government agencies and private sector stakeholders were consulted in the first and second NRAs. The NRA is organised through the National Risk Assessment Working Groups (NRAGWG). The SOCTA are coordinated by the Presidential Anti-Organized Crime Commission (PAOCC) and undertaken by the National Law Enforcement Coordinating Committee-Sub-committee on Organized Crime (NALECC-SCOC).

6. *Criterion 1.3* - AMLC is required to undertake an NRA every three years or as the council may deem necessary (AMLC Resolution No. 131 (QM-AMLC-03-03-007-02) and Rule 13(2) of the 2018 IRRs). In practice, the SOCTA has been, updated three times i.e. 2011, 2013 and 2016 and is scheduled to be updated at two-year-intervals. Two NPO assessment have been undertaken in 2008 and 2018.

TECHNICAL COMPLIANCE

7. *Criterion 1.4* - The Philippines has various mechanisms to share the findings of risk assessments. The NRA reports are publicly available on AMLC website. Results of the NRA and other assessments were further disseminated to FI/DNFBPs during seminars, meetings with industry associations and with high risk sectors. The full version of the NRA that contains sensitive information is disseminated to the Office of the President, supervisory authorities and other government agencies. The findings of the NRA were also featured in lectures and coordination workshops with LEAs, trainings for supervisory authorities. Generally, the platforms currently cover the findings of the NRA but do not exhaustively include other risk assessments.

8. *Criterion 1.5* - The Philippines has taken some steps in applying the risk-based approach to allocating resources and implementing appropriate measures to mitigate ML/TF risks. Among others, the steps include the wholesale re-licensing of MSBs, AMLC re-structuring and increasing resources into financial intelligence and high-threat predicate offences. While law enforcement agencies have applied some resources to predicates posing higher levels of ML/TF threat, alignment between risk and mitigation is not made across risks identified.

9. *Criterion 1.6* - The AMLA 2016 RIRR provides certain exemption for the application of AML/CFT requirements for areas that are proven to be low risks or risks are properly mitigated. Consequently, such exemption/relaxation is exercised the Philippines provided for the purpose of financial inclusion and during disasters. Exemption or simplified CDD are given to circumstances where identity of customer or beneficial owners are publicly available, or exist in the national system (SEC Memorandum Circular No. 16, Series of 2018). In addition, BSP Circular No. 950 allows reduced due diligence measures where lower risks of ML/TF have been identified through adequate analysis of risk by the covered person. The reduced due diligence procedures should be commensurate with the lower risk factors, but are not acceptable whenever there is suspicion of ML/TF, or specific higher risk scenarios apply. The new 2018 IRR, allows for exemptions to CDD and record keeping requirements in situation or financial activities where it is proven low risk, upon approval by AMLC (Rule 14, Section 2 of the 2018 IRR).

10. *Criterion 1.7* - Rule 14(3), of the 2018 IRRs requires all covered persons to manage and mitigate higher risks and to take into consideration higher risk areas into institutional risk assessments. BSP also issued circulars to its supervised FIs on the need to apply stricter controls on the sector that have been identified as higher risks in the NRA, i.e. MSBs and pawnshops. A directive was issued on 12 November 2018 to casinos to undertake institutional risk assessment based on the findings of the NRA under the CIRR/ ARGCC (PAGCOR Regulatory Order No 2018-11-001).

11. *Criterion 1.8* - The 2018 IRR, as amended, allows covered persons to take simplified measures to provided that risks are properly managed and mitigated. Specifically, Rule 18(11) allows for reduced due diligence where lower ML/TF risks have been identified. Rule 14(4) of the 2018 IRR, in addition, provides for AMLC and the supervisory authorities to allow covered persons to take reduced due diligence measures; provided that lower risks have been identified, and this is consistent with the results of the NRA.

12. *Criterion 1.9* - Section 10 of the AMLA, authorises the BSP to check compliance of the covered person with the requirements of the AMLA and its 2018 IRR enables the relevant supervisory authorities to supervise compliance with AML/CFT requirements including obligations under R. 1. The requirement is affected by scope gaps found under R. 28.

13. *Criterion 1.10* - Based on the 2018 IRR of the AMLA, these requirements in relation to consideration for risk factors, documentation and update/ review have been imposed to all covered persons, including DNFBP (See Rule 15(1)). The 2018 IRR requires covered persons to a) document the risk assessments; b) consider all relevant risk factors before determining the

level of overall risk and the appropriate mitigation measures to be applied; c) keep these assessments up to date; and d) establish appropriate mechanisms to provide the risk assessment results and any information related to AMLC and the SAs, when required. In addition, the pre-existing requirements, such as s.X805.5/4805Q.5 of the MORB/MORNBF1 and Section 7 of IC CL 2018-48 provide that covered persons are required to identify, understand and assess their respective ML/TF risks arising from customers, countries or geographic areas of operations and customers, products, services, transactions or delivery channels. The assessment methodology shall be appropriate to the nature of operations and complexity of the business of the covered person. The risk assessment shall (a) consider all relevant risk factors; (b) adequately document results and findings; and (c) be updated periodically or as necessary. Based on the risk assessment, the covered person shall take appropriate measures to manage and mitigate ML/TF risks which are stipulated under 2016 RIRR in relation to treatment for normal, simplified and enhanced CDD. The risk assessment is also required to be made available to the BSP/IC during examination or in other circumstances deemed necessary as part of continuous supervision.

14. *Criterion 1.11* - Rule 15(2.2) of the 2018 IRR requires all covered persons to (a) have policies, controls and procedures as approved by the board of directors, partners or sole proprietor, to enable them to manage and mitigate the risks that have been identified in the NRA, or by AMLC, supervisory authority or the covered person itself; (b) monitor the implementation of those controls and to enhance them if necessary; and (c) take enhanced measures to manage and mitigate the risks where higher risks are identified. In addition, similar requirements are found in CL 950 Subsection X805.1/4805Q.1 and X805.2/4805Q.2 for BSP supervised institutions, and Sections 5.A.1, 5.C.1, 5.C.3 and 5.D.1 of SEC Memorandum Circular No. 16, Series of 2018 for the securities sector, CL 2018-48 for the insurance sector, s.10 of the CIRR.

15. *Criterion 1.12* - Rule 15, Section 2.3 of the 2018 IRR provides that all covered persons may adopt reduced due diligence to manage and mitigate risks if lower risks have been identified, provided, that the requirements of Rules 13 to 16 are met. Reduced due diligence is not allowed whenever there is a suspicion of ML/TF. Other requirements could be found in BSP Circular No. 950, Subsection X806.1/4806Q.1, s.5.C.2 of SEC Memorandum Circular No. 16, Series of 2018 1.a, s.31 of IC CL No. 2018 - 48 provides for simplified measures (mainly CDD) for the respective covered institutions. Simplified CDD is not permitted in the case of suspicion of ML/TF, or other specific high risk scenarios per BSP, IC and SEC instruments.

Weighting and Conclusion

16. The Philippines had generally understood its risks through various iterations of NRAs and SOCTAs at the country level. These have been supplemented with other standalone risk assessments. The understanding of the vulnerabilities of legal persons/ legal arrangements in posing ML/TF risk, inter-linkages between covered persons and crimes, external threats/ foreign proceeds is weak and vulnerabilities related to the cash economy are not well understood. A recent revision of the 2018 IRR had rectified deficiencies with respect requirements on all covered persons to respond to identified risks. Compliance remains affected by the scope gap found under R.28 and coverage of other specific risk assessments i.e. legal persons.

17. **Recommendation 1 is rated largely compliant.**

Recommendation 2 - National Cooperation and Coordination

18. The Philippines was rated partially compliant for the previous R31. The main deficiency noted was that Philippines' human and financial resource constraints affect operational mechanisms for national cooperation.

TECHNICAL COMPLIANCE

19. *Criterion 2.1* - The National AML/CFT Strategy (NACS) was approved by AMLC in June 2018 and adopted through a Presidential Executive Order on 12 November 2018. The NACS applies for the period between 2018 and 2022, and required to be reviewed in 2020 or when circumstances warrant, (s.7 of the Executive Order No. 68). Action plans under the NACS are generally aligned with the risk identified under the NRA. In addition to the adoption of NACS, specific short-term action plans for relevant agencies are included in the 2nd NRA 2017 to quickly respond to the risks identified. In terms of CFT Strategy, the Anti-Terrorism Council produced the National Anti-Terrorism Strategy (NATS) in 2009, which is now outdated. However, this deficiency has been addressed by the adoption of NACS.

20. *Criterion 2.2* - The establishment of a National AML/CFT Coordinating Committee is formalised by Executive Order No. 68 (2018) which is headed by the Executive Secretary of the Philippines, \ BSP Governor/ AMLC Chairperson as Vice-Chair. AMLC is the Secretariat for the NACC, and is responsible for the coordination, logistics and operations of the meetings, and coordination with and monitoring of duties and responsibilities of the NACC and the subcommittees. The NACC comprises of the following sub-committees:

- a. Financial Intelligence, Law Enforcement and Prosecution subcommittee;
- b. Supervision of Financial Institutions sub-committee;
- c. Supervision of Designated Non-Financial Businesses and Professions sub-committee;
- d. Terrorism Financing and Proliferation Financing subcommittee;
- e. AML/CFT Awareness sub-committee.

21. The members of the NACC and sub-committees consist of 14 agencies including the BSP, Ministry of Foreign Affairs, Ministry of Finance, Ministry of Justice, Ministry of National Defence, Ministry of the Interior and Local Government, Ministry of Trade and Industry; SEC, IC, Philippine Amusement and Gaming Corporation; Cagayan Economic Zone Authority and Aurora Pacific Economic Zone and Freeport Authority.

22. *Criterion 2.3* - Prior to the establishment of NACC at the Committee and Sub-Committee levels (please see criterion 2.2), there were several committees established to allow competent authorities to cooperate and coordinate domestically on policy issues and operational issues relating to AML/CFT. Primarily, these include:

Policy making coordination:

- National Law Enforcement Coordinating Committee (NALECC), including the NALECC Sub-Committee on Anti-Money Laundering/Countering the Financing of Terrorism (SCAML/CFT). The NALECC has 59 Members and 18 sub-committees. NALECC is a forum for dialogue and coordination whose functions include: a) coordinate policies/procedures; b) Identify priority areas for coordinated/joint law enforcement activities; and c) Prepare and submit to the Chairman POC for strategies/plans.
- National Security Council (NSC) is the principal advisory body for the coordination and integration of plans and policies affecting national security. It advises the President on national security related matters, provides supervision and guidance over the NICA and general supervision over the intelligence community, and coordinate the national government efforts for the national security and strategic goals / objectives.

Operational coordination:

- Joint Terrorist Financing Investigation Group (JTFIG) includes members from the anti-terrorism groups of the NBI, PNP-IG, PNP-CIDG, the PNP-DI, the PNP-SAF, the Law Enforcement and Security Integration Office (LESIO), the PCTC, AMLCS and the US FBI. The JTFIG meets to address TF threats in the Philippines and Southeast Asia, and

enables member agencies to directly share intelligence information on terrorism and TF cases.

- Inter-Agency Committee Against Drugs (ICAD) is headed by PDEA and includes a wide range of agencies to implement and comply with all policies, laws and issuances pertaining to the government's anti-illegal drug campaign in an integrated and synchronized manner..
- Anti-Terrorism Council (ATC) has primary responsibility for the proper and effective implementation of the anti-terrorism policy of the country. The Secretariat to the ATC is the National Intelligence Coordinating Agency. TC is supported by the NBI, Bureau of Immigration, Office of Civil Defence, Intelligence Service of the AFP
- The Financial Sector Forum includes the BSP, SEC, IC and the Philippine Deposit Insurance Corporation and operates to (a) harmonise the coordination of supervisory and regulatory methods and policies; (b) support reporting, information exchange and dissemination;

23. The NACC establishes policy and operational level coordination, organised into five sub-committees, specific to cooperation and coordination of the AML/CFT matters.

24. *Criterion 2.4* - A TF and PF Sub-Committee has been established under the NACC which primarily responsible for the implementation of action plans under Strategic Objective 5. Prior to the NACS and NACC, the issue of PF was considered as a matter of management of 'strategic goods' which may be considered to be goods of military importance or for the purpose of the production of WMD. The National Security Council includes the NSC-Strategic Trade Management Committee (NSC-STMCom) which is the central authority for matters relating to strategic trade management. The Department of Foreign Affairs coordinates the implementation of the UNSC Resolutions and sanctions in relation to proliferation. The ATC Project Management Centre (ATC-PMC) as the NSC-STM Secretariat also holds meetings with concerned agencies regarding the implementation of UNSC Resolutions imposing sanctions on DPRK.

25. *Criterion 2.5* - While there are no specific cooperation and coordination mechanisms between relevant authorities, the AML/CFT requirements under the AMLA, and the TFPESA and domestic data protection and privacy rules, including the Data Privacy Act of 2012 (DPA) generally do not conflict. The AMLA and the TFPESA, which require disclosure of personal financial information, are recognized exceptions to the general rules on data privacy and secrecy of bank deposits under the DPA and R.A. 1405, respectively. In particular, Sec. 4 (e) of the DPA provides the ability for the sharing of "Information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance of the functions of the BSP, LEA and regulatory agencies.

Weighting and Conclusion

26. **Recommendation 2 is rated compliant.**

Recommendation 3 - Money laundering offence

27. In its 2nd round MER in 2009, the Philippines was rated partially compliant with former R.1 and largely compliant with former R.2. The MER found gaps in the coverage of elements of the Vienna and Palermo conventions and it was not clear whether the ancillary offence of conspiracy was criminalized. Many crimes were not defined as predicate offences for ML.

28. *Criterion 3.1* - Section 4 AMLA, criminalises ML on the basis of the Vienna and Palermo Conventions. This includes conversion, transfer, disposal of, movement, acquisition, possession or use, concealment or disguising the true nature, source, location, disposition, movement or

TECHNICAL COMPLIANCE

ownership of or rights with respect to the monetary instrument or property that represents, involves or relates to the proceeds of any unlawful activity. All the physical and material elements of the ML offence are covered in line with the requirements of the Vienna and Palermo Conventions.

29. *Criterion 3.2* - Predicate offences are listed through the definition as “unlawful activity”, which is defined in s.3(i) of the AMLA and covers a wide range of predicate offences. Only tax crimes are currently not included in the definition of an unlawful activity. Participation in an organised criminal group and racketeering is covered, as set out in the Palermo Convention, as an offence based on conspiracy (s.4(d) of the AMLA).

30. *Criterion 3.3* - The Philippines has adopted a list approach to define the scope of predicate offences (see analysis above in c3.2).

31. *Criterion 3.4* - The ML offence as laid out in Section 4 of the AMLA, covers any type of property, regardless of its value, that directly or indirectly represents the proceeds of crime. The term ‘proceed’ covers any amount, derived or realized from any unlawful activity (Rule 2, s.1 (bbbb) 2018 IRR); and property covers anything of value, tangible or intangible, or any interest, benefit, privilege, claim, or right with respect thereto (Rule 2, s.1 (cccc) 2018 IRR.). While these definitions are broad, the term “corporeal or incorporeal” which is included the FATF definition does not directly appear in the Philippines legislature. However, the definition of “property” appears to cover both corporeal and incorporeal (which can be read interchangeably with tangible/intangible property) whilst “monetary instruments” make reference to a “participation or interest”. The term “derived or realised from” in the definition of proceeds would cover indirect proceeds as well, particularly the term “derive” allowing for a less stringent relationship between cause (crime) and result (assets).

32. *Criterion 3.5* - Under the AMLA, prior conviction for the predicate offence or unlawful activity is not necessary in proving that the property is the proceeds of the crime. S.6 stipulates any person can be charged with and convicted of both the offence of ML and an ‘unlawful activity’ (which refers to predicate offences) and the prosecution under AMLA shall proceed independently of any proceedings relating to the unlawful activity.

33. *Criterion 3.6* - This criterion is satisfied as ‘unlawful offences’ (predicate offences) refer to any act or omission or series or combination involving or having a direct relation to offences of a similar nature punishable in other jurisdictions as predicate offences for the purpose of the AMLA (s.3(i)(34)).

34. *Criterion 3.7* - This criterion is satisfied as any person may be charged with and convicted of both the offence of ML and the unlawful activity. Criminal liability is attached with either self-laundering or third-party laundering (s. 6 of the AMLA).

35. *Criterion 3.8* - According to Rule 9, s.4.3 of the 2018 IRR, the element of knowledge may be established by direct or circumstantial evidence. Rule 9, s.4.4 says the rules of the courts shall govern all proceedings concerning the prosecution of ML. The Revised Rules of Court s.2 and s.5 refer to ‘proof beyond reasonable doubt’ and ‘circumstantial evidence’. In particular, the term circumstantial evidence is provided to be sufficient for conviction (in s.5 of the Revised Rules of Court) where the facts from which the inferences are derived are proven; and the combination of all the circumstances is such as to produce a conviction beyond reasonable doubt. Philippines provided two cases of the Supreme Court where intent was allowed to be inferred from the facts, and knowledge from the ‘overt acts of the person’.

36. *Criterion 3.9* - Section 14 of the AMLA stipulates the sanctions for ML. A person is convicted for violation of s.4 (a), (b), (c) and (d) of the AMLA⁸⁵, can be liable for imprisonment ranging from seven to 14 years and a fine of not less than three million Philippine pesos (approximately USD 56,520) but cannot be more than twice the value of the monetary instrument or property involved in the offence. The authorities indicate that the term “involved” pertains to the proceeds derived from or related to unlawful activity. With respect to violations of s.4 (e) and (f) (ancillary offences) liability is imprisonment from four to seven years and a fine of not less than one million five hundred thousand Philippine pesos (approximately USD 28,260) but not more than three million Philippine pesos (approximately USD 56,520).

37. In comparison with other serious proceeds generating offences in the Philippines, terms of imprisonment and fines for ML offences are sufficiently proportionate and dissuasive.

38. *Criterion 3.10* - Section 14(a) of the AMLA imposes sanctions on persons convicted under s.4 (a-f) of the AMLA. S.14, paragraph after (c) of the AMLA provides that where an offender is a corporation, association, partnership or any legal person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or allowed by their gross negligence, the commission of the crime. The Philippines authorities clarified the term “responsible officers” as directors, officers or employees of such legal person.

39. The only criminal sanction imposable where the offender is a legal person is a fine, suspension or revocation of licence by court. The Philippines indicated that under existing case law (Alfredo Ching vs. Secretary of Justice, G.R. No. 164317, 6 February 2006), a corporation may be charged and prosecuted for a crime if the imposable penalty is fine. Even if the statute prescribes both fine and imprisonment as penalty, a corporation may be prosecuted and, if found guilty, may be fined. According to s.14(e), the penalty of imprisonment ranging from four to seven years and a fine corresponding to not more than 200% of the value of the monetary instrument or property laundered can be imposed upon the covered person, its directors, officers or personnel who knowingly participated in the commission of ML.

40. Section 14 (f) of the AMLA, as amended, provides administrative sanctions, which shall be applied without prejudice to the filing of criminal charges against the persons responsible for the violations. Therefore, parallel criminal and administrative sanctions are possible. Rule XII(A)(2) of the 2016 RIRR specifies that no prior criminal chargers or conviction for predicate crime or ML is necessary for the commencement of civil forfeiture.

41. *Criterion 3.11* - Section 4(d) - (f), of the AMLA contains ancillary offences and s.14 of the AMLA provides sanctions for the same. These include attempt, conspiring to commit ML; aiding, abetting, assisting or counselling the commission of ML, and any act or omission that facilitates ML. The ancillary offence of ‘association’ is not specifically included in s.4. This void could have relevance where ML is associated with a joint criminal enterprise, especially to bring within the offences those who would have initiated or originated the idea of initiating the ML conduct.

Weighting and Conclusion

42. The Philippines mostly meets the requirements in relation to the ML offence. The shortcomings are that tax crimes are not a predicate offence and the lack specific inclusion of “association” in the definition of ancillary offences.

43. **Recommendation 3 is rated largely compliant.**

⁸⁵ transacts, converts, transfers, disposes of, moves, acquires, possesses or uses, conceals or disguises the true nature, source, location, disposition, movement or ownership of or rights with respect to the monetary instrument or property and attempts or conspires to commit ML offences mentioned above

Recommendation 4 – Confiscation and provisional measures

44. The Philippines was rated partially compliant with the former R.3 as the ability to identify and trace property, confiscate or apply provisional measures was not applicable in TF cases. The report also noted the impediments to efficient initial freezing and deficiencies in relation to designated LEAs to request freeze orders and initiate civil forfeiture proceedings.

Criterion 4.1

45. 4.1 (a) and (b) - Provisions for confiscation of property laundered, proceeds of (including income or other benefits derived from such proceeds), or instrumentalities used or intended for use in, ML or predicate offences are contained in s.12 (a) of the AMLA under the civil forfeiture provision. AMLC can file with the appropriate court through the office of the Solicitor General, *ex parte* petition for forfeiture of any monetary instrument or property (belonging to either offender himself or a third person or entity) is in any way related to an unlawful activity or ML offences. S.12 (a) read together with Rule 2, s.1(cccc) of the 2018 IRR where the definition of property covers the instrumentalities used or intended for use in the commission of any unlawful activity. The AMLA does not contain provisions for criminal forfeiture or conviction based confiscation. The Philippines indicate that where civil action for forfeiture is not instituted, civil action is deemed instituted with the criminal action.

46. Forfeiture provisions are available under different legislations related to predicate offences. S.6 of the RA 1379⁸⁶, provides for conviction-based forfeiture of illegally acquired assets of government officers and employees. S.20 of the Comprehensive Dangerous Drugs Act of 2002, provides for confiscation and forfeiture of the proceeds or instruments of the unlawful acts, including the properties or proceeds derived from the illegal trafficking of dangerous drugs. The Revised Forestry Code of the Philippines allows confiscation in favour of the government of the timber or any forest products cut, gathered, collected, removed, or possessed as well as the machinery, equipment, implements and tools illegally used in the area where the timber or forest products are found (s.68).

47. The Philippine Fisheries Code provides number of forfeiture provisions in connection with catch, fishing equipment and fishing vessel etc. Further, s.1113 to 1128 of the Customs Modernization and Tariff Act provides for administrative forfeiture of proceeds or property. S.279 of the National Internal Revenue Code (NIRC) provides confiscation and forfeiture of the proceeds or instruments of crime. However, tax crime is not a predicate offence in the Philippines. Article 45 of the Revised Penal Code stipulates every penalty imposed for the commission of a felony shall carry with it the forfeiture of the proceeds of the crime and the instruments or tools with which it was committed and this Article also serves as a residual capture of other offences.

48. 4.1 (c) - Section 4, 5, 6 and 7 of the Terrorism Financing Prevention and Suppression Act of 2012 criminalises TF and its ancillary offences. S.17 & 18 of the same act sees TF deemed as predicate offences for ML under the AMLA, as amended. This enables civil forfeiture provisions of the AMLA, as amended. Criminal forfeiture provisions are not contained in the Terrorism Financing Prevention and Suppression Act of 2012 and the Philippines indicates that the generic provision in Article 45 of the Revised Penal Code provides coverage.

49. 4.1 (d) - Forfeiture of property of corresponding value is provided under s.12 (c) of the AMLA. According to this provision, when, the monetary instrument or property cannot be located with due diligence or difficult to identify or be located for purpose of forfeiture, court can order the convicted offender to pay an amount equal to the value of the relevant monetary instrument

⁸⁶ An Act Declaring Forfeiture in Favor of the State Any Property Found to Have Been Unlawfully Acquired by any Public Officer or Employee and Providing for the Proceedings Therefor (1955)

or property. In addition, the forfeiture under the above section includes those other monetary instruments or property having an equivalent value (s.12(a) of the AMLA).

50. *Criterion 4.2* - The Philippines has provisions in several of its laws, authorizing relevant LEAs, mainly AMLC to conduct investigations into ML and associated predicate offences subject to forfeiture.

51. *4.2 (a)* - The Philippines has provisions in a number of laws authorizing the relevant LEAs to conduct investigations in order to identify, trace and evaluate property that is subject to forfeiture. Each LEA, including AMLC, has its own powers to collect evidence that would contribute to tracing property that may be subject to confiscation. PNP is empowered to enforce all laws and ordinances, investigate and prevent crimes search and seizure (s.24 of RA 6975) under its general police powers. NBI is mandated to collect evidence to investigate a range of serious offences, including ML, TF and predicate offences based on s.1 of the RA 157 and s.5 of the RA 10867. The PDEA can investigate all violators and other matters involved in the commission of any drug crime (s.84 of RA 9165), which would include related ML. The Bureau of Customs (BOC) is mandated to prevent and suppress smuggling in the country and seize property or evidence (s.216 of RA 10863). The Securities and Exchange Commission (SEC) can investigate violations under the Securities Regulation Act and secure evidence. (s.53).The Bureau of Fisheries (BFAR) to enforce all laws, formulate and enforce all rules and regulations governing the conservation and management of fishery resources(s.65(n) of RA 8550). Intellectual Property Office of the Philippines (IPOPhil) is authorised to enforce IP offences under s.7 (c) of RA 8293.

52. AMLC has authority to issue orders addressed to the appropriate supervising authority or the covered person to determine the true identity of the owner of any monetary instrument or property subject of a covered transaction or suspicious transaction report or request for assistance from a foreign state (s.7 of the AMLA, as amended). Further, they can enlist the assistance of any branch, department etc. of the government owned and control cooperation, in undertaking any anti-money laundering operations (s.7(10) of the AMLA). S.11 of the AMLA, as amended, provides authority to inquire into bank deposits, which allows AMLC to inquire into or examine any particular deposit or investment, including related accounts, with any banking institution or non-bank financial institution, upon order of any competent court based on an *ex parte* application in cases of violations of the AMLA. No court order is required in cases involving activities defined in s.3(i)(1), (2) and (12), and felonies or offenses of a nature similar to those mentioned in those sections, which are punishable under the penal laws of other countries, and terrorism and conspiracy to commit terrorism as defined and penalised under the Human Security Act (R.A. No.9372).

53. Out of the LEAs responsible for investigating predicate offences, only AMLC has power to access bank records. Other LEAs have power to trace other types of properties and can obtain information, under the existing MOA provisions, from the AMLC including financial and banking records. The absence of direct empowerment to access financial information, limits the identification of property subject to confiscation by LEAs.

54. Section 15 of the Ombudsman Act of 1989 provides powers to investigate cases involving government officials and employees. The Office of the Ombudsman has authority to administer oaths, issue subpoena and subpoena duces tecum, and take testimony in any investigation or inquiry, including the power to examine and have access to bank accounts and records. However, judicial pronouncement in *Marquez v. Desierto* (G.R.No. 135882. 27 (2001)) narrowed the power of the OMB to access the bank information during investigations such that they can only access bank information where court proceedings are already under way.

55. *4.2 (b)* - AMLC can file *ex parte* petition in connection with any monetary instrument or property, which is in any way related to predicate offence (s.10 of the AMLA). The Court of

Appeals can issue a freezing order which shall be effective immediately for a period of twenty days. However, within the twenty day period, the Court of Appeals shall conduct summary hearings, with notice to the parties, to determine whether or not to modify or lift the freeze order, or extend its effectivity (s.10 of the AMLA, as amended). In addition, Rule of Procedure in Cases of Civil Forfeiture (s.11, 12 and 15) provides *ex parte* issuance of provisional asset preservation orders, which is comprehensive as it may be maintained until the matter is finally determined by the court. S.11 of the TF Act, provides administrative freezing for 20 days in relation to property or funds connected with financing of terrorism or act of terrorism as outlined at 4.2(a) LEAs responsible for conducting investigations into predicate offence have the authority to seize instruments of crime and some property that may represent evidence of an offence, but would otherwise rely on AMLC powers and court orders under the AMLA.

56. AMLC and OMB lack powers to carry out seizures but are empowered to seek the assistance of other empowered agencies. S.1 of RA 157, as amended by Section 4, 7 and 9 of RA 10867 authorizes the NBI to undertake seizures. Similarly by s.24 of RA 6975 the PNP, by s.84 of RA 9165 the PDEA and s.216 of RA 10863 empowers the BOC to seize smuggled goods and other instruments or evidence of crime, but this does not extend to a comprehensive provision to seize all proceeds of crime.

57. 4.2 (c) - The Philippines does not have any provisions that enable the authorities to take steps to void or prevent actions that prejudice the country's ability to freeze, seize or recover property subject to confiscation.

58. 4.2 (d) - The AMLA and other respective laws related to predicate offences, provide powers to take any appropriate investigative measures. S.7 of the AMLA, as amended, gives a wide range of powers to AMLC to conduct investigations. In addition, s.15 of the Ombudsman Act provides power to administer oaths, issue subpoena and subpoena duces tecum, and take testimony in any investigation or inquiry, including the power to examine and have access to bank accounts and records. However, the latter's access to bank accounts have been restricted by the judicial pronouncement referred to earlier. Furthermore PNP (s.24 of RA 6975, as amended), NBI (s.1 of RA 157, as amended), PDEA (s.84 of RA 9165), SEC (s.5 of RA 8799) and the BOC (sections 215 to 225 of RA 10863) are empowered to take appropriate investigative measures.

59. *Criterion 4.3 - Bona fide* third parties have the rights of claim, in both civil and criminal forfeiture, by a verified petition to seek a declaration that the property subject to forfeiture legitimately belongs to him/her and for segregation or exclusion of the monetary instrument or corresponding property (s.12(b) of the AMLA, as amended). Further, sections 35 to 42 of the Rule of Procedure in Cases of Civil Forfeiture allow bona fide third parties to make claims in respective courts in relation to ML offences. The Rule of Court 19 s.1 of the 1997 Rules of Civil Procedure provides, in general, opportunities for intervention by third parties in civil actions only to leverage relief. It does not extend to cover predicate offences and TF offences. In addition, art.45 of the Revised Penal Code provides that third party persons not liable for offence of felony will not have any property confiscated or forfeited.

60. *Criterion 4.4* - Under the 2018 IRR Rule 32 s.1 (Management of Frozen, Preserved and Forfeited Assets) AMLC must establish mechanisms for managing and/or disposing preserved and forfeited assets (see also ss.19 to 21 of A.M. No. 05-11-04-SC, Rule of Procedure in Cases of Civil Forfeiture read together with AMLC Resolution No. 22, Series of 2018). Whilst a formal mechanism is yet to be established, AMLC has established an asset management group in July 2018 with three officers with appropriate guidelines. Most assets frozen by AMLC are held by the commercial banks and is tracked by AMLC Asset Management Office. Other LEAs have in place appropriate guidelines for managing and control of property seized as evidence. The disposal of confiscated property from all LEAs is handed over and managed by the Bureau of the Treasury

asset management team. However, there is no evidence of a clear mechanism for disposing of property frozen or seized by other LEAs.

Weighting and Conclusion

61. The Philippines has legislative measures for confiscation of a property including freezing or seizing. The identified shortcomings include gaps with respect to seizing a wide range of property that is subject to confiscation, a lack of provisions to enable authorities to void or prevent actions that prejudice the ability to restrain or recover property subject to confiscation as well as practical impediments to LEAs other than AMLC to directly access bank records in tracing assets; and minor gaps with mechanisms for the preservation and management of assets.

62. **Recommendation 4 is rated partially compliant.**

Recommendation 5 – Terrorist financing offence

63. The Philippines was rated non-compliant for Special Recommendation II in its 2009 MER. The main deficiency noted was that terrorism financing was not criminalised as a separate offence. Legislative amendments were the basis for APG's 2012 progress report finding compliance with SR.II to be equivalent to largely compliant.

64. *Criterion 5.1* - The TFPSA criminalises TF on the basis of the UN TF Convention. S.4 makes it an offence to possess, provide, collect, use or make available property, funds or financial service, directly or indirectly, if there is an unlawful and wilful intention that they should be used, or with the knowledge that they are to be used, in full or in part: (a) to carry out or facilitate the commission of any terrorist act; (b) by a terrorist organisation, association or group; and (c) by an individual terrorist. The TFPSA covers all elements of art.2 of the TF Convention and references the treaties annexed to the Convention, all of which the Philippines is a party to.

65. *Criterion 5.2* - Section 4 of the TFPSA confirms that it is sufficient for there to be an unlawful and wilful intention for the funds/assets to be used, or with the knowledge that they are to be used, by a terrorist organisation, association or group, or by an individual terrorist. While it is not explicit that no link is required to a specific terrorist act, s.4(b) and (c) cover instances where there is no link to a specific terrorist act, but where there is the use of funds by a terrorist organisation, association or group, or by an individual terrorist.

66. *Criterion 5.2^{bis}* - The Philippines does not specifically criminalise the financing of travel of individuals for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training.⁸⁷ While the TFPSA IRR, Rule 8(a) penalises any person who makes available any property or funds to a designated person, organisation, association or group of persons may be considered to be broad enough to include providing funds for the purpose of financing travel, it is limited in that it only applied to the provision of funds to those designated under Rule 3.a.5 of the IRR. This rule defines 'designated persons' to include a person, organisation, association or group: (a) designated under the applicable UNSCR, or by another jurisdiction, (b) proscribed under s.17 of the HSA, or (c) whose property or funds are subject to seizure and sequestration under s.39 of the HSA.

67. *Criterion 5.3* - The definition of property in s.3 of the TFPSA is consistent with the definition of funds in the TF Convention, being assets 'however acquired', extending the reach of

⁸⁷ Section 5(E) of the House Bill No. 7141 also known as The Prevention of Terrorism Act of 2018 criminalises travel, attempt to travel, recruitment or assistance of another person to travel, and the facilitation of the travel of another person, to another state or country for the purpose of planning or preparation of, or participation in, terrorist acts, or the providing or receiving of training for terrorism. Under the Bill, the penalty for this activity is life imprisonment without the possibility of parole, or death.

TECHNICAL COMPLIANCE

the TF offence to property acquired through both legitimate and illegitimate means. The definition extends to financial assets, property of every kind, whether tangible or intangible, movable or immovable, and legal documents of any kind, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including but not limited to, bank credits, traveller's cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets.

68. *Criterion 5.4* - Under s.4 of the TFPSA, for an act to constitute an offence it is not necessary for the funds to actually be used to carry out a crime as contained within one of the treaties annexed to the Terrorist Financing Convention, nor is it necessary for the funds or assets to be linked to a specific terrorist act.

2. *Criterion 5.5* - The TFPSA, s.4, provides that 'for purposes of this Act, knowledge or intent may be established by direct evidence or inferred from the attendant circumstances'. Attendant circumstances are the facts surrounding an event.

69. *Criterion 5.6* - Criminal sanctions for the TF offence are found in s.4 of the TFPSA and include imprisonment and fines. The minimum term of imprisonment available is 12 years and one day, and the maximum term is 40 years. The minimum imprisonment term is likely to be dissuasive. In addition to imprisonment, a fine can be imposed of between P500,000 (USD9,500) and P1,000,000 (USD19,000). When compared to sanctions for predicate offences, these criminal sanctions are proportionate, and the pecuniary penalty is high. Overall, the criminal sanctions available for natural persons are proportionate and dissuasive.

70. *Criterion 5.7* - Where the TF offence is found to have been carried out by a corporation, association, partnership or any other type of legal person, criminal liability and sanctions can apply under s.9 of the TFPSA. The criminal sanctions (imprisonment or fine) are imposed upon the responsible officers who participated in or allowed by gross negligence the commission of the crime. This extends to those who knowingly permitted or failed to prevent the commission of the crime. This does not preclude parallel administrative liability and sanctions.

71. It is unlikely however that the fines available under s.4 of the TFPSA, being under USD 10,000, are sufficiently dissuasive to legal persons financing terrorism.

72. *Criterion 5.8* - Under s.5 of the TFPSA it is an offence to attempt to commit a crime under s.4 (financing of terrorism) and s.8 (prohibition against dealing with property or funds of designated persons) of the Act, with the penalty available being two degrees lower than that prescribed for the actual commission of the crime. S.4 also includes a provision making it an offence to organise or direct others to commit financing of terrorism.

73. Section 6 of the TFPSA provides that any person who cooperates in the execution of the TF offence or the conspiracy to commit the TF offence is an accomplice and shall be subject to a penalty one degree lower than that prescribed for the conspirator. Additionally, s.7 of the TFPSA provides for penalty against an 'accessory', being a person who, having knowledge of the TF offence profits from it, assists the principal/s to profit from it, conceals or destroys the effects of the crime, or harbours, conceals or assists in the escape of a principal, shall be subject to a penalty two degrees lower than that prescribed for principals.

74. In relation to 'participating as an accomplice' in an attempted TF offence, the assessment team is of the view that this is not envisaged under the TFPSA. The legislation is specific in relation to the offences, only referring to a person who cooperates in the crime of TF (a s.4 offence) – which is a separate offence in the law to attempted TF – or conspiracy to commit TF. As s.5 clearly

separates conspiracy and attempt, the specific reference to ‘conspiracy’ excludes participating as an accomplice in an attempted TF offence.

75. *Criterion 5.9* - The financing of terrorism is a ML predicate offence in the Philippines under s.17 of the TFPSA.

76. *Criterion 5.10* - The TFPSA has extra-territorial application under s.19, where there is a treaty. The criminal provisions of the TFPSA apply to an individual who:

- is a Philippines national and commits a TFPSA offence outside of the Philippines
- is outside of the Philippines and commits, conspires or plots to commit a TFPSA offence within the Philippines
- is outside of the Philippines and commits a TFPSA offence on board a Philippines ship or plane
- commits a TFPSA offence within an embassy, consulate or diplomatic premises belonging to or occupied by the Philippines Government in an official capacity
- is outside of the Philippines who commits a TFPSA offence against Philippines citizens or persons of Philippines descent, where the citizenship or ethnicity was a factor in the commission of the crime
- is outside of the Philippines and commits a TFPSA offence against the Philippines Government
- is an alien whose extradition is requested under the TF Convention and not extradited to the requesting State.

Weighting and Conclusion

77. The Philippines has not specifically criminalised the financing of travel of individuals for the purpose of terrorist acts and the providing or receiving of terrorist training.

78. **Recommendation 5 is rated largely compliant.**

Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing

79. In its 2009 MER, the Philippines was rated partial compliant with former SR.III. The freezing process under UNSCR 1267 was not ‘without delay’ and allowed judicial discretion over UNSC resolutions. There was no power to freeze, seize or confiscate assets related to TF except in the context of UNSCR 1267 or domestic designation. Further, there were doubts around the length of the freeze and domestic designation pursuant to UNSCR 1373, which did not allow designation of individuals.

Criterion 6.1

80. *6.1 (a)* - The Anti-Terrorism Council (ATC) is the competent authority responsible for proposing persons or entities to the 1267/1989 Committee or 1988 Committee for designation. NICA acts as the ATC’s secretariat.

81. *6.1 (b)* - Rule 24(a) of the IRR to the TF Law assigns the AMLC, in coordination with the ATC and other relevant agencies, to coordinate CFT efforts in the Philippines in cooperation with other nations. This includes identifying targets for UNSCR 1267 designation. A technical working

TECHNICAL COMPLIANCE

group is the mechanism for identifying targets for designation, based on the designation criteria set out in the relevant UNSCRs.

82. 6.1 (c) - The threshold, described by NICA, for proposing a UNSCR 1267 designation is a criminal evidentiary standard, i.e. a court case must have commenced. This requires a higher standard of 'probable cause' rather than 'reasonable grounds' or 'reasonable basis' and is a significant deficiency.

83. 6.1 (d) and (e) - The Philippines advised that its procedures and standard forms for listing are as adopted by the relevant committee. However, the Philippines procedures require as much relevant information and detail as possible, including a statement of case on the basis for the listing and specifying whether its status as a designating state may be made known. No proposals for UNSCR 1267 designation have been made since 2008.

Criterion 6.2

84. 6.2 (a) - For UNSCR 1373 designations, s.17 of the Human Security Act (HSA), as amended by HB No. 7141, states that upon application of the Department of Justice before a Regional Trial Court, an organisation, association or group of persons be declared as a terrorist entity. This includes requests from other countries. S.3(e)(2) of the TF Law and Rule 3(a5) of its IRR affirm that an organisation, association, or group of persons proscribed pursuant to s.17 of the HSA is a designated terrorist entity. There is no mechanism in s.17 of the HSA for an individual to be declared as a terrorist. Notwithstanding this, an individual (or an entity) may be designated a terrorist under s.3(e)(3) of the TF Law and Rule 3(a5) of its IRR. This is possible if their property or funds are subject to seizure and sequestration under s.39 of the HSA.

85. 6.2 (b) - Rule 24 of the IRR of the TF Law requires that AMLC, in coordination with ATC and other government agencies coordinate to identify targets for UNSCR 1373 designation. This includes examining and giving effect to actions initiated under the freezing mechanisms of other countries. The technical working group is the mechanism for identifying targets for designation under s.17 of the HSA.

86. 6.2 (c) - Section 3(e)(1) of the TF Law and Rule 3(a5) of its IRR state that a designated person includes any person or entity designated by another jurisdiction. Rule 22(e) of the IRR, and pursuant to s.54(7) of the HSA, states that designations from other jurisdictions shall be referred from DFA to ATC to determine if designation under s.17 is warranted. There is no stated requirement that a prompt determination be made. Nor that the request is supported by 'reasonable grounds', or 'reasonable basis'. Notwithstanding Rule 3(a5) of the IRR, s.17 of the HSA does not enable an individual designated in another jurisdiction to be designated as a terrorist in the Philippines. However, as with criterion 6.2(a) above, an individual (or an entity) designated by another jurisdiction may be designated a terrorist under s.3(e)(3) of the TF Law and Rule 3(a5) of its IRR. This is possible if their property or funds are subject to seizure and sequestration under s.39 of the HSA.

87. 6.2 (d) - Designation is dependent on the application to the Regional Trial Court. A criminal evidentiary standard of 'probable cause' is required rather than the lower standard of 'reasonable grounds' or 'reasonable basis'. This is a significant deficiency.

88. 6.2 (e) - There are no provisions relating to requesting another country to give effect to actions initiated under the HSA mechanisms.

Criterion 6.3

89. 6.3 (a) - Rule 24(a) of the IRR to the TF Law states that AMLC, in coordination with the ATC and other relevant agencies, shall coordinate all efforts to prevent and suppress terrorism financing in the Philippines and maintain coordination and cooperation with other nations in combating terrorist financing. This includes identifying targets for UNSCR 1267 or UNSCR 1373 designation. In practice, the technical working group is responsible for collecting or soliciting information to identify entities that, based on reasonable grounds, or a reasonable basis to suspect, meet the criteria for designation. Regional intelligence networks can also be utilised. Collection of information is conducted without involvement of or prior notice to the entity.

90. 6.3 (b) - Once an entity has been identified and is being considered for proposal for designation, it is not possible to operate *ex parte* against them. Rather, due notice must be given and the entity should have the opportunity to be heard. As it is not possible to propose an individual for UNSCR 1267 or UNSCR 1373 designation unless their property or funds are subject to seizure and sequestration under s.39 of the HSA, it is not possible to operate *ex parte* against an individual either.

91. *Criterion 6.4* - Section 8 of the TF Law and Rule 8(a) of its IRR prohibit all persons and entities in the Philippines from dealing with property or funds of designated persons and entities, which covers all UN designated persons and entities. S.11 of the TF Law and Rule 11(a) of its IRR authorise AMLC to issue an order to freeze without delay. For UNSCR 1267 designations, a standing court order is provided by AMLC Resolutions TF-01 and TF-02 of 2012 which directs all covered persons and relevant government agencies to freeze without delay the property or funds, including related accounts, of designated persons or entities. In accordance with Rule 15(a) and 22(a) of the IRR, any future UNSCR 1267 designations are automatically covered by this standing order once they have been published on AMLC website. Updates and changes to the list of UNSCR 1267 designations must be immediately transmitted from DFA to AMLC. In practice, AMLC receives updated lists directly from the UN and updates these onto its website and its portal for covered persons within one business day. This means that in some circumstances, such as over a weekend, the requirement to freeze may not take effect without delay.

92. For UNSCR 1373 designations, the same provisions apply. Section 11 of the TF Law and Rule 11(a) of its IRR authorise AMLC to issue a standing court order to freeze without delay. This includes requests from other countries, although without a UNSCR 1373 designation in the Philippines, the standard of proof for a freeze order is 'probable cause'.

Criterion 6.5

93. 6.5 (a) - Rule 8 of the IRR to the TF Law creates an enforceable prohibition on all natural and legal persons from 'dealing' with the property or funds of a designated person or entity. 'Dealing' is defined comprehensively at Rule 3(a4). This prohibition is a *de facto* freezing obligation. In addition, s.16 of the TF Law and Rule 16 of the IRR requires covered persons or relevant government agencies to freeze without delay, the funds or other assets of designated persons and entities upon receipt of a freeze order.

94. 6.5 (b)(i) - Section 3(h) of the TF Law and Rule 3(a10) of the IRR defines property or funds. Property or funds are broadly defined as financial assets, property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, or other income accrued from such funds or other assets. The prohibition on dealing or freezing action does not require that funds are linked to terror acts, etc.

TECHNICAL COMPLIANCE

95. 6.5 (b)(ii) – Section 8 of the TF Law and Rule 8(a) of its IRR extends the *de facto* freeze to funds owned or controlled, directly or indirectly, but does not expressly cover funds jointly owned or controlled.

96. 6.5 (b)(iii) – Section 8 of the TF Law and Rule 8(a) of its IRR extends the *de facto* freeze to funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities.

97. 6.5 (b)(iv) – Section 11 of the TF Law and Rule 11(a) of its IRR authorise AMLC to freeze covers property or funds that are in any way related to terrorism or TF. This includes funds or other assets of persons and entities acting on behalf of, or at the direction of, designated persons or entities. It is not clear that property can be seized by AMLC under any statutory provision.

98. 6.5 (c) – Section 8 of the TF Law prohibits any person from making available any property or funds, or financial or other related service to a designated person or entity. Rule 8(a) of its IRR also prohibits any person from dealing with property or funds, directly or indirectly, wholly or jointly, for the benefit of designated persons. This provision does not extend to persons and entities acting on behalf of, or at the direction of, designated persons or entities.

99. 6.5 (d) – Rule 15(a) of the IRR provides that a list of designated persons should be published on the DFA and ATC websites. For UNSCR 1267 designations, Rule 22(a) of the IRR states that immediately upon receipt of the list of designations, AMLC shall adopt and publish the list and order the freezing without delay of property or funds of the persons, organisations, associations or groups of persons named in the list. For UNSCR 1373 designations, the list of persons, organisations, associations or groups of persons whose property or funds are subject to seizure, must be disseminated to all covered persons.

100. 6.5 (e) – Rule 16(c) of the IRR holds that within 24 hours, covered persons must submit by personal delivery a detailed written return specifying assets frozen or actions taken in compliance with the freeze order. Rule 16(d) of the IRR also requires covered persons to report any and all attempted dealings with regards to the frozen property or funds within 24 hours from such attempt. This obligation does not extend to real estate agents.

101. 6.5 (f) – Rule 11(b) of the IRR provides that if a freeze has been effected based on mistaken identity, no administrative, criminal or civil proceedings shall lie against any person or entity for effecting a freeze in the absence of bad faith.

Criterion 6.6

102. 6.6 (a), (d) and (e) – Rule 23(b) of the IRR provides that a petition for de-listing may be filed with the appropriate UNSC Sanctions Committee. Grounds for de-listing are mistaken identity, relevant and significant change of facts of circumstance, newly-discovered evidence, death of designated person, dissolution or liquidation of designated persons, or any other circumstance which would show that the basis for designation no longer exists. Pursuant to Rules 23(c) and (d), submissions for de-listing can occur through the Office of the Ombudsperson or through the Focal Point.

103. 6.6 (b) and (c) – There is no prescribed mechanism to de-list and unfreeze funds or assets of persons or entities designated pursuant to UNSCR 1373. The Philippines advised that there have been no challenges to listing, but if there were, this would occur through the courts.

104. 6.6 (f) – Rule 23(a) of the IRR provides that persons or entities whose property or funds were frozen may file a verified petition with AMLC on the basis of mistaken identity for the lifting of a freeze order.

105. 6.6 (g) - Rule 23(e) holds that where designated persons or entities are de-listed, AMLC or ATC shall immediately issue a resolution or notice that the person has been de-listed and the freeze order has been lifted. The resolution shall be disseminated for publication and posted on the websites of AMLC, ATC and DFA and if needed, delivered by personal service.

106. *Criterion 6.7* - Section 13 of the TF Law and Rule 13 of the IRR contain provisions for humanitarian exemptions and procedures to access frozen funds or assets for monthly family needs. This requires a petition to be filed with the Court of Appeals for an Order allowing such withdrawal. S.14 of the TF Law and Rule 14 of the IRR to the TF Law exempt the Public Attorney's Office from violation of the TF Law if providing legal services to designated persons. These provisions are in keeping with UNSCR 1452.

Weighting and Conclusion

107. There are shortcomings relating to the evidentiary standard of proof for making a UNSCR 1267 proposal for designation, as well as for domestic designations under UNSCR 1373. For UNSCR 1373 designations, there are further shortcomings relating to the ability to operate *ex parte* against an individual or entity proposed for designation. In combination, these moderate shortcomings significantly affect the Philippines' ability to implement TFS.

108. **Recommendation 6 is rated partially compliant.**

Recommendation 7 – Targeted financial sanctions related to proliferation

109. Targeted financial sanctions related to proliferation is a new requirement added to the FATF Recommendations in 2012 and so it was not assessed in the Philippines' 2009 MER.

110. *Criterion 7.1* - The Philippines does not implement targeted financial sanctions without delay to comply with the UNSCRs that relate to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing.

111. Rule 19, s.6.5 of the IRR amended in Nov. 2018 requires covered persons to secure the consent of their customers to be bound by obligations set out in the relevant UNSCR on PF including the freezing and unfreezing actions as well as prohibitions from conducting transactions with designated persons and entities. Subsection C806.2 of BSP CL 706 (as amended by CL 950 and 1022) require BSP supervised FIs to adopt appropriate policies and procedures to implement TFS relating to PF and to report to AMLC the actions taken in compliance with the prohibition requirements, including attempted transactions. While these measures do not establish an asset freezing mechanism, they will support a framework once established.

112. *Criterion 7.2* - The Philippines does not have any provisions which obligate natural and legal persons to freeze the funds and other assets of designated persons or entities. Further, there is no provision which establishes the legal authority and identifies competent authorities for implementing and enforcing targeted financial sanctions related to PF.

113. *Criterion 7.3* - There are no legislative provisions imposing relevant obligations on FIs and DNFBPs and therefore has no measures for monitoring or ensuring compliance by covered persons.

114. *Criterion 7.4* - There is no publicly known procedure to submit de-listing requests of those who do not or no longer meet the criteria of designation, including a procedure to unfreeze funds or assets in the case of false positives or a procedure to authorise access to funds or access in accordance to the relevant procedures in the UNSCRs.

TECHNICAL COMPLIANCE

115. *Criterion 7.5* - In the absence of freezing obligations, there are no relevant measures in place to permit the addition of interest or other earnings due, or to make a payment due under a contract entered into prior to designation.

Weighting and Conclusion

116. The Philippines does not have specific measures in place to implement targeted financial sanctions related to proliferation of WMD.

117. **Recommendation 7 is rated non-compliant.**

Recommendation 8 – Non-profit organisations

118. In its 2009 MER, the Philippines was rated partially compliant with former SR.VIII. Not all NPOs were licensed or registered. No assessment of the types of NPOs at risk of TF had been undertaken.

Criterion 8.1

119. *8.1 (a)* - Section 1.3.6 of SEC Memorandum CN. No. 15, series of 2018 (SEC 2018 NPO Guidelines) continues the definition of NPO from previous SEC memorandums. An NPO is defined as “an SEC-registered Non-Stock Corporation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for carrying out of other types of good works”. These activities align with the activities in the FATF definition of NPO.

120. In October 2018, the Philippines completed an assessment of its NPO sector to identify the features and types of registered NPOs likely to be at risk of TF abuse. This only considered those organisations that are registered with SEC as NPOs. The types of registered NPO most at risk of TF abuse are assessed to be service type NPOs that provide charitable, social development, humanitarian disaster relief or educational activities.

121. As at 31 December 2017, there were 101,843 NPOs in the Philippines registered with SEC. Of these registered NPOs, 19,511 were classified as religious organisations and 13,139 were classified as Education NPOs, both of which are service type NPOs. A further 11,734 were classified as ‘Foundations’. S.1.3.4 of the SEC 2018 NPO Guidelines define a ‘Foundation’ as ‘a non-stock, non-profit corporation established for the purpose of extending grants or endowments to support its goals or raising funds to accomplish charitable, religious, educational, athletic, cultural, literary, scientific, social welfare or other similar objectives’. As per SEC’s earlier Memorandum CN No. 8 of 2006, an NPO may register as a Foundation if it has initial capital of at least PHP1 million (approx. USD 19,000) and complies with additional reporting requirements to SEC (which were later relaxed in 2016 by SEC Memorandum CN No 15 of 2016). Only registered Foundations are able to use the word ‘Foundation’ in their corporate name and when describing their NPO activities.

122. Of the 101,843 registered NPOs, there are a further 52,917 NPOs that have no clear classification. There is no clear data available on what type of NPO activities they undertake.

123. *8.1 (b)* - The October 2018 assessment of the NPO sector identifies the nature of the threats posed to higher risk registered NPOs as the diversion of funds to support terrorist entities and the exploitation of legitimate NPOs as a conduit for TF.

124. *8.1 (c)* - The October 2018 assessment of the NPO sector includes a review of the adequacy of the measures, laws and regulations to address the risks of TF abuse relating to higher

risk NPOs. It states that the regulatory framework and supervision is generally effective, although enforcement is an issue.

125. 8.1 (d) - The October 2018 assessment of the NPO sector is recent. As such there has been no opportunity for a review or reassessment of the relevant issues over time.

Criterion 8.2

126. 8.2 (a) - Registration with SEC is not required for a NPO to exist; however it is required to obtain a legal personality as a NPO and be eligible to open bank accounts, to enter into contracts and to raise or receive funds. In November 2018, the SEC 2018 NPO Guidelines were released to promote accountability, integrity and public confidence in the administration and management of registered NPOs, and to protect NPOs from ML/TF abuse. The 2018 NPO Guidelines require all registered NPOs to establish a system that will enable them to know where their funds are coming from, know who their beneficiaries are, ensure funds are used for the purpose intended and report any fact that gives rise to suspicion of ML/TF.

127. The SEC 2018 NPO Guidelines also require all registered NPOs to file a mandatory disclosure within six months. This must include information about their objectives, activities, funds, location and key personnel. Requirements for medium or high risk NPOs (to be assessed by SEC) then include annual audited financial statements, a sworn statement relating to the source and amount of funds, programs and activities planned, an internal audit system, participating in an outreach program and background checks on officers and trustees. Audits are conducted by SEC on a case by case basis.

128. In addition to the requirements to register with the SEC, service type NPOs that provide social welfare and development programs (who are identified as a type of NPO at higher risk of TF abuse) must also be registered, licensed and/or accredited with DSWD. This requires annual accomplishment forms and audited financial statements to be submitted to DSWD (see DSWD AO. No. 16, series of 2012 mandated by RA4373, as amended by RA5175 and by PD603).

129. Registered NPOs are also able to join PCNC. PCNC is a self-regulatory body designated to prescribe rules and standards and accredit NPOs as charitable “donee” institutions for favourable tax treatment. The October 2018 assessment of the NPO sector states that 91% of PCNC accredited NPOs are service type NPOs (who are identified as a type of NPO at higher risk of TF abuse).

130. The Solicitation Permit Law (RA4075, as amended by PD1565) is in place to promote accountability and integrity in the NPO sector. The law mandates DSWD to regulate fund drives, public solicitations and donations for charitable or public welfare purposes. DSWD Memorandum CL. No. 17, series of 2014, requires ‘any person, corporation, organisation or association desiring or intending to conduct solicitation activities for public welfare and charitable purposes’ to obtain a solicitation permit from DSWD to conduct fund-raising activities. While there is an exemption for fund raising for religious purposes, LGUs have the right to issue their own ordinances regarding the conduct of solicitation drives to fund raise for religious purposes.

131. 8.2 (b) and (c) - The Philippines has undertaken outreach and education programmes with the NPO sector to promote good governance and integrity. Both AMLC and SEC have conducted seminars and held meetings with NPOs and other stakeholders. This has been conducted with the types of NPOs most at risk of TF abuse and has included content to raise awareness about the potential vulnerabilities of NPOs to TF. However, there has not been any sustained outreach with the donor community to raise and deepen awareness of TF abuse. Nor has significant work been undertaken with NPOs to develop and refine best practices to address TF risk and vulnerabilities.

TECHNICAL COMPLIANCE

132. 8.2 (d) - The SEC 2018 NPO Guidelines require NPOs to have a policy of financial accountability and transparency. AMLC promotes the Guideline, including the use of regulated financial channels during regular meetings with the NPO sector, including with DSWD, PCNC and other stakeholders such as CODE-NGO (a coalition of NGOs). Foundations are required to deposit all funds in a banking institution regulated by BSP (s.8 of SEC Memorandum CN. No. 8 of 2006). This is also required by PCNC as part of its accreditation process. Further, for any funds raised under a Solicitation Permit (s.6.5.2 of DSWD Memorandum CN. No. 17 of 2014), requires that the funds be deposited in a banking institution regulated by BSP and in the name of the person, corporation, organization or association to whom the permit was issued. As noted in criterion 8.2(a) above, this in itself requires registration with SEC (and compliance with the SEC 2018 NPO Guidelines) and the opening and use a bank account. In combination, these measures encourage NPOs to conduct transactions via regulated channels wherever feasible.

133. *Criterion 8.3* - The NPOs registered with SEC include the substantial majority of the Philippine NPO sector in terms of financial resource (on the basis that most unregistered NPOs are small community based organisations). Further, a significant share of the registered NPO sector (in terms of financial resource) is subject to the additional requirements imposed by SEC on Foundations, and/or the separate registration, licensing and accreditation processes of DSWD and PCNC. Notably, those registered NPOs that have obligations to DSWD (and many also to PCNC) include service type NPOs providing social welfare and development programs, which are identified as of higher risk of TF abuse.

134. In addition to this existing regulatory framework, the Philippines has recently undertaken a formal assessment of the TF risks in the NPO sector and the SEC 2018 NPO Guidelines have taken effect. While there are still knowledge gaps regarding the composition of the NPO sector, the Philippines is taking steps towards a risk based approach to its supervision or monitoring of those registered NPOs at risk of TF abuse.

135. No formal assessment has been undertaken of the risk of TF abuse of NPOs that are not registered with the SEC. However, some controls are in place to mitigate the risk of abuse (including for TF) for such NPOs. These include the requirements of the Solicitation Permit Law.

Criterion 8.4

136. 8.4 (a) - SEC, DSWD, PCNC all undertake monitoring of NPOs as part of their respective registration, licensing and accreditation processes. This covers a substantial majority of the NPO sector in terms of financial resource, with significant monitoring of many of those registered NPOs that are determined most at risk of TF abuse. Triggers for monitoring include complaints, violating of reporting requirements and/or findings of examinations and review of documents. With the completion of the October 2018 assessment of the NPO sector and the SEC 2018 NPO Guidelines taking effect, monitoring of the specific requirements of this Recommendation is commencing. For unregistered NPOs, there are controls in place that restrict and activities mitigate the risk of abuse (including for TF).

137. 8.4 (b) - Chapter 11 of the SEC 2018 NPO Guidelines states that failure to comply with annual reporting requirements may result in revocation of a NPO's registration with SEC. Further, that non-compliance with SEC Rules by a NPO may result in a fine of no less than PHP10,000 (approx. USD 190) and not more than PHP1,000,000 (approx. USD 19,000), which can be extended by PHP2,000 (approx. USD 38) per day of violation. These penalties are without prejudice to legal action that may be available under other laws. DSWD AO No.16, series of 2012, contains provisions for suspension or revocation of registration, license or accreditations where there is non-compliance with DSWD requirements. DSWD MC No. 16, series of 2018, contains penalties and sanctions for NPOs providing social welfare and development programs without

the appropriate registration/license as well as revocation of the registration, accreditation, or license issued to NPOs found to have been involved in money laundering and terrorist financing.

138. For those NPOs that are not registered with SEC, there are penalties that can be imposed if the controls in place to mitigate abuse (including for TF) are violated, including under the Solicitation Permit Law. There are also penalties under the TF Law.

Criterion 8.5

139. *8.5 (a)* - Chapters 9 and 10 of the SEC 2018 NPO Guidelines enable SEC to investigate, cooperate and share information about NPOs with LEAs, other government agencies and enter into agreements with self-regulatory organisations and private organisations. AMLC also coordinates with SEC as the primary registrar. AMLC has 27 MOAs with law enforcement and government agencies that cover TF offences and enable cooperation, co-ordination and information sharing between appropriate authorities. AMLC also meets regularly with DSWD, PCNC and other stakeholders such as CODE-NGO.

140. *8.5 (b)* - AMLC is the lead agency in investigating TF and has ongoing capacity building to achieve its investigative expertise. S.10 of the TF Law authorises AMLC, either on its own initiative or at the request of the ATC, to investigate property or funds that are in any way related to TF or acts of terrorism. These provisions apply to any circumstance in which a NPO is suspected of being exploited by, or involved in, terrorist activity or TF. S.10 also states that AMLC may enlist the assistance of any other branch, department, bureau, office, agency or instrumentality of the government, including government-owned and controlled corporations in undertaking measures to counter FT. This includes use of personnel, facilities and resources. These provisions are broad and ensure that all expertise, resource and capability as is necessary can be utilised to combat TF.

141. *8.5 (c) and (d)* - Chapter 9 of the SEC 2018 NPO Guidelines enables SEC, as the primary registrar of NPOs, to pursue and implement effective cooperation and coordination through information and resource sharing with LEAs and government agencies. This enables full access to information on the administration of particular NPOs (including financial and programmatic information) when required, including during the course of an investigation. Further, the provisions set out in (a) and (b) above ensure that, where there is suspicion or reasonable grounds to suspect links between a NPO and TF or other forms of terrorist support, any information held by either SEC, DSWD, PCNC or AMLC may be promptly shared with competent authorities in order to take preventative or investigative action.

142. *Criterion 8.6* - Section 9(3) of the SEC 2018 NPO Guidelines requires SEC to establish an effective capacity to respond to international requests for information about NPOs of concern (in accordance with existing laws and the rules and regulations of SEC and AMLC). Section 7(8) of the AMLA also authorises AMLC to receive and take action in respect of requests from foreign states for information regarding their AML/CFT matters. This includes requests regarding NPOs suspected of involvement in TF or other forms of terrorist support. AMLC can share, spontaneously or upon request, information or provide assistance to foreign counterparts. AMLC also has 41 MOUs with other FIUs, which cover TF offences.

Weighting and Conclusion

143. The Philippines has a framework in place to protect its NPO sector from TF abuse. Minor Targeted risk based supervision or monitoring of the NPO sector has commenced, although there are still knowledge gaps regarding the composition of the NPO sector relating to both registered and unregistered NPOs.

144. **Recommendation 8 is rated largely compliant.**

Recommendation 9 – Financial institution secrecy laws

145. In its 2009 ME, the Philippines was rated partially compliant with former R.4. The previous MER noted banking secrecy laws that inhibit competent authorities obtaining necessary information regarding client accounts and to share such information. The Philippines subsequently achieved progress equivalent to largely compliant on this recommendation by revising the AMLA to empower AMLC to access bank records in all cases where they are conducting inquiries into ML, TF or a predicate crimes, including on behalf of other LEAs.

146. *Criterion 9.1* - Section of RA No. 1405 (Law on Secrecy of Bank Deposits) requires that all deposits and investment in government bonds of whatever nature with the banks or banking institutions in the country are considered absolutely confidential and may not be examined, inquired or looked into by any person or government authorities. The secrecy protects all information related to the deposits including customer identification documents. Similar secrecy provision is also set out in Section 8 of RA No. 6426 (The Foreign Currency Deposit Act) for bank deposits in foreign currencies.

147. The secrecy provisions do not apply (a) when there is written consent from the depositors; (b) in impeachment cases; (c) upon order of the court in bribery cases or dereliction of duty of public officials; and (d) cases where the money deposited is the subject of litigation. Further, Section 24 of the AMLA expressly amended the bank secrecy laws insofar as they are inconsistent with the AMLA. The AMLA relieves banks from violations of the bank secrecy and tipping-off when reporting information related to bank accounts in covered transactions and suspicious transactions to AMLC.

148. AMLC is able to obtain bank records for its use and for the use of other competent authorities for intelligence and regulatory purposes based on s.7(2) read together with s.24 of the AMLA (s.24 of the AMLA expressly amended the bank secrecy laws insofar as they are inconsistent with the provisions of the AMLA). These provide a basis for AMLC to order covered institutions to determine the true identity of the owner of any monetary instrument or property subject of a CTR or STR, or subject of a request from a foreign jurisdiction, or believed by the Council on the basis of substantial evidence to be related to proceeds of an unlawful activity.

149. Section 1.8.2 of the 2018 IRR requires covered persons to immediately act on such a request, submit certified true copies of the records of identification and documents within five working days. Further, s.1.8.2, Rule 6 of the 2018 IRR requires the request or order to be kept confidential in order to prevent tipping-off.

150. Section 11 of the AMLA allows AMLC to conduct inquiry and examine bank account information for evidentiary purposes. S.11 requires an evidentiary threshold of 'probable cause' to obtain information from banks through a court order for all crimes except kidnapping for ransom, certain drug offences, hijacking, destructive arson, murder, terrorism and conspiracy to commit terrorism. For these crimes, AMLC can access bank account information, through an AMLC Resolution issued for that purpose, without need of a court order. For court-authorized bank inquiry, the Court of Appeals, shall act on the application from AMLC within 24 hours. Other investigating authorities must request bank information (including CDD) from AMLC.

151. AMLC is the only investigating authority that has the power to identify whether natural or legal persons hold or control accounts (c.31.3). Other competent authorities must utilise MOUs with AMLC to obtain such information. There is no requirement in AMLC's MOUs/MOAs with other agencies to provide requested information in a timely manner.

152. AMLC and BSP are the only competent authority able to obtain CDD records from banks to access any available beneficial ownership information (c.24.6). If AMLC's database holds a CTR

or STR relevant to the target, then it can obtain CDD information in a timely manner from the CTR/STR to determine beneficial ownership. Relying on AMLC's powers to obtain up to date CDD information based on an order under s.7 of the AMLA may, in practice, impede other competent authorities from determining information on beneficial ownership of a company in a timely manner.

153. Section 10 of the TFPSA provides AMLC the power to examine bank deposits or foreign currencies deposits in TF investigation without requiring a court order.

154. AMLC has the power to provide bank account information (obtained directly or via court order) to foreign counterparts, through international information exchange mechanisms (i.e. ESW, direct written request to AMLC under MOUs/MOAs, or request through local competent authorities that have MOA/MOUs with AMLC). The MLATs which the Philippines has entered into with foreign counterparts do not permit refusal of MLA due to bank secrecy (see c.37.4).

155. Section VI of AMLC Resolution No. 40 Series of 2018 decides that AMLC will not disclose information related to a domestic PEP during an election period (i.e. from when an election is called), but does not prohibit the same information from being shared after the election period⁸⁸. The provision may cause a delay in information sharing with domestic competent authorities and timely execution of information request for foreign counterparts (R.40) however it does not impede AMLC's abilities to exchange information internally between its FIU and LEA functions (namely FIAG and FCIG) during the restricted period.

156. BSP can check AML compliance during the course of its periodic or special examination⁸⁹ (s.11 of AMLA), and Rule 11 of the 2018 IRR further stipulates the BSP can examine bank accounts for such purpose. Under s.9(a) of the AMLA, BSPs access to customer identification documents for non-checking numbered bank accounts is limited to determining the existence and true identity of owners.

157. The Ombudsman Office (OMB) has the power to subpoena bank deposit information pursuant to s.15 of RA No. 6770, however this is limited to situations where there is a pending case before a court against the account holder. Section 6(F) of RA No.10021 provides that BIR can access bank records limited to civil affairs and information exchange with foreign counterparts.

158. Section 4(e) and (f) of the Data Privacy and Protection Law (RA No.10173) exempts government authorities from the data privacy restriction and allows access of personal data in order for the BSP, law enforcement and regulatory agencies to exercise their mandated functions constitutionally and statutorily. The bank secrecy exemption also permits FIs to disclose information necessary to comply with the AMLA.

159. The bank secrecy legislation does not fully impede the transmission of information between financial institutions in R.13, 16 and 17. BSP has the power to disclose information of a confidential nature to other domestic supervising authorities when there is proper authorisation by the Monetary Board or the Governor of BSP (see c.40.13), however, does not include those covered under bank secrecy.

⁸⁸ Common practice is for elections to be held every 3 years and for the election period to run for 120 days. The Philippine Constitution sets out the term of the President (Article VII, Section 4) and Senators (Article VI, Section 4) as 6 years. There are elections every 3 years to replace half the Senators, as when the Constitution took effect half had served for only 3 years (Article XVIII, Section 2). The term of members of the House of Representatives (Article VI, Section 7) and elective local officials in various LGUs (Article X, Section 8) is 3 years. Synchronised elections every 3 years have been adopted as a matter of policy.

⁸⁹ The power for BSP to conduct periodic or special examination is set out in Section 25 of RA7653 (also see c.27.2).

Weighting and Conclusion

160. Philippines has confidentiality provisions protecting information related to deposits and investment in government bonds of whatever nature with the banks or banking institutions except for AML/CFT specific activities. AMLC is the primary LEA able to lift secrecy and share bank records with other competent authorities. AMLC does not share bank account information (directly or via court order) to local competent authorities or foreign counterparts during an election period if the information relates to a PEP. The bank secrecy legislation does not fully impede the transmission of information between financial institutions in R.13, 16 and 17. The centralisation of the function of lifting bank secrecy with AMLC may result in some practical delays with or hesitancy of other competent authorities seeking or obtaining bank records, but these implementation concerns are covered in the relevant immediate outcomes.

161. **Recommendation 9 is rated largely compliant.**

Recommendation 10 – Customer due diligence

162. The Philippines was rated partially compliant with former R.5. The main deficiencies noted were (i) no specific requirement to identify the natural person exercising ultimate effective control, (ii) no specific requirement by BSP and SEC that CDD be applied to existing customers on the basis of materiality and risk and that additional CDD be conducted at appropriate times.

Financial institutions

163. The coverage of financial institutions is set out in the definition of ‘covered person’ in s.3 of the AMLA. Covered persons include banks, non-banks, quasi-banks, foreign exchange dealers, money changers, remittance and transfer companies, other similar entities and all other persons and their subsidiaries supervised or regulated by BSP.⁹⁰ Covered persons also include pre-need companies and all other persons supervised or regulated by IC. Covered persons also include (i) securities dealers, brokers, salesman, investment houses and other similar persons managing securities or rendering services as investment agent, advisor or consultant, (ii) mutual funds, close-end investment companies, common trust funds and other similar persons, and (iii) other entities administering or otherwise dealing in currency, commodities or financial derivatives based thereon, valuable objects, cash substitutes and other similar monetary instruments or property supervised or regulated by SEC.

164. The definition of ‘covered person’ meets the requirements of the FATF definition of ‘financial institution’ except for persons that engage in lending or financial leasing (in the absence of engaging in any other financial activities). In the Philippines, there are 681 financing (including financial leasing) companies regulated under the Financing Company Act of 1998 (RA 8556), and 2,535 lending companies regulated under the Lending Company Regulation Act of 2007 (RA 9474). Under s1.2.4 of the SEC 2018 Guidelines, those financing companies and lending companies that have more than 40% foreign equity or a paid-up capital of PHP10 million (approx. USD 190,500) or more are declared as covered persons. There are 431 financing companies and 76 lending companies that meet this threshold. This results in a scope gap from the FATF definition of ‘financial institution’ of 250 financing companies and 2,459 lending companies. This scope gap is minor when considered in context, and the small size of the economic activity that these financing and lending companies engage in.

⁹⁰ Pawn shops and trust entities are also covered persons under AMLA supervised by BSP. For trust entities, please refer to Recommendation 22 – DNFBPs.

Law, regulation and Enforceable means

165. The CDD principle is set out in law, the AMLA, and specific requirements are set out in the IRR, which constitutes enforceable means as per the FATF definition.⁹¹ Rule 6(1) of the IRR enables AMLC to impose sanctions for violations of the AMLA and IRR. The CDD principle set out in law is as follows:

Customer Identification. - Covered institutions shall establish and record the true identity of its clients based on official documents. They shall maintain a system of verifying the true identity of their clients and, in case of corporate clients, require a system of verifying their legal existence and organizational structure, as well as the authority and identification of all persons purporting to act on their behalf. The provisions of existing laws to the contrary notwithstanding, anonymous accounts, accounts under fictitious names, and all other similar accounts shall be absolutely prohibited. Peso and foreign currency non-checking numbered accounts shall be allowed.

166. Rule 16(1) of the IRR states that covered persons must comply with AML/CFT guidelines issued by their supervisor. Rule 7(2) & (4) of the IRR empowers supervisors to issue AML/CFT guidelines to their sectors to complement the provisions of the IRR, issue rules on AML/CFT compliance checking, and also take enforcement actions to correct AML/CFT deficiencies. Rule 26(6) of the IRR empowers supervisors to formulate rules on the imposition of enforcement actions for violations of their respective circulars and orders. Therefore, guidelines, circulars and orders issued by supervisors are also enforceable means as per the FATF definition (that can be enforced by a supervisor over a covered person in its sector). Sanctions for violations of AML/CFT requirements not contained in a supervisor's respective guidelines, circulars and orders may only be imposed by AMLC (including on referral from a supervisor as per Rule 26(6) of the IRR).

General requirements

167. *Criterion 10.1* - Section 9(a) of the AMLA prohibits anonymous accounts and accounts under fictitious names, but allows peso and foreign currency numbered accounts⁹². BSP may conduct annual testing solely limited to the determination of the existence and true identity of the owners of such accounts. Rule 17(1) of the IRR prohibits anonymous accounts, fictitious name accounts and numbered accounts, except for non-checking numbered accounts.

168. The BSP Rules also prohibits anonymous accounts, accounts under fictitious names, numbered accounts and all other similar accounts (X806.2(q)/4806Q.2(q) MORB/MORNBFI). The BSP Rules state no peso and foreign currency numbered accounts shall be allowed without the true and full identity and existing of customers and applying enhanced CDD (X806.2(p)/4806Q.2(p) MORB/MORNBFI). The SEC and IC Guidelines also prohibit anonymous and fictitious name accounts and state accounts must be obtained only in the name of the holder (SEC: s5.A.14 2018 Guidelines, IC: s44 CL. 2018-48).

*When CDD is required**Criterion 10.2*

169. *10.2 (a)* - While there is no explicit provision requiring CDD to be undertaken when establishing a customer relationship, it is implied by Section 9(a) of the AMLA which requires 'covered institutions' to establish, record and verify the identity of customers. Under s.3 of the AMLA, the term 'covered institution' was amended by RA10365 to 'covered persons, natural or juridical'. Rule 2(1)(z) of the IRR defines 'customer/client' as any person who keeps an account, or otherwise transacts business with a covered person. Similar provisions are contained in the

⁹¹ As permitted by the footnote to R.10

⁹² The identity of numbered accounts are available to certain officers in the bank and the regulator. The system was established to help to protect depositors from kidnap for ransom and extortion.

TECHNICAL COMPLIANCE

BSP, SEC and IC Rules and Guidelines (BSP: X806(b)/4806Q(b) MORB/MORNBFI, SEC: s5.A.3 2018 Guidelines, IC: s21 CL. 2018-48).

170. *10.2 (b)* - Rule 18(1) of the IRR states that CDD must be conducted on any occasional transaction above PHP100,000 (approx. USD 1900). This includes situations where the transaction is carried out in two or more operations that appear to be linked. Similar provisions are contained in the BSP Rules, although for remittance and money changing, there is a lower occasional transaction value of PHP5,000 (approx. USD 95) (X806(b)/4806Q(b) MORB/MORNBFI). There are also similar provisions in the IC Guidelines (IC: s21 CL. 2018-48). While the SEC Guidelines do not contain specific requirements relating to occasional transactions, there are provisions relating to covered transactions of PHP500,000 (approx. USD 9,500) or more. The definition of 'covered transaction' is broad enough to include occasional transactions outside a business relationship. 'Covered transactions' must be reported to AMLC. To be able to report a covered transaction, a FI must conduct CDD (SEC: s5.A.3, s7.3 2018 Guidelines).

171. *10.2 (c)* - Rule 19(6) of the IRR states that FIs shall not accept instructions for wire transfers unless CDD has been conducted. These provisions are also included in the BSP Rules (X806.2(j)/4806Q.2(j) MORB/MORNBFI). The wire transfer provisions do not apply to SEC and IC supervised institutions.

172. *10.2 (d)* - Rule 18(1) of the IRR requires CDD when there is suspicion of ML/TF regardless of any exemptions or thresholds referred to elsewhere in the IRR. BSP Rules and IC Guidelines also specify that CDD must be conducted when there is any suspicion of ML/TF (BSP: X806(b)/4806Q(b) MORB/MORNBFI, IC: s21 CL. 2018-48), but the SEC 2018 Guidelines do not.

173. *10.2 (e)* - Rule 18(1) of the IRR requires CDD when there are doubts about the veracity or adequacy of previously obtained identification information and/or data. There are similar provisions contained in the BSP, SEC and IC Rules and Guidelines (BSP: X806(b)/4806Q(b) MORB/MORNBFI, SEC: s5.A.4 2018 Guidelines, IC: s21 CL. 2018-48).

Required CDD measures for all customers

174. *Criterion 10.3* - Section 9(a) of the AMLA requires FIs to establish, record and verify the identity of customers based on official documents. Rule 2(1)(z) of the IRR defines 'customer/client' as any person who keeps an account, or otherwise transacts business with a FI. Rule 18(3) of the IRR requires FIs to 'identify and record the true identity of their customers, whether permanent or occasional, and whether natural or juridical person, or legal arrangement'. Rule 18(4) of the IRR requires FIs to implement and maintain a system of verifying the true identity of their clients using reliable and independent sources, documents, data, or information. The BSP, SEC and IC Rules and Guidance also contain provisions requiring identify verification using official documents or other reliable, independent source documents, data or information (BSP: X806(a)/4806Q(a) MORB/MORNBFI, SEC: s5.A.3 2018 Guidelines, IC: s24 CL. 2018-48).

175. *Criterion 10.4* - Section 9(a) of the AMLA requires that the authority and identity of all persons acting on behalf of the customer must be verified when the customer is a 'corporate client', which is not defined in the AMLA. It is not clear that a requirement to identify the authority and identity of a person acting on behalf of the customer applies to all types of customer, such as natural persons, legal arrangements or juridical persons. AMLA, Rule 18(5) of the IRR requires verification of the authority and identity of a person acting on behalf of a customer. This requirement is also contained in the BSP, SEC and IC Rules and Guidelines (BSP: X806(a)/4806Q(a) MORB/MORNBFI, SEC: s5.A.3 2018 Guidelines, IC: s22 CL. 2018-48).

176. *Criterion 10.5* - Beneficial owner is defined in Rule 2(1)(l) of the IRR as:

'any natural person who 1) ultimately owns or controls the customer and/or on whose behalf a transaction or activity is being conducted; or 2) has ultimate effective control over a juridical person or legal arrangement; or 3) owns at least, twenty percent (20%) shares, contributions or equity interest in a juridical person or legal arrangement'. Rule 18(6) of the IRR requires FIs to identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source, such that the FI is satisfied it knows who the beneficial owner.

There are similar provisions contained in the BSP, SEC and IC Rules and Guidelines (BSP: X806(a)/4806Q(a) MORB/MORNBFI, SEC: s5.A 2018 Guidelines, IC: s22 CL. 2018-48).

177. *Criterion 10.6* - Rule 18(7) of the IRR requires FIs to understand and, as appropriate, obtain information on, the purpose and intended nature of the account, transaction, or the business or professional relationship with their customers. There are similar provisions contained in the BSP, SEC and IC Rules and Guidelines (BSP: X806(a)/4806Q(a) MORB/MORNBFI, SEC: s5.A.3 2018 Guidelines, IC: s22 CL. 2018-48).

Criterion 10.7

178. *10.7 (a)* - Rule 18(8) of the IRR requires FIs, on the basis of materiality and risk, to conduct ongoing monitoring to understand the normal and reasonable account or business activity of customers. It also requires FIs to scrutinise transactions undertaken throughout the course of the business or professional relationship to ensure that the customers' accounts and transactions are consistent with the FIs knowledge of its customer, their business and risk profile, including where necessary, the source of funds.

179. *10.7 (b)* - Rule 18(8) of the IRR requires FIs to, based on materiality and risk, ensure that information and documents collected under the CDD process are kept up-to-date and relevant, by undertaking reviews of existing records, particularly for higher risk categories of customers. There are comparable provisions contained in the BSP, SEC and IC Rules and Guidelines (BSP: X806(a)/4806Q(a), X806.3(a)/4806Q.3(a) MORB/MORNBFI, SEC: s5.A.2, s5.A.5 2018 Guidelines, IC: s34 CL. 2018-48).

Specific CDD measures required for legal persons and legal arrangements

180. *Criterion 10.8* - Section 9(a) of the AMLA requires FIs to maintain a system of verifying the legal existence and organisational structure of 'corporate clients'. 'Corporate client' is not defined in the AMLA. It is not clear that the requirement to verify the legal existence and organisational structure applies to all types of legal person or legal arrangement.

181. Despite this, Rule 18(4) of the IRR states that for customers that are legal persons or legal arrangements, FIs shall maintain a system of understanding the nature of the customer's business or profession, and ownership and control structure. There are comparable requirements contained in the BSP, SEC and IC Rules and Guidelines (BSP: X806(a)/4806Q(a) MORB/MORNBFI, SEC: s.5.A.3, s.5.H 2018 Guidelines, IC: s.24 CL. 2018-48)

182. *Criterion 10.9* - Section 9(a) of the AMLA requires FIs to maintain a system of verifying the legal existence and organisational structure of corporate clients. 'Corporate client' is not defined in the AMLA. It is not clear that the requirement to verify the legal existence and organisational structure applies to all types of legal persons or legal arrangements.

183. Despite this, Rule 18(4) of the IRR requires that for customers that are legal persons or legal arrangements, FIs must identify and verify the customer's (a) name, legal form and proof of existence (b) the powers and other legal requirements or contracts that regulate and bind the legal person or legal arrangement, as well as the names of the relevant persons having a senior

TECHNICAL COMPLIANCE

management position or perform significant responsibilities in the legal person or legal arrangement; and (c) the address of the registered office and, if different, a principal place of business. The BSP, SEC and IC Rules and Guidelines then set out various requirements that their supervised FIs must comply with to do this (BSP: X806(a)/4806Q(a), X806.2(a)-(c)/4806Q.2(a)-(c) MORB/MORNBFI, SEC: s.5.A.3, s.5.H 2018 Guidelines, IC: s.24 CL. 2018-48).

184. *Criterion 10.10* - For customers that are legal persons, Rule 18(6) of the IRR requires FIs to identify and take reasonable measures to verify the identity of beneficial owners through the following information:

185. *10.10 (a)* the identity of the natural persons, if any, who ultimately have controlling ownership interest in a legal person;

186. *10.10 (b)* to the extent that there is a doubt as to whether the persons with the controlling ownership interest are the beneficial owners or where no natural person exerts control through ownership interests, the identity of the natural persons, if any, exercising control over the legal person through other means; and

187. *10.10 (c)* where no natural person is identified under items (a) and (b) above, the identity of the relevant natural persons who hold senior management position. The BSP, SEC and IC Rules and Guidelines then set out various requirements that their supervised FIs must comply with to do this (BSP: X806(a)/4806Q(a), X806.2(a)-(c)/4806Q.2(a)-(c) MORB/MORNBFI, SEC: s.5.A.2, s.5.A.3 2018 Guidelines, IC: s.22, s.24 CL. 2018-48).

Criterion 10.11

188. *10.11 (a)* - For customers that are legal arrangements, Rule 18(6) of the IRR requires FIs to identify and take reasonable measures to verify the identity of beneficial owners. For trust agreements: the identity of the trustors/grantors/settlers, the trustees, the beneficiaries or class of beneficiaries, the protector, if any, and any other natural person exercising ultimate effective control over the trust agreement. In the case of beneficiaries of trust agreements that are designated by characteristics or by class: sufficient information concerning the beneficiary to satisfy the covered person that it will be able to establish the identity of the beneficiary at the time of the payout or when the beneficiary intends to exercise vested rights

189. *10.11 (b)* - the same Rule in the IRR requires FIs to identify and take reasonable measures to verify the identity of beneficial owners for other types of legal arrangements: the identity of persons in equivalent or similar positions. The BSP and IC Rules and Guidelines then set out various requirements that their supervised FIs must comply with to do this (BSP: X806(a)/4806Q(a), X806.2(a)-(c)/4806Q.2(a)-(c) MORB/MORNBFI, IC: s.24 CL. 2018-48), but the SEC 2018 Guidelines do not.

CDD for Beneficiaries of Life Insurance Policies

190. *Criterion 10.12* - For life and other investment related insurance policies, Rule 19(2) of the IRR requires that CDD is conducted in the following circumstances:

191. *10.12 (a)* On a beneficiary as soon as the beneficiary is identified as a specifically named natural person, or legal person, or legal arrangement.

192. *10.12 (b)* Where a beneficiary is designated by characteristics, or by class, or by other means, sufficient information must be obtained to satisfy the FI that it will be able to establish the identity of the beneficiary at the time of the payout.

193. *10.12 (c)* In both cases, the identity of the beneficiary should be verified at the time of the payout. There are similar provisions contained in the IC Guidelines (IC: s.33 CL. 2018-48).

194. *Criterion 10.13* - Rule 19(2) of the IRR requires FIs to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether EDD is applicable. If an FI determines that a beneficiary who is a legal person or legal arrangement presents a higher risk, it shall take enhanced measures, which include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout. There are comparable provisions contained in the IC Guidelines (IC: s33 CL. 2018-48).

Timing of verification

195. *Criterion 10.14* - Rule 18(4) and (6) of the IRR require that CDD be conducted before or during the course of establishing a business relationship, or conducting transactions for occasional customers. Verification of the identity of a customer or beneficial owner may be completed after the business relationship is established, provided that: (a) it occurs as soon as reasonably practicable; and (b) this is essential not to interrupt the normal conduct of business; and (c) the ML/TF risks are effectively managed. There are comparable requirements contained in the BSP and IC Rules and Guidelines (BSP: X806.2(b)/4806Q.2(b) MORB/MORNBFI, IC: s21 CL. 2018-48), but not in the SEC 2018 Guidelines.

196. *Criterion 10.15* - Rule 18(4) of the IRR requires FIs to adopt risk management procedures concerning the conditions under which a customer may utilise the business or professional relationship prior to verification. There are similar provisions contained in the IC Guidelines (s36 CL. 2018-48), but not in the BSP or SEC Rules or Guidelines.

Existing customers

197. *Criterion 10.16* - Rule 18(1) of the IRR requires FIs to apply CDD requirements to existing customers on the basis of materiality and risk, and to conduct due diligence on existing relationships at appropriate times. This must take into account whether and when CDD measures have previously been undertaken and the adequacy of information and document obtained. There are similar provisions contained in the BSP, SEC and IC Rules and Guidelines (BSP: X806(e)/4806Q(e) MORB/MORNBFI, SEC: s5.A.5 2018 Guidelines, IC: s35 CL. 2018-48).

Risk-based approach

198. *Criterion 10.17* - Rule 18(10) of the IRR requires FIs to undertake enhanced due diligence in certain circumstances, including where the risks of ML/TF are higher. There are similar provisions contained in the BSP, SEC and IC Rules and Guidelines (BSP: X806.1(b)/4806Q.1(b) MORB/MORNBFI, SEC: s.5.C.3 2018 Guidelines, IC: s.29 CL. 2018-48).

199. *Criterion 10.18* - Rule 18(11) of the IRR enables, where lower risks of ML/TF have been identified, and through an adequate analysis of risk by the FI, reduced due diligence procedures to be applied. The reduced due diligence procedures shall be commensurate with the lower risk factors, but are not acceptable whenever there is suspicion of ML/TF, or specific higher risk scenarios apply. There are similar provisions contained in the BSP, SEC and IC Rules and Guidelines (BSP: X806.1(d)/4806Q.1(d) MORB/MORNBFI, SEC: s.5.C.2 2018 Guidelines, IC: s.31 CL. 2018-48).

Failure to satisfactorily complete CDD

200. *Criterion 10.19* - Rule 18(12) of the IRR requires that FIs who are unable to comply with the relevant CDD measures shall: (a) refuse to open an account, commence business relations or perform the transaction; or shall terminate the business relationship; and (b) file an STR in relation to the customer, if circumstances warrant. There are comparable provisions in the BSP,

TECHNICAL COMPLIANCE

SEC and IC Rules and Guidelines (BSP: X806(a)/4806Q(a) MORB/MORNBFI, SEC: s.5.C.5 2018 Guidelines, IC: s.29 CL. 2018-48).

201. *Criterion 10.20* - Rule 18(13) of the IRR states where FIs form a suspicion of ML/TF and associated unlawful activities, and they reasonably believe that performing the CDD process will tip-off the customer, they need not pursue the CDD process, but should file an STR, closely monitor the account, and review the business relationship. There are comparable provisions contained in the BSP, SEC and IC Rules and Guidelines (BSP: X806(a)/4806Q(a) MORB/MORNBFI, SEC: s.5.C.5 2018 Guidelines, IC: s.46 CL. 2018-48).

Weighting and Conclusion

202. The Philippines meets almost all CDD requirements set out in R.10. All FIs must comply with the AMLA, IRR and the relevant supervisory Rules or Guidelines. The main shortcoming relates to the phrase 'corporate client' in the AMLA, which is not defined. Therefore, for some types of legal person or legal arrangement, there may not be a clear legislative basis requiring ownership structures to be examined, and beneficial owners or persons acting on behalf of the customer be identified and their identities verified.

203. **Recommendation 10 is rated largely compliant.**

Recommendation 11 – Record-keeping

204. In its ME 2009, the Philippines was rated as largely compliant with former R.10. The deficiency related to the lack of provision to permit AMLC to request extension of record-keeping when called for in appropriate circumstances.

205. The record keeping principle is contained in the AMLA, with specific measures set out in enforceable means.

206. *Criterion 11.1* - All covered persons are required to retain all records of all transactions for five years from the date of transactions (s.9(b) of AMLA). Rule 20 s.2 of 2018 IRR extends the definition of "all records of all transactions" as those related to i) customer records and ii) transaction documents. Rule 20 s.3 further requires the record keeping period shall exceed five years when the case is filed to the court. In such instances the retention will cease upon notification of AMLC that the case has been resolved, decided or terminated.

207. *Criterion 11.2* - All covered persons are required to maintain all CDD records, transaction documents and the results of any analysis undertaken for five years, in relation to closed accounts, those records shall be retained for at least five years from the dates they were closed, termination of business/professional relationship or after the date of occasion transaction (s.9(b) of AMLA). Rule 20, s.2 of the 2018 IRR supplements this requirement, including results of analysis.

208. *Criterion 11.3* - Transactions include any movement of funds by any means (S.3h of the AMLA). S.9b requires transaction documents to be subject to record keeping. S.11 of the AMLA empowers AMLC to inquire into any bank deposits or investment, including related accounts when there is probable cause that they are related to ML crimes. Related accounts refer to accounts, funds and source of which originated from and/or are materially linked to the monetary instrument or property.

209. Rule 20 s.4.1 of the 2018 IRR requires covered persons to retain all records as original and all records must be maintained in a manner that is admissible in court. S.X808 of the MORB also requires all covered persons to prepare and maintain documents such that any account, relationship or transaction can be reconstructed to enable AMLC and the courts to establish audit

trails. S.6.1(2) of the SEC Memorandum Circular No. 16-2018 and s.48 of IC Circular No.2018-48 also set out the requirements for transactions shall be able to provide audit trails for criminal prosecution that correspond to the same requirement in the 2018 IRR. The 2018 AMLC Guidelines on Digitization of Customer Records gives further support to keeping such records and permits reconstruction of transactions for ML/criminal investigations.

210. *Criterion 11.4* - All covered persons are required to immediately provide AMLC full access to all information in relation to accounts, transaction and/or person related to a person subject to investigation (Rule 8 s1.2 of the 2018 IRR). Rule 20 s.5 of same IRR requires FIs to ensure those records are available swiftly to domestic competent authorities in the exercise of their duties or upon order by a competent authority. This does not include bank customer information and transaction records related to bank accounts where competent authorities do not have legal competency to obtain the data and in most cases requires information request mechanism with AMLC or through court order.

211. BSP-regulated covered persons are required to appoint at least two officers jointly responsible in the safekeeping of all records and documents subject to the record keeping requirements in the AMLA and to make those records/documents available without delay during BSP regular or special examinations (s.X808.3 of the MORB and 4808Q.3 of the MORNBF (under BSP Circular 706 amended by Circular 950, 2017).

212. Section 6.6 of the SEC Memorandum Circular No. 16-2018 also requires the appointment of at least two persons to be responsible for the record keeping. Insurance institutions are required to assign a designated officer responsible for record keeping and permit AMLC and IC prompt access to records of customer identification and transaction documents during compliance checking or investigation (s.10 and s.50 of IC Circular No.48-2018).

Weighting and Conclusion

213. **Recommendation 11 is rated compliant.**

Recommendation 12 – Politically exposed persons

214. In its 2009 ME, the Philippines was rated as partially compliant with former R.6. There was no specific requirement for FIs (except insurance) to implement risk management systems to detect PEPs and to establish source of wealth in their businesses.

215. *Criterion 12.1* - The definition of PEPs is set out in Rule 2 Section 1 (xxx) of 2018 IRR of the AMLA and includes individuals who is or has been entrusted with prominent public position in a foreign state.

216. Rule 19 Section 1.3 of 2018 IRR covers all the measures required for foreign PEPs (risk management system, management approval and source of fund and wealth, and EDDs. The BSP adopted all requirements of foreign PEPs respectively into MORB/MORNBF Section X806.2/4806Q (h) of BSP Circular 1022 series 2018 for FIs under its supervision. The same requirements are adopted in Section 5.E.1, 5.C.3 and 5.C.4 (5) of 2018 AML/CFT guideline of the SEC (Memorandum Circular No.16, series 2018). S.41 of IC Circular No.2018-48 comprises of the requirements of foreign PEPs same as the RIRR for insurance companies and other IC-regulated covered persons.

217. *Criterion 12.2* - The definition of PEPs in Rule 2 s.1 (xxx) of 2018 IRR covers those with prominent public position in the Philippines with substantial authority over policy, operation or the use or allocation of government-owned resources, and those in an international organization. The requirements in Rule 19 s.1.2 of 2018 IRR of the AMLA adopts all FATF requirements for

domestic PEPs and those from international organisations. The AML/CFT guidelines for the BSP, SEC and IC adopt the same requirements as the IRR (MORB/MORNBFI s.X806.2/4806Q(h) of BSP Circular 1022 series 2018; Section 5.E.1, 5.C.3 and 5.C.4 (5) of the SEC Memorandum Circular No.16-2018 and s.41 of IC Circular No.2018-48).

218. *Criterion 12.3* - FIs are required to identify the true and full identity of PEPs, as well as their “immediate family members” and “close relationships/associates” (IRR Rule 19 of 2018). It does not, however, apply the obligations to manage the risks to those persons who are immediate family members or close relationships/associates. ‘Immediate family members’ applies to those within second degree of consanguinity in the 2018 IRR. MORB/MORNBFI Section X806.2/4806Q (h) of BSP Circular 1022 series 2018, Section 4(J) of IC Circular 2018-48 and Section 5.E.1 of SEC Memorandum Circular No.16-2018 go further than the IRR and apply PEP obligations to close family members and associates. However, BSP narrowed down the obligations to close associates under very specific circumstances when those persons are under beneficiary ownership and legal arrangements with the PEPs.

219. *Criterion 12.4* - Covered persons providing life insurance products and other investment-related insurance policies are required to exercise additional CDDs over beneficiaries at the time of payout, including determination of whether the beneficiaries are PEPs (Rule 19 S.2 of 2018 IRR). Rule 2 s.1 (n) defines beneficiary of life insurance or investment-linked insurance policies as any person being paid the policy proceeds. S.33 of IC Circular Letter No.2018-48 as amended by IC Circular Letter No.2018-60 sets out the requirement in c.12.4 verbatim.

Weighting and Conclusion

220. There is a minor shortcoming with PEP requirements set out by BSP are only applicable to close associates in restricted circumstances.

221. **Recommendation 12 is rated largely compliant.**

Recommendation 13 – Correspondent banking

222. In its 2009 MER, the Philippines was rated largely compliant with former R.7. Deficiencies were identified in the implementation of the recommendation due to the generic nature of guidance and a lack of supervisory attention.

223. *Criterion 13.1* - FIs are to adopt policies and procedures to prevent correspondent banking activities from being used for ML/TF (Rule 19(3) of the IRR). (a) FIs must gather sufficient information about the respondent institution to understand the nature of its business, and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a ML/TF investigation or regulatory action. (b) The FI must assess the respondent institution’s AML/CFT controls, (c) obtain approval from senior management before establishing new correspondent relationships and (d) clearly understand the respective AML/CFT responsibilities of each institution. These provisions are also contained in the BSP Rules (X806.2(i) MORB).

224. *Criterion 13.2* - With respect to ‘payable-through accounts’, FIs are required to satisfy themselves that the respondent bank (a) has performed CDD obligations on its customers that have direct access to the accounts of the correspondent bank, and (b) is able to provide relevant CDD information upon request to the correspondent bank (Rule 19(3) of the IRR). These provisions are also contained in the BSP Rules (X806.2(i) MORB).

225. *Criterion 13.3* -. FIs are prohibited from entering into, or continuing, correspondent banking relationships with shell banks and should have measures to satisfy themselves that

respondent financial institutions do not permit their accounts to be used by shell banks (Rule 19(3) of the IRR). The definition of 'shell bank' in the IRR is the same as the FATF definition of 'shell bank'. These provisions are also contained in the BSP Rules (X806.2(i) MORB).

Weighting and Conclusion

226. **Recommendation 13 is rated compliant.**

Recommendation 14 – Money or value transfer services

227. In its 2009 MER, the Philippines was rated partial compliant with former SR.VI. The main technical deficiency was that there was no requirement to maintain and update lists of agents.

228. *Criterion 14.1* - Remittance and transfer companies (RTCs) are covered persons and are supervised or regulated by BSP (S.9(a1) of the AMLA and Rule 4(1) of the IRR). RTC are defined in keeping with the FATF definition as any entity that provides MVTS, which includes financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network (s.4511N.1 of the MORNBF, as amended by BSP CL No. 942).

229. New registration provisions for RTCs come into force in January 2017 which require any all new RTCs to register with BSP before they can operate and all previously registered RTCs had to re-register by 30 April 2018 (S.4511N.2 of the MORNBF, as amended by BSP CL No. 942.). RTC includes any agent operating a remittance business network (RA), or any remittance sub-agent (RSA) with at least one branch i.e. two or more locations (S.4511N.1).

230. In addition to registering with BSP, s.4511N.2d of the MORNBF requires RTCs to register with AMLC within thirty days of commencing business. This is required for the purpose of reporting covered and suspicious transactions.

231. *Criterion 14.2* - The BSP has mechanisms to identify and take action against RTCs operating without registration. This includes having an MOU in place with the Department of Interior and Local Government to allow information sharing with city and municipal governments units (LGUs). This enables the BSP to cross-check registered RTC information against records held by LGUs of business permits issued by them to provide a MVTS service.

232. Another mechanism to identify and take action against RTCs operating without registration involves banks, as they may only deal with RTCs that are registered with BSP (S.X806.2(m) of MORB). Banks are required to undertake ongoing monitoring of customers, accounts and transactions to understand their normal and reasonable account activity, and to detect unusual or suspicious patterns of activity (X806.3). BSP has instructed banks that this includes a requirement that banks identify customers or accounts that are being used to facilitate remittance activities while unregistered to do so (BSP Memorandum M-2017-009). When banks submit STRs relating to this, they can be used to assist identify an unregistered RTC.

233. When an RTC is identified to be operating without registration, the BSP may request that an LGU take further action. An LGU may require the RTC to register with BSP or to cease operations. Alternatively, the BSP may itself impose sanctions on unregistered RTCs (s.4511N.15 MORNBF). This includes disqualification from registration. And where the failure to register is wilful a fine sanctions of not less than PHP50,000 (approx. USD950) and not more than PHP200,000 (approx. USD3,800), or imprisonment of not less than two years and not more than ten years, or both are available (s.36 of RA No. 7653). These sanctions are proportionate.

TECHNICAL COMPLIANCE

234. While the Philippines has a framework to apply fines for operating while unregistered, most of the action taken as at the date of the on-site visit has focussed on promoting and ensuring re-registration under the new system. There has been extensive coordination with LGUs and multiple warning letters issued to previously registered MSBs requiring them to re-register as RTCs, with the date of registration extended until 30 April 2018. As at the date of the on-site visit, no fines (or terms of imprisonment) have been imposed on an RTC for operating while unregistered under the new system.

235. *Criterion 14.3* - The AMLA mandates BSP to conduct periodic or special examination of RTCs to ensure their compliance with the AMLA (s.11). Rule 4(1) of the IRR also prescribes that BSP supervise or regulate RTCs. RTCs must comply with Part 8 of the MORNBF1.

236. *Criterion 14.4* - RTC includes any agent operating a remittance business network (RA), or any remittance sub-agent (RSA) with at least one branch, i.e. two or more locations (s. 4511N.1 of the MORNBF1). These types of agent must be registered with BSP and with AMLC as per criterion 14.1 above.

237. For other RSAs (i.e. those with only one location), the requirements of the MORNBF1 ensures that RSAs maintain a current list of its agents. Subsection 4511N.3b requires a RTC to notify BSP of all new RSAs within five working days from signing a contract. Additional notification requirements are imposed on RTCs by Memorandum No. M-2017-015, which requires RTCs to notify BSP when an RSA closes or when its location changes. This information regarding RSAs is accessible by competent authorities from the BSP.

238. *Criterion 14.5* - Subsection 4511N.2a of the MORNBF1 states that any person authorised by an RTC to perform certain relevant undertakings in its remittance business is an RSA. Subsection 4511N.2c of the MORNBF1 states that RTCs may accredit their own RSAs. It also states that the RSA is an extension of the RTC and shall be subject to the same obligations of the RTC. The RTC is required to conduct appropriate due diligence in this regard and maintain effective oversight of its RSAs. A Deed of Undertaking, which is a prescribed form, must also be signed by the RTC. This states that the RTC undertakes full responsibility for the RSA's compliance with all AML/CFT requirements.

Weighting and Conclusion

239. The Philippines has a comprehensive framework for regulating MVTS and for identifying and taking action against unregistered RTCs. However, since the new registration provisions took effect, most of the action taken has focussed on promoting and ensuring re-registration under the new system.

240. **Recommendation 14 is rated largely compliant.**

Recommendation 15 – New technologies⁹³

241. *Criterion 15.1* - Section 19(5) of the IRR requires AMLC, in coordination with the relevant supervisory agencies, LEAs, or other government agencies, and FIs, to identify and assess the ML/TF risks that may arise in relation to the development of new products and new business

⁹³ The FATF revised R.15 in October 2018 and its interpretive note in June 2019 to require countries to apply preventive and other measures to virtual asset service providers and virtual asset activity. This evaluation does not assess [Country name] compliance with revised R.15 because, at the time of the on-site visit, the FATF had not yet revised its assessment Methodology accordingly. [Country name] will be assessed for technical compliance with revised R.15 in due course, in the context of its mutual evaluation follow-up process.

practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

242. BSP and IC-supervised FIs are required to identify and assess the ML/TF risks that may arise from the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products (s.X805.5/4805Q.5 of the MORB/MORNBF, and s.18 of CL No. 2018-48 respectively).

243. For SEC-supervised FIs, FIs are required to pay special attention to ML threats that may arise from new or developing technologies that might favour anonymity, and take measures, if needed, to prevent use in ML schemes (s.5.A.11 of the 2018 Guidelines).

244. *Criterion 15.2* - Rule 19(5) of the IRR requires FIs to (a) undertake risk assessments prior to the launch or use of such products, practices and technologies; and (b) take appropriate measures to manage and mitigate the risks. There are similar provisions contained in the BSP and IC Rules and Guidelines (BSP: X805.5/4805Q.5 MORB/MORNBF, IC: s.32 CL No. 2018-48), but not in the SEC 2018 Guidelines.

Weighting and Conclusion

245. **Recommendation 15 is rated compliant.**

Recommendation 16 – Wire transfers

246. In its 2009 MER, the Philippines was rated partial compliant with former SR.VII. Applicable rules relating to inclusion or originator information were found to be incomplete. Also, applicable rules relating to transfers not accompanied by originator information or to the monitoring of implementation of SR.VII were also incomplete.

247. *Criteria 16.1* - Rule 19(6) of the IRR requires that for cross border wire transfers over a threshold amount, FIs must (a) obtain the (i) name of the originator, (ii) the originator account number and (iii) one of the originator's address, national identity or customer identification number, or date and place of birth. CDD must be conducted to establish the true and full identity of the originator. (b) FIs must also obtain the name and account number of the beneficiary. The originator and beneficiary information must accompany the wire transfer. The BSP Rules contain the same provisions (X806.2(j)/4806Q.2(j) MORB/MORNBF). The threshold is set at PHP50,000 (approx. USD950).

248. *Criterion 16.2* - Rule 19(6) of the IRR states that where several individual cross-border wire transfers from a single originator are bundled into a batch file for transmission to beneficiaries, the batch file should contain required and accurate originator information, and full beneficiary information that is fully traceable within the beneficiary country. The FI must also include the originator's account number or unique transaction reference number. The BSP Rules contain the same provisions (X806.2(j)/4806Q.2(j) MORB/MORNBF).

249. *Criterion 16.3* - For cross border wire transfers below the threshold of PHP50,000 (approx. USD 950), Rule 19(6) of the IRR requires that (a) the originator's name and account number or a unique transaction reference number and (b) the beneficiary's name and account number or a unique transaction reference number, accompanies the transaction. The BSP Rules contain the same provisions (X806.2(j)/4806Q.2(j) MORB/MORNBF).

250. *Criterion 16.4* - Rule 19(6) of the IRR requires that originator and beneficiary information accompanying cross border wire transfers below the threshold of PHP50,000

TECHNICAL COMPLIANCE

(approx. USD 950) must be verified where there is suspicion of ML/TF. The BSP Rules contain the same provisions (X806.2(j)/4806Q.2(j) MORB/MORNBFI).

251. *Criterion 16.5* - Rule 19(6) of the IRR requires that for domestic wire transfers, originator information as indicated for cross-border wire transfers should accompany the wire transfer unless this information can be made available to the beneficiary institution and appropriate authorities by other effective means. The BSP Rules contain the same provisions (X806.2(j)/4806Q.2(j) MORB/MORNBFI).

252. *Criterion 16.6* - Rule 19(6) of the IRR states that where the information accompanying the domestic wire transfer can be made available to the beneficiary institution and appropriate authorities by other means, the ordering institution need only include an account number or unique transaction number. This number must allow the transaction to be traced back to the originator or the beneficiary. The ordering institution shall make the information available within five working days from receipt of the request from either the beneficiary institution or from appropriate authorities. This is a deficiency and is longer than the FATF requirement for the ordering institution to make the information available within three business days. The BSP Rules contain the same provisions, although the ordering institution must make the information available within three working days (X806.2(j)/4806Q.2(j) MORB/MORNBFI). LEAs are not able to compel immediate production of wire transfer information.

253. *Criterion 16.7* - Rule 20 of the IRR requires FIs to maintain and safely store records for five years following the end of a business relationship or occasional transaction. This includes wire transfer records. These records must be retained in original form or otherwise to provide admissible evidence in court. CDD and transaction records must also be made swiftly available to competent authorities in the exercise of official functions or upon order by a competent authority. There are similar provisions in the BSP Rules, although there is no requirement that records be made available to competent authorities other than AMLC (X808/4808Q MORB/MORNBFI).

254. *Criterion 16.8* - Rule 19(6) of the IRR states that an ordering institution shall not execute instructions for a wire transfer unless it has complied with all obligations of an ordering institution. The same provisions are contained in the BSP Rules (X806.2(j)/4806Q.2(j) MORB/MORNBFI).

255. *Criterion 16.9* - Rule 19(6) of the IRR states that for cross-border wire transfers, intermediary institutions should ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it. The same provisions are contained in the BSP Rules (X806.2(j)/4806Q.2(j) MORB/MORNBFI).

256. *Criterion 16.10* - Rule 19(6) of the IRR states that where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, an intermediary institution should keep a record of all the information received from the ordering or another intermediary institution for at least five years. The same provisions are contained in the BSP Rules (X806.2(j)/4806Q.2(j) MORB/MORNBFI).

257. *Criterion 16.11* - Rule 19(6) of the IRR states that intermediary institutions should take reasonable measures, which are consistent with straight through processing, to identify cross border wire transfers that lack required originator or beneficiary information. The same provisions are contained in the BSP Rules (X806.2(j)/4806Q.2(j) MORB/MORNBFI).

258. *Criterion 16.12* - Rule 19(6) of the IRR states that intermediary institutions shall have risk based policies and procedures for determining (a) when to execute, reject, or suspend a wire transfer lacking required originator or beneficiary information and (b) the appropriate follow-up

action. The same provisions are contained in the BSP Rules (X806.2(j)/4806Q.2(j) MORB/MORNBFI).

259. *Criterion 16.13* - Rule 19(6) of the IRR states that a beneficiary institution must take reasonable measures, which may include post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers that lack required originator or beneficiary information. The same provisions are contained in the BSP Rules (X806.2(j)/4806Q.2(j) MORB/MORNBFI).

260. *Criterion 16.14* - Rule 19(6) of the IRR states that a beneficiary institution shall verify the identity of a beneficiary if the identity has not previously been verified, and maintain this information. This applies to cross-border wire transfers over the threshold. Rule 20 of the IRR requires FIs to maintain and safely store records for five years following the end of a business relationship or occasional transaction. This includes wire transfer records. These records must be retained in original form or otherwise to provide admissible evidence in court. CDD and transaction records must also be made swiftly available to competent authorities in the exercise of official functions or upon order by a competent authority. There are similar provisions in the BSP Rules, although there is no requirement that records be made available to competent authorities other than AMLC (X806.2(j)/4806Q.2(j), X808/4808Q MORB/MORNBFI).

261. *Criterion 16.15* - Rule 19(6) of the IRR states that where a wire transfer is not accompanied by required originator or beneficiary information, a beneficiary institution must adopt risk-based policies and procedures for determining (a) when to execute, reject, or suspend a wire transfer lacking required originator or beneficiary information, and (b) the appropriate follow up action. The same provisions are contained in the BSP Rules (X806.2(j)/4806Q.2(j) MORB/MORNBFI).

262. *Criterion 16.16* - Remittance and transfer companies (RTCs) are required to comply with Rule 19(6) of the IRR and s.4806Q.2(j) of the MORNBFI relating to wire transfers in all countries in which they operate, directly or through their agents. Where an RTC provides its remittance service through remittance sub-agents (RSAs), BSP CN.942 states that the sub-agent is an extension of the RTC. The RTC is responsible for ensuring that transactions processed through an RSA also comply with the relevant wire transfer rules.

263. *Criterion 16.17* - Rule 19(6) of the IRR states that if an RTC controls both the ordering and beneficiary side of a wire transfer, the RTC should (a) consider 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 FIU. The same provisions are contained in the BSP Rules (4806Q.2(j) MORNBFI).

264. *Criterion 16.18* - Section 11 of the TF Law and Rule 11(a) of the IRR of the TF Law authorises AMLC to issue an order to freeze without delay. For UNSCR 1267 designations, a standing AMLC order is provided by AMLC Resolutions No. TF-01 and TF-02 of 2012 which directs all covered persons and relevant government agencies to freeze without delay the property or funds, including related accounts, of UNSCR 1267 designated persons or entities. This also includes the processing of funds by wire transfer. Updates and changes to the list of UNSCR 1267 designations must be immediately transmitted from DFA to AMLC. In practice, AMLC receives updated lists directly from the UN and updates these onto its website and its portal for covered persons within one business day. For UNSCR 1373 designations, the same provisions apply. S.11 of the TF Law and Rule 11(a) of the IRR of the TF Law authorises AMLC to issue a standing order to freeze without delay. Rule 19(6) of the IRR and the BSP Rules make reference to these requirements in relation wire transfers.

Weighting and Conclusion

265. There is a minor shortcoming relating to the timeframe by which information must be made available by ordering institutions to beneficiary institutions for domestic wire transfers. A further shortcoming relates to the requirement that CDD and wire transfer transaction records be made swiftly available to competent authorities. The wire transfer provisions do not apply to FIs supervised by SEC or IC.

266. **Recommendation 16 is rated largely compliant.**

Recommendation 17 – Reliance on third parties

267. In its 2009 MER, the Philippines was rated partial compliant with former R.9. SEC did not require covered persons to have immediate access to CDD information and IC did not require the covered persons to conduct CDD in instances where policies are purchased through salary allotment. Also the SEC and IC guidance placed ultimate responsibility for customer identification and verification on the third party.

268. *Criterion 17.1* - Rule 21(1) of the IRR states that a FI may rely on another covered person or a FI or DNFBP outside the Philippines that is covered by equivalent CDD and record keeping measures. Ultimate responsibility for identifying the customer remains with the FI that is relying on the third party. An FI must (a) obtain immediately the necessary information received and gathered during the conduct of the different CDD measures; and (b) take steps to satisfy itself that copies of record of identification information and documents shall be made available from the third party upon request without delay; and (c) satisfy itself that the third party is a covered person, and has measures in place for compliance with CDD and record-keeping requirements. The BSP, SEC and IC Rules and Guidelines then set out various specific requirements that their supervised FIs must comply with to do this.

269. *Criterion 17.2* - Rule 21(1) of the IRR states that when determining in which countries the third party that meets the conditions can be based, FIs shall have regard to information available on the level of country risk. There are similar provisions in the BSP and IC Rules and Guidelines (BSP: X806.2(f)/4806Q.2(f) MORB/MORNBFI, IC: CL. s37 2018-48), but not in the SEC 2018 Guidelines.

270. *Criterion 17.3* - Rule 21(1) of the IRR allows FIs to rely on a third party that is part of the same financial, business or professional group under the following circumstances: (a) the group applies CDD and record-keeping requirements in line with all AMLA requirements; and (b) the implementation of CDD and record-keeping requirements is supervised at a group level by a supervising authority; and (c) any higher country risk is adequately mitigated by the group's AML/CFT policies. There are similar provisions in the BSP and IC Rules and Guidelines (BSP: X806.2(f)/4806Q.2(f) MORB/MORNBFI, IC: s37 CL. 2018-48), but not in the SEC 2018 Guidelines.

Weighting and Conclusion

271. **Recommendation 17 is rated compliant.**

Recommendation 18 – Internal controls and foreign branches and subsidiaries

272. In its 2009 MER, the Philippines was rated compliant with former R.15 and partially compliant with former R.22. There was no requirement for FIs to require a supervisor be informed if a foreign branch or subsidiary could not implement AML/CFT measures equal to or at a higher standard than those in the Philippines. There was also no requirement for FIs to pay

particular attention to branches and subsidiaries in countries that do not sufficiently apply the FATF recommendations.

273. *Criterion 18.1* - Rule 16(1) of the IRR requires FIs to formulate a comprehensive and risk-based MLPP that is compliant with all AML/CFT requirements and commensurate to size and risk profile. This must include internal policies, controls and procedures for: (a) the compliance management setup, including the designation of a compliance officer at the management level or creation of compliance unit; and (b) screening procedures to ensure high standards when hiring employees; and (c) continuing education and training program; and (d) an independent audit function. The BSP, SEC and IC Rules and Guidelines then set out various requirements that their supervised FIs must comply with to do this. There is a minor scope gap for covered FIs of 250 financing companies and 2,459 lending companies.

274. *Criterion 18.2* - Rule 16(7) of the IRR requires FIs to implement a group wide MLPP which should be applicable, and appropriate to, all branches and majority owned subsidiaries of the financial group. The MLPP must include: the measures set out in criterion 18.1 and (a) policies and procedures for sharing information required for the purposes of CDD and risk management and (b) the provision, at group-level compliance, audit, and/or AML/CFT functions, of customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. This should include information and analysis of transactions or activities which appear unusual, if such analysis was done. Similarly branches and subsidiaries should receive such information from these group-level functions when relevant and appropriate to risk management; and (c) adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

275. There are similar provisions contained in the BSP, SEC and IC Rules and Guidelines (BSP: X805/4805Q MORB/MORNBFI, SEC: s.5.D.2 2018 Guidelines, IC: s.11, s.37 CL. 2018-48). However, the SEC do not have specific policies or procedures for sharing information required for the purpose of CDD and ML/TF risk management. Nor do SEC include specific provisions requiring adequate safeguards on the confidentiality and use of information exchanged.

276. *Criterion 18.3* - Where the minimum AML/CFT requirements of the host country are less strict, and to the extent that the laws and regulations of the host country permit, Rule 16(8) of the IRR requires FIs to ensure their foreign branches and majority-owned subsidiaries apply measures consistent with Philippine AML/CFT requirements. If the host country does not permit the proper implementation of Philippine AML/CFT requirements, FIs shall apply appropriate additional measures to manage the ML/TF risks, and inform their respective supervisory authority and AMLC. There are similar provisions contained in the BSP Rules and IC Guidelines (X805/4805Q MORB/MORNBFI, IC: s.12, CL. 2018-48), but not in the SEC 2018 Guidelines.

Weighting and Conclusion

277. There is a minor scope gap of 250 financing companies and 2,459 lending companies that are not captured as covered persons, and therefore not required to formulate a comprehensive and risk-based MLPP.

278. **Recommendation 18 is rated largely compliant.**

Recommendation 19 – Higher-risk countries

279. In its 2009 MER, the Philippines was rated partial compliant with former R.21. The SEC and IC did not require special attention to transactions with persons in countries that do not sufficient apply FATF recommendations.

TECHNICAL COMPLIANCE

280. *Criterion 19.1* - Rule 19(8) of the IRR requires FIs to apply EDD, proportionate to the risks, to accounts, transactions, and business and professional relationships with customers who are nationals or citizens from foreign jurisdiction or geographical location that presents greater risk for ML/TF or its associated unlawful activities, or is recognised as having inadequate internationally accepted AML/CFT standards, as determined by the relevant domestic or international bodies. There is no explicit reference to the FATF as a relevant international body. Nor is there an explicit requirement that customers that are legal persons from these countries be subject to EDD. There are comparable provisions contained in the BSP, SEC and IC Rules and Guidelines, which do cover legal persons from higher risk countries and make specific reference to FATF as a relevant government body. (BSP: X806.2(n)/4806Q.2(n) MORB/MORNBFI, SEC: s5.D.1 2018 Guidelines, IC: s27 CL. 2018-48).

281. *Criterion 19.2* - Rule 19(8) of the IRR requires AMLC and the supervisory authorities to apply proportionate countermeasures to address risks posed by customers from high-risk jurisdiction or geographical location. While this may occur independently of any call by the FATF, there is no explicit requirement for it to occur when called upon to do so by the FATF.

282. *Criterion 19.3* - Rule 19(8) of the IRR requires AMLC and the supervisory authorities establish measures to ensure that FIs are advised of concerns about weaknesses in the AML/CFT systems of other countries. Neither AMLC, BSP, SEC nor IC provide regular updates to FIs regarding countries that have weaknesses in their AML/CFT systems.

Weighting and Conclusion

283. There is no explicit requirement in the IRR that EDD be applied to customers from higher risk countries when called upon to do so by the FATF. There is no explicit requirement in the IRR that customers that are legal persons from higher risk countries be subject to EDD. AMLC, BSP, SEC or IC do not provide updates to FIs regarding countries which have weaknesses in their AML/CFT systems.

284. **Recommendation 19 is rated largely compliant.**

Recommendation 20 – Reporting of suspicious transaction

285. The Philippines was rated partially compliant for the former R.13 and non-compliant for the former SR.IV in its previous MER. The main deficiencies noted were that the requirement to report transactions linked to terrorism were incomplete and there was insufficient STR reporting in sectors other than the banking sector.

286. *Criterion 20.1* - The AMLA requires all covered person to report suspicious transactions to the ALMC within five working days of establishing suspicion, unless AMLC prescribes a different period not exceeding fifteen working days from the occurrence of transactions (s.9(c)). This does not meet the requirement of 'promptly'. Rule 22 of the 2018 IRR requires all covered persons to file STRs in accordance with AMLC Registration and Reporting Guidelines (ARRG). The ARRG states that covered persons shall report suspicious transactions to AMLC within five working days. This requirement is also sated in AMLC Resolution No. 61). 'Suspicious transaction' is defined in Section (b-1) of the AMLA to include transactions that are in any way related to an unlawful activity or offence under the AMLA, that is about to be, is being, or has been committed. Unlawful activity is defined in the Section 3(I) of the AMLA to include a range of predicate offences, including TF. However, tax crimes are not included, resulting in a scope gap.

287. *Criterion 20.2* - Section 3 (b-1) of the AMLA, defines a suspicious transaction as a transaction, regardless of amount, in which listed circumstances existed. Rule 2 of the 2018 IRR defines suspicious transactions as a transaction, regardless of amount, where suspicious

circumstances exist. Rule 22 of the 2018 IRR states that covered persons shall file all STRs in accordance with the ARR. The body of the ARR does not contain a requirement for covered persons to report suspicious transactions which include attempted transaction; however Annex D to the ARR, titled “Examples of Alerts and Red Flags”, contains examples of suspicious indicators, including indicators that may point to a transaction “whether completed or attempted”. This is listed as an example in the Annex, rather than a requirement in the substantive provisions in the ARR, and is therefore not enforceable. For some covered persons the requirements to report STR on attempted transactions are stipulated under their respective enforceable sectoral guidelines (s.X803(d)/s.4803(d) of the MORB/MORNBFI, s.7.7 of the SEC 2018 Guidelines and s.4H, Title III of IC Circular letter No. 2018 48). Rule 3.a.15, IRR of RA 10168 states that suspicious transaction refers to a transaction with a covered institution, related to terrorism financing or terrorist acts. It includes attempted transactions made by suspected or designated terrorist individuals, organizations, associations or groups of persons.

Weighting and Conclusion

288. There are deficiencies in relation the requirement for STR reporting to include attempted transactions, as the requirement to report attempted transactions is not directly covered in law or regulation. Some sectors are subject to the reporting to report attempted transactions under their sectoral guidelines. The five working day timeframe to report STRs does not fulfil the ‘promptly’ requirement. There is a scope gap in relation to the requirement to report STR related to tax offences as this is not a predicate offence under the AMLA.

289. **Recommendation 20 is partially compliant.**

Recommendation 21 – Tipping-off and confidentiality

290. The Philippines was rated LC with former R.14 in its 2009 MER, which the report noted that the AMLA did not specifically include the disclosure of STRs that are in the process of being reported in its tipping off provisions.

291. *Criterion 21.1* - Section 9C of the AMLA provides that no administrative, criminal or civil proceedings shall lie against any person for having made a STR in the regular performance of their duties in good faith, whether or not such reporting results in any criminal prosecution under the AMLA or any other law. Similar safe harbour provisions are also set out in Rule 22, Section 5 of the 2018 IRR.

292. *Criterion 21.2* - The prohibition on disclosing that an STR or related information is contained in the AMLA, AMLC Registration and Reporting Guidelines and SEC Revised Guidelines in the Preparation of the AML Operating Manual and Sections 58 and 59 of the IC CL No. 2018-48. When filing STRs, covered institutions and their officers and employees are prohibited from communicating, directly or indirectly, in any manner or by any means, to any person or entity or the media. Such reporting may not be published or aired in any manner or form by the mass media, electronic mail, or other similar devices. In case of violation, the concerned officer and employee of the covered institution, covered person and media shall be criminally liable (Rule 9C of AMLA, X807.6 of MORB and Section 7.8 of Operating Manual). Furthermore, the ARR requires that the internal reporting chain of covered persons include proper controls to guarantee the confidentiality of the process and that no “tipping-off” occur during the process. (Part 1-6, ARR)

Weighting and Conclusion

293. **Recommendation 21 is rated compliant**

Recommendation 22 – DNFBPs: Customer due diligence

TECHNICAL COMPLIANCE

294. In its 2009 evaluation, the Philippines was rated non-compliant with former R.12. The major deficiencies were the lack of CDD or record-keeping requirements for DNFBPs. The Philippines extended the AML/CFT requirements to some DNFBPs through the enactment of RA10365 in 2013 (including dealers of precious stones and metal, company service providers, lawyers and accountants) and RA10927 in 2017 (for casinos).

Criterion 22.1

295. 22.1 (a) - Casinos have been captured as covered persons in the AMLA since 2017 and are therefore subject to the customer identification requirements set out in Section 9(a). However casinos are defined as covered persons only in relation to cash transactions (s.3 (a)(8) of AMLA). S.16 of CIRR requires casinos to conduct CDD upon opening an account and further narrows the CDD requirement for conducting financial transactions to only the redemption of chips or other gaming instruments, but not all financial transactions that occur in casinos (e.g. buy-in of chips). S.18 requires CDD of all customers, and to the extent possible, the intermediary and the person or entity on whose behalf a transaction is being conducted.

296. CDD for occasional customers without an account is required under Section 10 (a)(i) and Section 20 of PAGCOR Regulatory Order RO-2018-11-002 (PAGCOR CDD guideline) for financial transactions exceeding PHP500,000 (approx. USD 9500/EUR 8.3K) in aggregation within one gaming day, or when customers make use of any financial services. This is not consistent with the narrower scope of financial transactions contained in Section 16 of CIRR, which states that CDD is only required for redemption. The threshold for occasional cash transactions is also higher than the FATF threshold of USD/EUR3,000. S.23 of CIRR prohibits casinos to carry out a number of specific financial transactions related to cash. Pursuant to s.16 of the CIRR, casinos are required to verify the identity of customers through official identification documents. S.20 of CIRR further requires casinos to conduct face-to-face CDD during account opening to verify the identity. The use of communication technology is permitted for CDD (particularly for proxy and online gaming accounts). Casinos are also required to establish appropriate system/methods to verify and record the identity of customers. All accounts must be maintained in true and full name. Anonymous accounts and accounts under fictitious names are prohibited (s.21E). S.16 of the CIRR requires casinos to carry out CDD for accounts opened by legal persons under trust arrangement on behalf of a customer, including maintaining a system to verify the legal existence and organisation structure of the legal persons.

297. Section 18 of the CIRR further defines CDD to be risk-based and s.21 requires EDD for casino customers posing a high risk of ML/TF, and permits reduced CDD for lower-risk situations, taking into account risk factors (product/services, purpose of account, materiality and frequencies of funds/transactions etc.) S.10(c) of the CDD guideline notes that CDD is required when there is a suspicion on ML or TF.

298. 22.1 (b) - Real estate agents are not covered persons in the AMLA or TFP SA (RA 10168). There are no requirements for real estate agents to conduct CDD.

299. 22.1 (c), (d) and (e) - Rule 18, Section 1.2 of 2018 IRR contains CDD requirements for occasional transactions for other DNFBPs at a threshold of PHP100,000 (approx. USD 1,900/EUR1,600) or above. AMLA includes those dealers in precious stone and metals having transactions which exceeds PHP1,000,000 (approx. USD19,000/EUR16,000) (s.3 (a)(4-5)), which is ambiguous. Other CDD requirements which apply for FIs in the 2018 IRR also applicable to other DNFBPs, including CDD for suspicious transactions (s.1,2 (d) of Rule 18), identification of agent, beneficial owners, purpose of relationship and on-going monitoring (s.2 of Rule 18). Trust companies are regulated by BSP and subject to same CDD requirements as non-bank FIs under MORN BFI s.4806Q that satisfy this criterion.

300. Some lawyers and accountants included in the FATF definition may not be subject to the AMLA as the definition of covered persons in s.3 of the AMLA excludes lawyers and accountants “acting as independent legal professionals acting in relation information concerning their clients or where disclosure of information would compromise client confidences or the attorney-client relationship”. Rule 2 s.1 (tt) and (dddd) of the 2018 IRR further define independent legal professional refers to those purely litigation, notarial, legal counselling, and/or other services that can only be undertaken by a lawyer. There is no legal reference that lawyers or accountant provided services in s.3(7) are precluded from professional secrecy to permit their exercise of AMLA requirements.

301. *Criterion 22.2* - Section 9(b) of AMLA requires all covered persons including DNFBPs to retain all records of all transactions for five years from the date of transactions.

302. Section 25 of the CIRR further requires casinos to retain all CDD records and casino transactions for at least five years, including CDDs conducted by any other parties (including junket operators and overseas group casinos) on their behalf under s.21(C), (D) and s.22 of CIRR. An officer is required to be appointed to be responsible for the records required under AML/CFT regime and make them readily available upon requests from competent authorities. Casino accounts (though can be examined by authorities under Section 33 of the CIRR) and the electronic AML monitoring system (s.21B) are not mentioned to be under the five year retention requirements in the CIRR. There is no requirement for casinos to obtain or to retain financial transactions conducted by third parties to permit reconstruction of individual transactions.

303. Record keeping requirements contained in Rule 20 in 2018 IRR apply to dealer in precious stones and metal, lawyers, notaries, accountants or other company service providers and satisfy R.11. The scope gap relating to the definition of lawyers and accountants referenced in c22.1 also applies here.—Record keeping requirements in MORNBFI Section 4808Q for non-bank FIs are also applicable to trust companies, in line with R.11. There are no recordkeeping requirements for real estate brokers.

304. *Criterion 22.3* - Section 26 of PAGCOR CDD Guideline applies to all PAGCOR-regulated land-based casinos as is in line with the PEP requirements set out in R.12. Gaps exist with respect to implementation of c.12.1 and c.12.2, as in the CIRR which impact all online gaming operators and CEZA-/APECO regulated land-based casinos—including foreign PEPs—are not required to be considered as high risk. Moreover, there is no requirement for senior management approval before establishing business relationship with foreign PEPs. Filipino citizens are prohibited from participating in offshore (online) gaming under Section 3 of the PAGCOR Offshore Gaming Regulatory Manual, hence there are no requirements relating to domestic PEPs.

305. The CDD requirements for foreign and domestic PEPs in Rule 19 Section 1 of 2018 IRR are applicable for dealer in precious stones and metal lawyers, notaries, accountants or other company service providers. Rule 19 s.1 (1.1) of 2018 IRR applies to other DNFBPs, however covered persons are only required to identify family members and close associates. There is no further legal reference that those individuals shall be subject to additional PEP measures under c.12.1 and c.12.2. The gap related to close associates in c.12.3 applies to BSP-covered persons extend to trust entities.

306. The definition of immediate family members of PEPs for other DNFBPs are set out in the 2018 IRR and include second degree consanguinity or affinity. The definition of family members in Rule 3 (W) of CIRR however is narrower than the FATF requirement.

307. *Criterion 22.4* - The NRA Report 2015-2016 covered the assessment of new technologies in DNFBPs including online casinos, e-games and video streaming table games (remote proxy betting). S.20 of CIRR requires face-to-face requirements to obtain true identify of proxy betting

TECHNICAL COMPLIANCE

account holder but only limited to account opening. S.15 of the CIRR, Rule 19, Section 5 of 2018 IRR for DNFBPs require casinos and other DNFBPs to include the identification, assessment, and mitigation of ML/TF risks that may arise from new business practices, services, technologies, new products and pre-existing products. This satisfies the requirements contained in Recommendation 15. Real estate brokers are not a covered person in the AML regime subject to any new technologies requirements.

308. *Criterion 22.5* - Section 21C of the CIRR, Rule 21 of 2018 IRR and Section 30 of DNFBP AML/CFT guideline permit casinos and other DNFBPs to rely on third parties for CDD provided that the third parties are covered persons in the AMLA or a foreign FIs or DNFBPs with the same level of CDD requirements. The ultimate responsibility of CDD remains with the covered persons. S.21D of the CIRR permits casinos to outsource the conduct of customer identification and due diligence to a counterparty, intermediary or agent. This appears broader than the exception for outsourcing and agency relationships set out in the interpretive note to R.17. S.22 to 24 of PAGCOR CDD guideline permits casinos to rely on the junkets, intermediaries or any counter parties to conduct CDD, identifying beneficiary owners and those parties are required to submit those CDD documents to casinos without delay. There is no requirement for these parties to have an outsourcing or agency agreement with the casino, noting that not all categories are covered persons in the Philippines, or foreign FIs or DNFBPs with the same level of CDD requirements.

309. Section 6.A (c) of CEZA MC 18-001 and Rule 21 of 2018 IRR require CEZA-regulated casinos and other DNFBPs to account country risk for third party reliance. It is not applicable for PAGCOR-regulated casinos. S.25 of PAGCOR CDD guideline, Section 6A (c) of CEZA MC 18-001 and Rule 21 s.1.4 of 2018 IRR fulfil the requirements of c.17.3 for DNFBPs to rely on third party when it is part of the same financial group. It does not apply to on-line casinos regulated by PAGCOR.

310. Real estate brokers are not a covered person in the AML regime subject to the provision related to third parties reliance. Trust companies regulated by BSP are subject to the same requirements as non-bank FIs under MORNBFIs.4806Q, which satisfy R.17. The scope deficiency in c.22.1 related to lawyers/accountants and other TCSPs also applies to this criterion.

Weighting and Conclusion

311. The Philippines has incorporated requirements for DNFBPs (except real estate) into the AMLA and issued separate AML/CFT guidelines for casinos. The discrepancy with the coverage of CDD by casinos and record keeping (noting AMLA only covers cash transactions of casinos), and scope deficiencies in relation to third party reliance present moderate shortcomings. Other shortcomings include the exclusion of the real estate sector from AML/CFT obligations, inconsistency in the definition of lawyers-/accountants as covered and the absence of requirements for DNFBPs to apply additional measures to family and associate of PEPs. Minor deficiencies in R.12 are applicable to BSP-regulated trust entities.

312. **Recommendation 22 is rated partially compliant.**

Recommendation 23 – DNFBPs: Other measures

313. In its 2009 ME, the Philippines was rated non-compliant with former R.16. The major technical deficiencies were that the AMLA did not impose the STR obligations on DNFBPs. The enactment of revised AMLA in 2013 and 2017 extended the suspicious transaction requirements and tipping-off to most DNFBPs.

314. *Criterion 23.1* - Section 9(c) of the AMLA, AMLC Resolution No.61/2016 requires covered persons including all DNFBPs to file STRs, regardless of the amounts involved, within five working days from the date the suspicion is formed. As set out in R.20, this does not meet

the 'promptly' requirement. Rule 17 of the IRR of TFPSPA defines offenses punishable under Section 5 to 8 of TFPSPA are considered as predicate offenses to ML in AMLA and subject to STRs. The deficiencies noted in R.20 in relation to the lack of coverage of tax crimes and attempted transactions extend to DNFBPs. S.34 of DNFBP Guideline requires STR filed for refused transactions when CDD cannot be fulfilled. Scope deficiencies of lawyers and accountants in the AMLA extend to their STR obligation (see c.22.1). There are no obligations for real estate brokers to report suspicious transactions.

315. *Criterion 23.2* - Rule 5 of CIRR (for casinos) include the requirements for institutional risk management policies, appointment of compliance officers (s.13), independent audit functions reporting to board of directors to monitor assessment of the AML/CFT compliance and effectiveness (s.14), employee screening (s.15 sub-paragraph c) and trainings (s.15.c.) Group-wide program is required when the casinos are complex and comprise of multiple business locations (s.15). S.25 of CDD guideline of PAGCOR and Section 15 (b) of CEZA MC 18-001 require PAGCOR land-based casinos and CEZA-regulated casinos to exercise paralleled AML/CFT measures for overseas companies under same group. This does not include PAGCOR on-line gaming operators. Paralleled AML/CFT measures with foreign branches and subsidiaries under Rule 16 Section 8 of 2018 IRR are applicable for other DNFBPs covered persons. The internal controls requirements for other DNFBPs set out in Rule 16 (1), (7) & (8) of 2018 IRR and Section 4805Q for BSP-regulated trust entities satisfied Recommendation 18.

316. Real estate brokers are not subject to internal control requirements. There are scope gaps of certain lawyers and accountants being covered persons in the AMLA.

317. *Criterion 23.3* - CIRR requires covered persons to developed risk-based policies that include the risk of customers from high risk countries (s.10). AML/CFT guideline for DNFBPs defines customers originated from countries with high risk factors, including those called for by the FATF, as high risk and requires covered persons to conduct enhanced CDD (s.26). PAGCOR CDD guidelines extend risk-based EDD requirements for PAGCOR regulated land-based casinos to customers from countries called for by FATF ((s.19(d)).

318. Section 7(7) of the AMLA provides broad power to AMLC that includes issuance of any guideline and circular pertaining to AML. There are no specific policies by supervisors in relation to application of counter measures and notification of higher risk countries of concern. Rule 19(8) of 2018 IRR applies to non-casino DNFBP covered persons and Section 4806Q for BSP-regulated trust entities both largely fulfil Recommendation 19.

319. Real estate brokers are not a covered and the scope deficiency of lawyers and accountants being covered persons in the AMLA per c.22.1 also extend to this criterion.

320. *Criterion 23.4* - Section 9(c) of AMLA states that reporting covered transactions or STRs to AMLC is not deemed to be a violation of the Law on Secrecy of Bank Deposits, the Foreign Currency Deposit Act or The General Banking Law of. Further, filing CTRs or STRs in good faith will not constitute a breach of any criminal, administrative or civil consequences, regardless of whether the report will result in criminal prosecution, provided that the covered persons, their officers and employees are restricted from informing or disclosing the fact that a covered transaction report or STR was made. This is applicable to all DNFBPs. Real estate brokers are not covered persons in the AML regime and are therefore not subject to the tipping-off requirements.

Weighting and Conclusion

321. While a number of the requirements for R.23 have been applied to most DNFBPs, there are deficiencies in the omission of tax crimes as predicate offences and attempted

TECHNICAL COMPLIANCE

transactions subject to STRs (see R.20), real estate agents are not covered and there is a scope deficiencies related to lawyers and accountants. In addition, there is an absence of supervisory measures imposed to casinos for high risk countries that warrant attention by the FATF or by the supervisory authorities.

322. **Recommendation 23 is rated partially compliant.**

Recommendation 24 – Transparency and beneficial ownership of legal persons

323. The Philippines was rated partially compliant with former R.33 in the 2009 MER due to a lack of information held on the beneficial ownership of foreign parent companies of Philippines corporations and beneficial ownership information not being accessible where lawyers acted as the nominee shareholders.

324. *Criterion 24.1* - Article 44(3) of the Philippines' Civil Code divides legal persons for private purposes into three categories:

- Corporations (stock or non-stock);
- Partnerships (general and limited); and
- Cooperatives.

325. Three statutes provide the legislative and administrative requirements for registration and operation in the Philippines of these entities, namely: the Corporation Code for corporations, the Civil Code for partnerships, and the Cooperative Code for cooperatives.

Stock Corporations

326. Stock corporations are divided into two general types: private and foreign.

327. Private corporations have stock divided into shares and are authorised to distribute dividends to its shareholders (s3). Any number of persons, but not less than five (s10), can form a private corporation. A private corporation comes into existence with independent status on issuance of a certificate of incorporation is issued (s19).

328. Foreign corporations (companies formed outside the Philippines) must obtain a license from SEC before they can conduct business in the Philippines (s123).

Non-stock Corporations

329. Non-stock corporations are similar to foundations in other countries: they do not issue shares and no part of their income is distributable as dividends to its members, trustees or officers (subject to dissolution rules - s87). Non-stock corporations may be organised for the following purposes:

- charitable, religious, educational;
- professional, cultural, fraternal;
- literary, scientific, social;
- civil service; and
- other purposes, including trade, industry and agriculture.

330. Specific categories of stock and non-stock corporations can also be formed: e.g. (i) close corporations (Title XII); (ii) educational corporations established as stock corporations (s108)

and; (iii) religious corporations, established as non-stock corporations (s109) to administer and manage the affairs, as trustee, of the property of a religious denomination, sect or church.

Partnerships

331. Partnerships may be formed under the Civil Code by two or more natural persons (art.1767). Under art.1768 a partnership has independent legal status as a legal person. However, unlike corporations, a partnership becomes a juridical person from the time the contract begins, while corporations only become juridical persons upon SEC registration. General partnerships have unlimited liability while limited partnerships have limited liability, although one of its partners must have unlimited liability.

Cooperatives

332. Cooperatives are “autonomous self-help organisations controlled by their members” (art.4(4), Cooperative Code) and acquire separate legal personality upon registration with the Cooperative Development Authority (CDA) under art.16. Cooperatives have limited liability (art.12) and may sue and be sued (art.9(1)). Under art.23 of the Cooperative Code, 20 different types of cooperatives may be formed.

333. *Criterion 24.2* - The Philippines has not assessed the ML and TF risks associated with all types of legal persons that can be created in the country.

Basic Information

334. *Criterion 24.3* - Under the Corporation Code, all applications for incorporation must be submitted to the SEC (company registry). S.14 requires that articles must include the corporation’s name, legal form and status, a list of initial directors, and the address of the registered office (which must be within the Philippines). Basic regulating powers must be lodged with the SEC separately within one month of incorporation (s.46, Corporation Code). Under s.125, foreign corporations registered with the SEC to do business in the Philippines must submit the same information to the SEC for a licence to operate and have a registered agent (s.128) for the purpose of service.

335. In the case of partnerships, the information contained within the Articles of Partnership lodged with the SEC, includes the above as well as basic regulating powers. The SEC maintains an online system that allows the public to access reports for a fee or they may be requested in person. Under Articles 14 and 15 of the Cooperative Code, cooperatives must file Articles of Cooperation and bylaws on registration. Article 14 information disclosure requirements on registration complies with this criterion. The CDA maintains a public list of registered and delisted cooperatives on its website. Further information can be obtained through an on-line freedom of information request.⁹⁴

336. *Criterion 24.4* - Corporations are required to keep and maintain a register of shareholders (‘stock and transfer book’) in the corporations’ registered office or with its stock transfer agent who must be in the Philippines (s.74, para 4, Corporation Code). This book must contain the names of stockholders, the instalments paid and unpaid on all stock, the date of payment for any instalment, a statement of every sale or transfer of stock, the date and the names of the seller and purchaser, and any other entries required by the by-laws.

⁹⁴ <https://www.foi.gov.ph/requests?agency=CDA>

TECHNICAL COMPLIANCE

337. Cooperatives are required (art.52 Cooperative Code) to maintain a registry of members and shareholders together with other information at the office of the cooperative within the Philippines and have those documents available for inspection by the CDA.

338. *Criterion 24.5* - The Corporation Code requires that the information outlined in c. 24.3 and 24.4 is to be kept up-to-date and accurate. An untrue statement or omission to state a material fact may result in penalties. The SEC has taken action against corporations where the information submitted has been found to be false.

339. As for partnerships the Articles of Partnership must contain information as per criterion 24.3 and these should be amended when there is any change to the partnership through written document signed and sworn by all partners and provided to the SEC (art.1864 of the Civil Code).

340. Under Memorandum Circular No. 2012-16, cooperatives are required to update the members' registry regularly in accordance with the policy promulgated by the board of directors. No information was provided to the assessment team on updating the CDA registry, or on available penalties for failing to ensure information is accurate and updated.

Beneficial Ownership Information

341. *Criterion 24.6* - The mechanisms in the Philippines for competent authorities to determine beneficial ownership information in a timely manner relies on using existing information obtained by FIs and DNFBPs, in accordance with R.10 and R.22. However, there are impediments to most competent authorities obtaining this information.

342. Elements of beneficial ownership of account holders in Philippines Stock Exchange can be obtained from the Customer Account Information Form (CAIF). The CAIF is an account opening form and must be completed by any corporate customer intending to engage in stock transactions and must be updated every two years, but not at the point of changes to the details of customers. The information in the form includes the customer's identity and related details and the broker dealer must be reasonably satisfied of the identity of the person ultimately responsible for originating the instruction in relation to a transaction, the person who stands to gain the commercial or economic benefit of the transaction, or who bears the commercial or economic risk. The broker dealer must maintain an electronic database of the CAIF information of its clients and make available to the SEC when requested or during the conduct of an audit.

343. While all FIs and most DNFBPs are required to identify and verify beneficial owners of customers who are legal persons, there is no requirement that all legal persons maintain accounts with FIs. There are impediments to competent authorities using this mechanism to obtain such information from banks as banking secrecy laws hinder competent authorities accessing this information in a timely manner (see R.9 for relevant analysis). AMLC can access records from banks for their own use, or for the use by other authorities, with varying requirements depending on whether the information is for intelligence or regulatory purposes or for use as evidence. There are further impediments on obtaining and sharing such information in relation to PEPs during election periods.

344. *Criterion 24.7* - Rule 18, s.8.3 of the 2018 IRR of the AMLA requires FIs to ensure that information and documents collected in the CDD process are kept up-to-date and relevant based on materiality and risk, by undertaking reviews of existing records, particularly for higher risk categories of customers. There are similar provisions contained in the BSP, SEC and IC Rules and Guidelines. However, these provisions only apply when a legal person opens a relationship with a FI or DNFBP and will only be updated periodically, not whenever beneficial ownership information changes. Under the IRR of the SRC, a broker dealer only has a responsibility to keep

current all material information contained in the CAIF (Rule 52.1.6.15), which goes further than the biannual CAIF update.

345. *Criterion 24.8* - Under Rule 23, s.3.3 of the 2018 IRR, the SEC shall ensure that judicial persons cooperate with AMLC to determine beneficial ownership. SEC requires that at least one natural person resident in the Philippines is authorised to provide all basic and available beneficial ownership information and to give further assistance to AMLC. AMLC requires DNFBPs to provide AMLC with basic information and available beneficial ownership information.

346. *Criterion 24.9* - The AMLA and implementing guidelines require all covered FIs and DNFBPs to comprehensively keep relevant records for at least five years from the date accounts are closed. Additionally, all corporations must make, keep and preserve records (accounts, correspondence, memoranda, etc. as required under s.53.2 of the SRC) for such periods as the SEC by its rules and regulations may prescribe. The SEC retains corporate and partnership records beyond the five-year minimum.

Other Requirements

347. *Criterion 24.10* - Government agencies, including LEAs, can access the SEC database through the online system for basic information for a fee. However, the information is limited as not all corporation information is available. For information that is not uploaded (prior to 1998), requests need to be made directly to the SEC.

348. LEAs can also submit requests to the SEC for information on companies in evidential form. Responding to such requests and transmitting documents to the requesting authority could take a period of one week. Additionally, the 2018 IRR to the AMLA provides that competent authorities (specifically AMLC, other supervising authorities, LEAs) shall have timely access to the basic and beneficial ownership information held by the SEC, covered persons or juridical person.⁹⁵ No further guidance is provided as to the interpretation of 'timely'. It is not clear how this provision would operate to empower competent authorities to benefit from timely access to the relevant information.

349. If competent authorities wish to access basic and beneficial ownership information on cooperatives held by the CDA, they must make a freedom of information request through the FOI portal. A review of the completed requests on the portal show that requests are taking, on average, between three and six weeks to be completed and the requested information provided.

350. Among LEAs, only AMLC is able to obtain access to beneficial ownership information held by banks due to bank secrecy laws (see R.9 for relevant analysis). Instead a request must be made to AMLC, and AMLC will then need to undertake its own procedures to access the information.

351. *Criterion 24.11* - Under s.63 of the Corporation Code no transfer of shares is valid "...until the transfer is recorded in the books of the corporation showing the names of the parties to the transaction, the date of the transfer, the number of the certificate or certificates and the number of shares transferred." Hence, bearer shares are not permissible. The Philippines has also put in place mechanisms for covered persons when dealing with entities that issue bearer shares (for example a foreign entity that issues bearer shares). Where a covered person deals with such an entity, enhanced due diligence must be carried out on the entity and the existing stockholders and/or beneficial owners (Rule IX-A 3 of the Revised IRR of AMLA). The bearer share issuing entity is then subject to ongoing monitoring and the list of stockholders and/or beneficial owners

⁹⁵ Rule 23, Section 4.1, 2018 IRR to the AMLA

TECHNICAL COMPLIANCE

must be updated within 30 days of a transfer of ownership. The new stockholder and/or beneficial owner will then be subject to the enhanced due diligence procedures in place.

352. There is no clear prohibition on the issuance of bearer share warrants in the Philippines. An SEC opinion states that 'the issuance of bearer stock certificates is not allowed under the law', and 'certificates of stock may be issued only to registered owners of stock in a corporation upon full payment of subscription' (SEC Opinion No, 05-02, issued on 31 January 2005). This opinion however does not include bearer warrants which are not stock certificates. There are no measures in the Corporation Code or elsewhere to mitigate the risk associated with these instruments.

353. *Criterion 24.12* - The Philippines does not have any mechanisms in place to address or mitigate the ML and TF risks relating to nominee shareholders and nominee directors as outlined in c 24.12(a) and (b).

354. *Criterion 24.13* - The SRC contains both administrative sanctions and criminal penalties for violation of the SRC, its rules or its orders. Violations include failure to register securities prior to sale or distribution, failure to file required reports, Administrative sanctions include the suspension or revocation of any registration for the offering of securities; a fine of no less than PHP10,000 (approx. USD 191) nor more than PhP1,000,000 (approx. USD 19,000) plus up to two thousand pesos (USD 38) for each day of continuing violation; and other penalties within the power of the SEC to impose.

355. Fines of this nature are unlikely to be effective at dissuading failure to comply with requirements under the SRC. Criminal penalties for persons who violate the SRC or the rules and regulated promulgated by the SEC under the authority of the SRC, comprise fines (PHP50,000 – PHP5,000,000, approx. USD 953 – USD 95,250), terms of imprisonment (7 - 21 years), or both. If the offender is a legal person the penalty may be imposed upon the legal entity or the officer/s of the legal entity responsible for the violation.

356. There is no difference in fines for natural persons and legal persons.

357. For covered persons, non-compliance with the AMLC Guidance on Identifying Beneficial Ownership (in force 27 November 2018) may warrant imposition of administrative sanctions by AMLC under the AMLA and its IRR. Under the AMLC's Rules on Imposition of Administrative Sanctions (RIAS), graduated penalties are provided for based on the risks involved, value and gravity of the offence, and the size of the covered person. These are discussed under R.35.

358. Article 140 of the Cooperative Code provides penalties for violations of the Code, including influencing the appointment of directors, illegal use of information, omission or refusal to furnish any information or report required under the Code, providing false or misleading information, and hindering an authorised person from making an inspection under the Code. Penalties range from between six months to ten years imprisonment and fines of between 1,000 to 500,000 pesos (USD26 to 13,000). Although the terms of imprisonment are proportionate and dissuasive, the monetary penalties available under the Cooperative Code are not dissuasive.

359. Violations of the Corporation Code, including failure to file or amend Articles of Incorporation; failure to meet Director requirements; and failure to adopt appropriate by-laws, are penalised by both fines (P1,000 – P10,000 or USD19 – USD190) and/or imprisonment from 30 to five years. Additionally, if the violation is committed by a corporation, the SEC may dissolve the corporation following notice and hearing. The same concerns arise regarding the financial penalty as did for the sanctions and penalties under the SRC.

360. *Criterion 24.14* - The Philippines SEC, following a request from a foreign enforcement agency on the basis of reciprocity, is allowed to share basic and beneficial owner information contained on its database under s.66.5 of the SRC as well as details of shareholders held.

361. The ability to rapidly provide international cooperation is impacted with regards to beneficial ownership information, as this information is not readily available outside AMLC (see R.9 for further analysis).

362. However any information that has been filed with or transmitted to the SEC, in its role as the company registry, is able to be shared. If the requested information is not available the SEC has the power to subpoena the information under s.5.1(1) or 53.2 of the SRC. This could include requesting beneficial ownership information from FIs.

363. Additionally, the SEC makes the SEC iView available, subject to payment of relevant fees, to competent authorities (and members of the public) in foreign jurisdictions.

364. *Criterion 24.15* - Although the Philippines has provided statistics on requests through Egmont Secure Web made to foreign FIUs involving beneficial ownership information related to legal persons (26 in total, with 13 made in 2018), and the responses to a number of requests, no evidence has been provided to show that the quality of assistance received has been monitored.

Weighting and Conclusion

365. The Philippines has mechanisms to describe the different types of legal persons operating in the country. Basic information maintained by the SEC is publically available, while basic information on cooperatives is available through a freedom of information request. There are no measures in place to mitigate the risk associated with bearer share warrants nor to address the risks relating to nominee shareholders and nominee directors. Access to beneficial ownership information held by banks is limited across competent authorities other than AMLC and BSP due to the operation of bank secrecy laws.

366. **Recommendation 24 is rated partially compliant.**

Recommendation 25 - Transparency and beneficial ownership of legal arrangements

367. The Philippines was rated LC for Recommendation 34 (legal arrangements – access to beneficial ownership and control information). The deficiency noted in the 2009 MER was the lack of an established procedure for obtaining information on beneficiaries and trustees, noting that accessing beneficial ownership information on trusts was likely to be a cumbersome process. The new Recommendation 25 is much more detailed than the previous standard.

368. There are four general categories of express trusts in the Philippines: private donative trusts, charitable trusts, foreign trusts, and business trusts. Private donative trusts include discretionary trusts, bare trusts and testamentary trusts.

369. Of the four general trust categories noted above, only business trusts are subject to regulation by the BSP. S.79 of the General Banking Law of 2000 permits a stock corporation or a person authorised by the Monetary Board to act as a trustee, referred to as a 'trustee entity'. The Monetary Board authorisation required under s.79 of the General Banking Law applies to a 'trust business'. While the MORB defines a 'trust business' as any activity resulting from a trustor-trustee relationship, an isolated or single transaction is not considered as "doing business" under

TECHNICAL COMPLIANCE

the MORB. This is consistent with case law,⁹⁶ which states that the term “doing” or “engaging in” or “transacting” business implies a continuity of commercial dealings, and specifically that a single or isolated business transaction or occasional, incidental and casual transactions do not come within the meaning of the term “engaging in business.”⁹⁷ Therefore, in addition to the other categories of trusts that are not subject to the regulatory requirements outlined below, trustees dealing with legal arrangements through occasional, incidental and casual transactions are not captured under Philippines law.

370. Business trustee entities are regulated by the BSP. As at 11 September 2018, there were 39 of these trustee entities operating in the Philippines. AML/CFT regulation in the Philippines with respect to legal arrangements is limited to those managed by these trustees, and not to the totality of all legal arrangements. As such, compliance with R.25 suffers from gaps in the scope of measures and the below criterion are assessed against this.

371. *Criterion 25.1* - AMLA classes trustee entities as ‘covered persons’ thereby obligating them to undertake CDD under the 2018 IRR, including identifying the beneficial owners. S.X806 of the MORB requires covered persons to collect basic information as well as identify and verify the true identity of the customers, the identity of the beneficial owners (including taking reasonable measures to verify), as well as the ownership and control structure of the customer. Subsection X806.2 item a(3) of Part 8 of the MORB further requires trustee entities to obtain and hold adequate, accurate and current information on the identity of the settlor, the beneficiary and any other natural person exercising ultimate effective control over the trust. .

372. Following the amendments made to Part Eight of the MORB by BSP Circular No.1022 in November 2018, Subsection X806.2 requires trustees to hold basic information on other regulated agents of, and service providers to, the trust.

373. AMLA requires trustee entities, as covered persons, to retain all records on customer identification, account files and business correspondence for at least five years from the date of closure. The BSP can only access this information as part of its supervisory activities, however AMLC can access it anytime due to the trustee entities’ status as ‘covered persons’. The MORB also requires covered persons to maintain all customer identification records and transaction documents for at least five years from the date the account closes.

374. There are no similar obligations on trustees of non-business trusts (private trusts).

375. *Criterion 25.2* - Subsection X806.3 of the MORB requires covered persons to ensure they have established the ‘true and full identity of their customers’, and update all customer identification information and documents, as required to be obtained under the AMLA, on the basis of materiality and risk.

376. There are no similar obligations on trustees of non-business trusts (private trusts).

377. *Criterion 25.3* - Under s.X806.2 the MORB, as amended by BSP Circular No. 1022, trustees are required to disclose their status when entering into a business or professional relationship, as well as when they carry out an occasional threshold transaction. There are no similar obligations on trustees of non-business trusts (private trusts).

378. *Criterion 25.4* - Trustee entities are not prevented from providing the regulator, BSP, with any information relating to a trust. Subsection X808.3 of the MORB places an obligation on the trustee entity to make available to the BSP, without delay, all records and documents required to be retained under the AMLA. Subsection X806.2, as amended by Circular 1022, further provides

⁹⁶ The Mentholatum Co., Inc., et al. vs. Mangaliman, et al (72 Phil 525 [1941])

⁹⁷ Top-Weld Manufacturing Inc. vs. ECED, S.A. (138 SCRA 120)

that trustees shall make available information on the assets of the trust and beneficial ownership to competent authorities to the extent allowed by law.

379. There are no similar obligations on trustees of non-business trusts (private), however there are also no enforceable means preventing the provision of such information.

380. *Criterion 25.5* - While AMLC and BSP can request information held by FIs and DNFBPs (including trustee entities), these powers do not extend to other law enforcement authorities. There is also a gap in powers available regarding trustees dealing with legal arrangements through single or isolated business transactions, occasional, incidental and casual transactions, or non-business trusts.

381. If a trustee opens an account with a securities broker, the securities broker must be furnished with a copy of the trust deed. The trustee must disclose the identity of the beneficial owner. The SEC is able to require the broker to provide the beneficial ownership information and the account opening documents under the 2015 SRC Rules. Law enforcement authorities can request this information from the SEC.

382. *Criterion 25.6* - BSP must be granted authorisation by the Monetary Board or the Governor before it can share information of a confidential nature or information about the condition or business of a BSP-supervised entity.⁹⁸ The international cooperation must also be consistent with any existing cross-border supervisory arrangements.

383. This leaves gaps with respect to trustees of non-business trusts (private).

384. AMLC can share information in relation to trustee entities that are covered persons with foreign counterparts, including making inquiries and issuing orders to the covered person to determine the true identity of the beneficial owner of property or other information, subject to a request from a foreign State (s.7(2) of the AMLA). The SEC, insofar as it holds or requests information under criterion 25.5, can share basic and beneficial ownership information with foreign counterparts under s.66.5 of the SRC.

385. While these mechanisms provide competent authorities with the ability to share information for international cooperation purposes, the requirements for Monetary Board authorisation (BSP), as well as the need to seek AMLC assistance to access information held by banks, do not allow for this information to be shared rapidly.

386. *Criterion 25.7* - The MORB (s.X802) provides that, as trustee entities are under the regulation and supervision of the BSP and need to comply with the AML rules and regulations, they are covered by the sanctions set out under the MORB and AMLC. Part Eight of the MORB provides sanctions and penalties for violations of that part, which includes identification, verification and record keeping. Non-monetary sanctions include written reprimand, restriction on certain licences, suspension and disqualification. BSP can also impose monetary penalties in coordination with AMLC.

387. There are no similar obligations on trustees of non-business trusts (private).

388. For covered trustee entities, Section 14(b) of AMLA provides a penalty of six months to one year imprisonment, and/or a fine of between 100,000 and 500,000 pesos (USD 1,865 – 9,329) for failure to comply with record keeping obligations. Rule 15 of the 2018 IRR also provides for administrative sanctions, including monetary penalties and warnings for violation of the AMLA and the 2018 IRR, which includes identification and verification obligations (Rule 9 of the 2018

⁹⁸ Sections 16 and 27, New Central Bank Act

TECHNICAL COMPLIANCE

IRR) as well as record keeping (s.9 of the AMLA and Rule 9 of the 2018 IRR). Monetary penalties are left to the discretion of AMLC but shall be no more than 500,000 pesos per violation (USD 9,329). Although the sanctions under the MORB are not significant, the penalties provided for under the AMLA and the 2018 IRR are proportionate and dissuasive. These however do not apply to trustees dealing with legal arrangements through single or isolated business transactions or occasional, incidental and casual transactions, as they are not covered persons under AMLA.

389. *Criterion 25.8* - If a trustee entity fails to provide timely access to information regarding the trust referred to in criterion 25.1, the New Central Bank Act provides criminal and administrative sanctions against the bank or individual acting as trustee as outlined in 25.7 above. However these penalties, particularly those under the MORB, are not proportionate and dissuasive, given that all trustees currently authorised in the Philippines are corporations. There are no similar obligations on trustees of non-business trusts (private trusts).

Weighting and Conclusion

390. There are limited measures in place with respect to business trusts only. There are no obligations on trustees of non-business trusts (private trusts) to obtain and hold adequate, accurate, and current information on the identity of the settlor, the trustees, the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust. There are no obligations on private trustees to disclose their status to financial institutions and DNFBPs when forming a business relationship or carrying out an occasional transaction above the threshold. Beneficial ownership and control information for private trusts is not available. The penalties available if the trustee entity fails to provide timely access to information regarding the trust are not proportionate or dissuasive.

391. **Recommendation 25 is rated partially compliant.**

Recommendation 26 – Regulation and supervision of financial institutions

392. In its ME 2009, the Philippines was rated partially compliant with former R.23. Deficiencies included a lack of explicit provision prohibiting the licensing of shell banks; BSP did not conduct on-site examinations of MVTS providers and on-site AML examinations of IC were not risk-based.

393. *Criterion 26.1* - Section 3 of the AMLA defines supervising authorities as the appropriate supervisory or regulatory agency, department or office supervising or regulating covered institutions. In relation to FIs, The FI supervisory authorities under Rule 2 S.1 (www) of the 2018 IRR includes i) the BSP for bank sector (including non-bank financial institutions performing quasi-banking functions and those engaged in money value transfer services or foreign exchanges), ii) the SEC for the securities sector and iii) the IC for the insurance sector. These supervising authorities are required to issue AML/CFT guidelines (s.18 of the AMLA and Rule 7 Section 2.2 of 2018 IRR), and Rule 27 of IRR of TFPSA set out the functions of supervisory authorities to assist AMLC in AML/CFT supervision including issuance of guideline, monitoring AML/CFT compliance of covered persons and taking appropriate supervisory actions for deficiencies. Those supervision functions are also applicable AMLC pursuant to Rule 7 Section 1.2.

394. Some financing and lending companies are included as other entities regulated by SEC under Section 3(i) of the AMLA. The SEC Memorandum Circular No.16/2018 only covers

financing and lending companies with foreign holding over 40% in voting stock or with paid-up capital of PHP10 million or above⁹⁹.

395. *Criterion 26.2* - BSP licences all entities or persons engaged in banking operations and quasi-banking functions (S.6 & 14 of The General Banking Law (RA 8791)). S.4 of the Revised Non-Stock Savings and Loan Association Act (RA 8367) specifies that non-stock saving and loans associations (NSSLAs) shall obtain license from the BSP prior to operation.

396. The BSP is also the registration authority for persons or non-bank entities that are eligible to operate as foreign exchange dealers, money changers and remittance transfer entities (including e-money issuers) pursuant to Circular 471, series 2005 (as amended by Circular 942, series 2017 and incorporated as Section 4511N of the MORNBF1).

397. SEC licenses / registers all companies and professional within the financial and capital markets. This includes brokers, dealers, salesman and associated persons that engaged in trading of securities (S.28 of the Securities Regulation Code (RA 8799 or the SRC). Mutual funds and close-end investment companies are subject to SEC licensing (s.7 of the Investment Company Act (RA 2629)) as are investment advisors/fund managers (s. 5.1 of its IRR (2018)). Investment houses (securities underwriter) are subject to registration requirements with the SEC (s.4 of Investment Houses Law (PD 129)).

398. Financing companies and lending companies are governed by separate laws, namely the Financing Company Act 1998 (RA 8556) and the Lending Company Act 2007" (RA 9474). These entities are required to be licensed by SEC prior to operating, including those excluded from AML/CFT supervision by the SEC (see c.26.1).

399. IC licences various entities under the Revised Insurance Code (RA 10607). License renewal every three years applies to insurance companies (S.193), mutual benefit associations (S.404), servicing insurance companies (those with restricted insurance operations by IC) (s.287), reinsurers (S.288), and insurance intermediaries including the agents and insurance brokers (s.307). Pre need companies are subject to yearly licence renewals (s. 10 of the Pre-need Code (RA 9829)). Since 2015, transferred the supervision of health maintenance organizations (HMOs) from the Department of Health (DOH) to the IC and the licensing requirement is continued as per Section 5 of the EO.

400. Under MORB Section X806.2 (o) of BSP Circular 1022 series 2018, shell bank are not allowed to operate or be established in the Philippines.

401. *Criterion 26.3* - Section 27 of the Corporation Code provides that no person convicted by final judgment of an offense punishable by imprisonment (local) for a period exceeding six years, or a violation of this Code committed within five years prior to the date of his election or appointment, shall qualify as a director, trustee or officer of any corporation.

402. Rule 4 (3.4) of 2018 IRR requires all supervisory authorities to take necessary measures to prevent covered persons from being controlled by criminals or their associates through shareholding, beneficial ownerships or management functions. The BSP has the power to assess fit and proper for banks and quasi-banks, including incorporators and subscribers (stockholders) of an entity applying for bank license (s.14 of RA8791); appointment of directors and officers (s.16 of RA8791); and in a transaction of voting stocks (MORB X.126.2) that will

⁹⁹ As of 2017 there were three financing companies with foreign equity of more than 40% and 428 with paid up capital of PHP10 million or more. As a result 431 financing companies (63%) are captured as covered persons, out of a total of 681. With respect to lending companies, in 2017 there were 4 with foreign equity of more than 40% and 72 with paid-up capital of PHP10 million or more. 76 (3%) are therefore captured as covered persons, in a market of 2,525. In 2018, around 72% of financing companies are BSP-regulated (in terms of asset size).

result in i) transfer of ownership/control over 20% of voting stocks, ii) making someone elect or to be elected as director of the bank, iii) any sales or transfers that would result in a change in majority ownership, or iv) change of control of voting stocks of a bank from one group of persons to another group. Under Appendix 37 of s.X102 of MORB (vol. 2), the BSP requires fit and proper of the directors, officers, incorporators and subscribers in terms of integrity, financial capacity, and specifically must not have been convicted of any crime involving moral turpitude. There is no definite range of crimes under the term moral turpitude and the definition can change depending on Supreme Court decisions. MORB s.X150.1 and X150.2 prohibits a person from holding a director or officer position in banks when there is any conviction to specific offenses involving dishonesty or breach of trust; a sentence for a maximum term of imprisonment of over six months by a court; convicted by court for violation of banking laws, or previously noticed by the BSP for those bank violations or those previously removed from those positions by the BSP.

403. Foreign banks must be established, reputable and publicly listed in the home jurisdiction (s.3 of the Foreign Bank Liberalization Act). Appendix 37 of s.X102 requires foreign banks to provide certification from its home supervisor with relevant supervisory information on foreign bank subscriber.

404. Section 4511.2b in BSP Circular 942 S. 2017 requires the proprietor, partner, directors or principal officers for MSBs including FX dealers, money changers and RTC and non-bank e-money issuers (EMI), to be fit and proper. This assessment is based on their integrity, probity, market reputation, competence and financial capacity. For any MSBs based abroad, proof of remittance operator license issued by the overseas home authority and document evidence the operator is subject to AML requirements.

405. Section 22 of RA8367 requires integrity of organisers, administrators, trustees, and officers of the NSSLAs. MORNBF Section X.4143S provides the fit and proper requirements for directors and officers, same as applicable to banks.

406. The SEC has the power to refuse or suspend the registration of securities brokers, dealer and salesmen (SRC S. 29.1d). For investment companies and investment advisor/fund managers, SEC has powers to disqualify an officer, director, member of an advisory board, investment adviser, or depositor of any registered investment company, or principal underwriter for any registered open-end company (S.8(a) of RA 2629). For investment companies operating as fund managers SEC has the power to apply fit and proper criteria for to prevent criminal influence on directors, key officers and shareholders (s.5.1 (5.1.1c) 2018 IRR of RA2629). Lending companies must be formed as a stock corporation (s.4 of RA9474) and are only subject to the fit and proper requirement under S.27 of the Corporation Code covering directors and officers.

407. The revised Code of Corporate Governance Rules for SEC-supervised entities (art.3(E) of SEC Memorandum Circular NO.6, s.2009) requires directors to not have any convictions for offences related to integrity and honesty, misconduct or wilful violations in banks and securities sectors. Further, directors must not have had any suspension of a registration or licenses issued by SEC or BSP. The fit and proper requirements do not apply to prevent criminals from being shareholders and beneficial owners of SEC-covered persons (except investment companies).

408. The IC has the power to assess the integrity of the management (the organisers and administrators) in granting licenses for insurance companies (s.193) and mutual benefit associations (s.404). S.193 also requires fit and proper qualification for the election and appointment of directors and officers for insurance companies. S.11 of RA9829 requires fit and proper checks of preneed companies. IC Circular 13-2004 provides clear guidance that

stockholders, directors, trustees or officers of insurance entities and mutual benefit associations must be in good moral character, and Circular 2005-31 (guidelines on corporate governance) requires directors to not have been convicted of an offence involving dishonesty or breach of trust, violation of insurance laws or there to be derogatory information with any court or LEA that adversely affects its integrity. IC Circular No.2016-51 set out the fit and proper requirements for HMOs however only for directors and officers only.

409. *Criterion 26.4* - BSP has adopted Basel Core Principles in their banking supervision. In relation to Principle 29 on abuse of financial services, existing provisions under the AMLA and 2018 IRR, as well as other existing BSP AML regulations incorporated into Part 8 of the MORBs, provide adequate AML requirements, including CDD, to prevent financial abuse within the Philippines banking and financial system. BSP has adopted a risk-based supervisory approach to conduct examinations of FIs that includes assessment of corporate governance, risk management process, robustness of internal controls, and review of the institution operations and overall risk profile (s.X001 of the MORB and s.4001Q of the MORNBF). Further, under Rule 7 of 2018 IRR supervisory authorities (including the BSP) shall monitor AML/CFT compliance of FIs and apply a risk-based approach by identifying the ML/TF risks of their sector, and applying consolidated group supervision to FIs for AML/CFT purpose. BSP has a framework in place to conduct consolidated group supervision pursuant to Resolution No.553 (1998), which includes overseeing overseas branches and subsidiaries. BSP has instruments in place to permit supervision of cross-border banking groups and share information and cooperate with key foreign counterparts for effective supervision. Minor gap exists in relation to the rules for information sharing between home and host supervisors, which need to be updated in order to align with the MOUs (see c.40.16).

410. SEC is a member of IOSCO. The Financial Sector Assessment Program related to IOSCO was conducted in 2002. The SEC was found to comply with IOSCO in terms of ensuring market entry standards for intermediaries, namely broker dealers, financing companies and investment houses, and ensured fit and proper of operators of collective investment scheme, namely the investment companies. The report also indicated that requirements are in place (SRC s.28 & 30) for broker dealers to maintain sound internal control and require appointment and registration of associated person (compliance officer) for every broker dealer.

411. IC, as member of the International Association of Insurance Supervisors (IAIS), adopted the Core Principle No.22 in AML/CFT supervision in issues guidelines. Risk-based AML/CFT supervision under Rule 7 of 2018 IRR is also applicable to IC in line with the insurance core principles. S.437 of Insurance Code and IC Circular Letter No.2018-61 provide IC the legal framework for international cooperation with foreign counterparts, however the circular does not fully adopted Core Principle 3 (Information Exchange), in particular the lack of proactive exchange of material and relevant information with supervisors of the same group.

412. As set out in criterion 26.1, MSBs are subject to licenses and supervision of the BSP.

413. *Criterion 26.5* - BSPs examination procedures are risk-based and governed by the Revised Examination Manual of AML/CFT Activities (March 2014). Memorandum 2012-17 governs the rules for the AML/CFT risk rating system (ARRS) which rates the level of AML/CFT compliances in banks. BSP establish risk profiles for banks through ARRS to determine frequency of on-site examinations of banks. Banks with a rating of 4 (sound system) are not subject on-site examination every three years. The BSP issued Sector Guidance No. 2018-07 provides clear rules for the frequency of BSP examination to be based on characteristics, institutional frameworks and risk profiles of each banks (ARRS rating). Prioritised banks are subject to on-site examination by more expert personnel and lower risk banks are allocated to other departments. The risk-based model has not been inputted with timely information of the broader ML/TF risk context present in the sector and country to inform priority of sectoral risk

TECHNICAL COMPLIANCE

in its supervision. S.20 of RA 8791 requires that any bank in the Philippines that is authorized to set up branch offices overseas shall be align with head office (or otherwise shall notify the BSP) and will be treated as one unit to permit group supervision. The BSP also conducts special examination trigger by events that pose significant risk to the sector. Approval is required from the monetary board for such examinations.

414. In the MSB sector, only higher risk covered persons are subject to on-site examination. The BSP internal supervision manual “Risk Profiling Guidelines for MSBs” provides the framework for on-site examination to be determined through a systematic risk profiling process to identify those higher risks MSBs for on-site examinations.

415. SEC has an AML/CFT unit under the Enforcement and Investor Protection Department (EIPD) delegated to carry out AML/CFT examination of SEC regulated FIs, except those covered person which are an affiliate or subsidiary of a bank or quasi-banks. In 2018 SEC has formulated an on-site examination manual. Part 3 (s.2) of the procedures set out the pre-examination process which permits flexibility dependent on the risk profile of the institution and their past examination results (s.3).

416. In relation to the insurance sector, IC formed an AML department in 2015. AML examinations are performed annually and on a risk-sensitive basis focused on higher risk life insurance products. IC’s AML/CFT Compliance Checking Manual 2018 (AMLCG Division Memo No. 2018-01) outlines the risk-based approach for on-site examinations.

417. *Criterion 26.6* - Section II.A(1) of the Revised Examination Manual of AML/CFT Activities requires BSP examiners to gather information and understand the risk profiles and major developments of FIs prior to the conduct of an annual on-site examination. The ARRS also supports BSP’s understanding of whether the AML/CFT risk management policies and practices, internal controls of banks and other FIs are in place, well disseminated and effectively implemented. The BSP has utilised the ARRS since 2012 and other off-site surveillance tools to maintain the understanding and updating risk profiles of banks pursuant to on-site examinations or during the follow-up process (overseeing examination). The system is also applied for the supervising of MSBs. The risk rating of covered institutions is reviewed as part of planning of on-site examinations to identify institutions that require prioritised actions, including corrective action, sanction or additional supervisory action. According to MORB Section 811, the ARRS for banks is updated after every on-site examination for formulating the supervisory actions to be taken (e.g. fine penalties). S.VI of the manual of ARRS for MSBs states that the risk profiles for the covered institutions are updated on annual basis.

418. SEC’s examination procedures provide the grounds for maintaining the risk profile of covered persons. Part 3 (s.3.1.8) of the SEC manual requires the updating of risk assessments on an on-going basis. Risk profiles are updated during the on-site examination.

419. IC’s Compliance Checking Manual requires the ML/TF risk profile to be reviewed during on-site examination. Noting the deficiency in c.26.4, it is not clear whether the risks of IC-FIs are being updated on group basis.

Weighting and Conclusion

420. Gaps exist in the market entry requirements of FIs, including that SEC does not apply fit and proper requirements to prevent criminals from being shareholders and beneficial owners of SEC-covered persons (except investment companies) and IC has fit and proper requirements for directors and officers of HMOs only. Some financing and lending companies are excluded as covered persons. The BSP risk-based model does not include timely information

of the broader ML/TF risks presented in the country to inform priority of supervision on sectoral basis. Information exchange has not been implemented by IC (IAIS Core Principle 3).

421. **Recommendation 26 is rated largely compliant.**

Recommendation 27 – Powers of supervisors

422. In its 2009 MER, the Philippines was rated largely compliant with former R.29. The deficiencies were included a lack of proportionate administrative sanctions available to the FI supervisors.

423. *Criterion 27.1* -Rule 2 & 7 s.2.2 (b)(c) of the 2018 IRR and Rule 27 of IRR of the TFPISA provides BSP, IC and SEC the power as the competent authority for monitoring and ensuring compliance with FI covered persons.

424. BSP has the power under the New Central Bank Act (s.3) to supervise banks and quasi-banks. The General Banking Law (s.4) further sets out the supervisory power, includes establishing standards of operation, oversight to ascertain that laws and regulations are complied with, and the ability to enforce corrective action.

425. Section 5.1 of the SRC provides SEC the powers to regulate, investigate and supervise the activities of securities dealers, brokers, salesmen to ensure compliance. S.19 of Omnibus Rules and Regulations for investment house and Securities underwriters 2002 (for investment houses), s.4 of RA 8556 for financing companies and s.9 of RA 9474 for lending companies reiterate SEC's power. Under s.1.2.4 of SEC AML/CFT Guideline 2018, financing and lending companies subject to AML/CFT requirements are only those having more than 40% foreign participation in its voting stock or with paid-up capital reaches PHP10 million (approx. USD 195,500). S.35 of RA 2629 provides the authority to SEC issue rules and regulations or orders as are necessary or appropriate to investment companies.

426. Section 437 (Chapter 6, Title I) of the RA 10607 defines the power of the IC to issue rulings, instructions, circulars, orders and decisions as may be deemed necessary for enforcement of the code. The supervisory power of IC is further set out in s.6 9(c) of RA 9829 over the pre-need companies and s. 4 of EO No.192 over HMOs.

427. *Criterion 27.2* - Rule 7 s.2.2 (c) of 2018 IRR provides the powers to BSP, SEC and IC to perform compliance checking over the covered persons under their supervisions on behalf of AMLC. The New Central Bank Act (s.25) provides BSP with the power to conduct periodic or special examinations on banking institutions and quasi-banks (including their subsidiaries and affiliates engaged in allied activities), NSSLAs and MVTs providers. The same is set out in s.22 of RA 8367 for NSSLAs. S.4.1 of RA 8791, which defines the power of BSP, also includes conducting examination to determine the legal compliance of regulated entities (s.4.1) and over bank subsidiaries during the examination (s.7).

428. Section 52.1 of the SRC (for securities brokers and dealers) and s.28 of RA 2629 (for investment companies) states that persons/entities subject to registration under the law shall prepare and maintain all books and records that will be subject to periodic, special or other examinations at any time by the SEC. S.39 of RA2629 and s.19 of Omnibus Rules and Regulations (2002) for investment house provides the SEC with the power to conduct examination and investigations for investment companies and investment houses, Rule 8 of IRR of RA9474 permits the SEC to examine the books and records of lending companies. The power for inspection of financing companies is supplemented by Rule 7 s.2.2 (s) of 2018 IRR of the AMLA for AML/CFT inspection. S.253 of RA 10607 (for insurance companies) and s.46 of RA 9829 (for pre-need companies) stipulates that IC can conduct an examination at least once a

year or any time necessary over institutions subject to these laws. S.4(f) of EO 192, series 2015 provides IC the power to carry out examinations over HMOs.

429. *Criterion 27.3* - Section 25 of RA 7953 provides the power for the BSPs to require any director, officer, or employee of any institution under its supervision or subject to its examination to compel the presentation of all books, documents, papers or records necessary to ascertain the facts relative to the true condition of those institutions, and also the books and records of persons and entities relative to or in connection with the operations, activities or transactions of the institution under examination. Sections 52.1 and 53 of the SRC provide the powers for the SEC to require books and records in any investigation, or any periodic, special or other examinations at any time. S.28(b) of RA 2629 requires a registered investment company and its subsidiaries to maintain all accounts, books, and other records, which shall be subject at any time or any periodic, special and other examinations by the SEC. S.19 of Omnibus Rules and Regulations for Investment House and Underwriter of Securities provides the SEC with the power to obtain books and records during examination with any applicable laws. Rule 7 of IRR of RA9474 requires lending companies to maintain books and records. Correspondingly Rule 8b) provides the SEC power to examine those records. The supervision and investigation power of SEC in Section 5.1 also applies for financing companies and permits the authority to compel any information.

430. In relation to the IC, s.252 of RA 10607 set out the books and records requirements of insurance companies and under Section 253 the IC can, during examination, require insurance companies to submit all books and records. S.45 of RA 9829 and Section 4.f of EO No. 192, series 2015 provides IC the power to demand the books and records from pre-need companies and HMOs. S.60 of IC Circular 2018-48 provides clear power to IC to demand all IC covered person records necessary for AML/CFT compliance examination.

431. *Criterion 27.4* - Section 7(7) of the AMLA defines AMLC as the only authority to impose administrative/criminal sanctions set out in Section 14 of the law. S.14 (f) permits the AMLA to define the rules for fine and penalties to be applied for administrative sanctions. S.7 (10) of the AMLA provide the legal basis for AMLC and the BSP to enter into an MOU which establishes the framework for the BSPs to refer any AML violations/findings observed during its AML/CFT examinations to AMLC to further investigate with the covered persons involved (s.IV A.b of the MOU with the BSP) and to enable AMLC to enforce the sanctions in Section 14 of the AMLA, which includes both imprisonments and fines (see c. 35.1 for those AMLC-governed penalties).

432. In May 2017 AMLC issued guidance on “Rules on the imposition of Administrative Sanctions”, which formalises the procedures for supervising authorities to refer non-compliance to AMLC. The guidance document contains a broad range of circumstances in which AMLC can impose administrative sanctions, and the method to calculate the fines to be imposed.

433. Without prejudice to any sanctions that the AMLA may have imposed to the covered persons, the BSP can exercise its powers contained in the New Central Bank Act to enforce sanctions over AML/CFT non-compliance. AML/CFT non-compliance is considered a form of “conducting business in an unsafe and unsound manner” and is therefore subject to sanctions pursuant to s.37 of the RA7953. The BSP extends its power of sanctions for AML/CFT non-compliance in Sec. X811 over all BSP-supervised covered persons (including MVTS providers), including written reprimand, restriction on certain licenses/products, suspension the directors/officers from office, and disqualification of directors/officers to hold a position in any covered institutions, and the development of a corrective action plan (when an FI has a low rating under BSP’s AML/CFT risk rating system) and fine penalties. Suspension of licenses is set out in the New Central Bank Act for quasi-banks and s. 4511N.15 for MVTS providers. The BSP has the power to place banks under receivership and liquidation under s.30 any wilful violation of a cease and decess order resulted from any wilful failure or refusal to comply with

BSP regulations or conducting business in unsafe manner. S.4631S in MORNBF1 provides the BSP the power to suspend the license of NSSLAs under the grounds of repeated or wilful violations of rules and regulations promulgated by the BSP.

434. SEC is empowered to impose sanctions, including suspension of licenses, and the range of sanctions is contained including fine penalties, suspension or revocation of registered securities products (s.5.1 c) and f) of RA 8799 (SRC)). The sanction imposed by SEC under Section 12.2 of the SEC Revised AML/CFT Guideline 2018 referred to s.54 of SRC.

435. Section 254 of RA10607 states IC has the power to revoke the licence of an insurance company for any failure in legal compliance and Section 438 provides other types of the sanctions available. The AML guideline of IC (Circular 48-2018) provides IC with clear power and rules of administrative sanction (s.61 to 63) to covered persons, including fine penalties (that cannot be duplicated if has been fined by AMLC for same non-compliance), disqualification of directors and management and impairment to license renewal.

436. There are gaps with the administrative liability of directors and management of SEC regulated institutions that are legal persons.

Weighting and Conclusion

437. There are gaps with the administrative liability of directors and management of SEC regulated institutions that are legal persons.

438. **Recommendation 27 is rated largely compliant.**

Recommendation 28 – Regulation and supervision of DNFBPs

439. In its 2009 MER, the Philippines was rated non-compliant with former R.24. The major deficiencies were that casinos and other categories of DNFBPs were not covered in the AMLA or subject to any AML/CFT supervision and monitoring of compliance. The Philippines included dealers of precious stones and metal, company service providers, lawyers and accountants for AML/CFT supervision in the subsequent revisions of AMLA in 2013 and casinos in 2017.

Criterion 28.1

440. 28.1 (a) - All casinos are required to be licensed. The Philippines Amusement and Gaming Corporation (PAGCOR) is the national-wide casino regulator that covers the whole country, except those special economic zones that are granted power to operate and license casinos independently, namely the two zones/freeports governed by the Cagayan Economic Zone Authority (CEZA) and the Aurora Special Economic Zone Authority (APECO).

441. PAGCOR has the power (s.8 and 10 of PD 1869) to issue land-based casino licenses, offshore internet gaming licenses (internet gaming), onshore internet gaming (e-game sites) and for ship-based casinos (s.14) in the territorial waters of the Philippines except those covered by the gaming supervisors of special economic zones. PAGCOR is also the operator of national-owned casinos that are not subject to licensing.

442. Section 6 (f) of RA7922 provides CEZA the power to grant gaming license for all types of casinos in the Cagayan Economic Zone and Freeport, either on its own or through a subsidiary or a third party. CEZA subsequently outsourced its gaming power to two private entities, through “Master Licensor Agreements” for granting sub-license to other third parties and regulating online (interactive) gaming and land-based casinos in the zone.

TECHNICAL COMPLIANCE

443. APECO is granted the power to operate gaming either its own, through a subsidiary entity, or through concession or license under Section 12 of Republic Act 9490 as revised by Section 6 (f) of Republic Act 10083.

444. 28.1 (b) - Rule 7 s.2.2 (d) of 2018 IRR requires supervisors to take measures to prevent criminals or their associates from holding significant controlling interests, beneficial ownerships and management functions. The fit and proper requirements for PAGCOR are set out in Section II of Responsible Gaming Scope of Practice applicable to for all types of PAGCOR-licensees. In granting license, the PAGCOR requires information on integrity, financial soundness, and business ability of applicants and suitability of board of directors. Under Annex B of the Code, the board of directors, compliance officer representing a gaming corporation, sole proprietors and partners are subject to submission of personal disclosure statement (PDS) to PAGCOR on annual basis. The PDS contains the necessary information for PAGCOR to preventing criminal influence for individuals filing the PDS. However, the PDS also does not apply to individual shareholders holding significant interests or who are not board of directors, or any beneficial owners.

445. CEZA and APECO comprise of two-layered licensing: master licenses and sub-licenses. S.6 1.d.1 of CEZA Interactive Gaming Rules and Regulation set out the probity check requirement on key officials in terms of finances, integrity, competence and criminal history of applicant of master licensors. The fit and proper requirements of online gaming operators (sub-licenses) are further stipulated under s.17(c & d) and s.18 of same regulation, which require that the financial resources of the applicant are not sourced from illegal activity and that there must be a satisfactory corporate, ownership and trust structure. S.19 set out the fit and proper rules for operators with a license recognised by CEZA and master licensor in terms of their ability in AML/CFT.

446. There is no fit and proper requirement for master licensor of APECO. APECO applies fit and proper rules the same as CEZA for sub-license, as set out in Section 5.3 of APECO Online Gaming Rules and Regulations. No information was provided on the fit-and-proper requirements for land-based casinos licensed by CEZA and APECO.

447. 28.1 (c) - Casinos were incorporated as covered persons in the AMLA in the amendment RA 10927 in August 2017. S.18 of the AMLA delegates AMLC, PAGCOR, CEZA and APECO to jointly issue the guideline "Casino Implementing Rules and Regulations (CIRR)". Under Section 6E and Section 8 of the Casino Implementing Rules and Regulations (CIRR), PAGCOR, CEZA and APECO are the competent government agencies to supervise, assess and monitor the compliance of casinos with the AMLA. Under Rule 7 s.1.2 of 2018 IRR, AMLC has the authority to conduct its own compliance checking.

448. *Criterion 28.2* - Casinos are subject to AML/CFT supervision by PAGCOR, CEZA and APECO pursuant to s.18 of AMLA and s.8(a) of CIRR. Entities engaged in trust businesses under RA 8791 are covered persons under s.3(a)(1) of the AMLA subject to supervision of the BSP to ensure AML/CFT compliance.

449. Lawyers, accountants, CSPs, dealers of precious metal and stones are covered persons in s.3(a) of the AMLA. AMLC has a broad power in the AMLA under Section 7(7) to implement measures necessary for the Act. This is supported by Rule 6 s.1.1.1(e) of 2018 IRR that states AMLC can conduct on-site and off-site examinations or other forms of compliance checking on covered persons to ensure AML/CFT compliances. S.1e) in the DNFBPs AML/CFT guideline also reiterates that AMLC is responsible for ensuring AML/CFT compliance for the all DNFBPs.

450. Rule 2, Rule 7 s.2.2 (b)(c) in 2018 IRR and Rule 27 of IRR of the TFPISA provides BSP the power as the competent authority for monitoring and ensuring compliance with trust companies' AML/CFT requirements.

451. Real estate agents are not covered persons subject to AML/CFT compliance.

452. *Criterion 28.3* - Other DNFBPs are monitored by AMLC for compliance with AML/CFT requirements under Rule 7 of 2018 IRR and s.1(e) of AML/CFT guideline of the DNFBPs.

453. Trust companies are monitored by BSP for their compliance with AML/CFT obligations under Rule 7 s.2.2 (b-c) of 2018 IRR. Real estate agents are not covered persons and are not subject to monitoring.

454. *Criterion 28.4* - AMLC has the power to impose AML/CFT sanctions on covered persons, as set out in Section 14 of the AMLA. Rule 7 of 2018 IRR provides AMLC with the power to act as competent authority to carry out the AML/CFT supervision on any covered persons. In the casino sector, the gaming supervisors PAGCOR, CEZA and APECO have the power to supervise and monitor the compliance of casinos (CIRR Section 8a), while the compliance checking power is jointly held by both gaming supervisors and AMLC (CIRR Section 8f) and Section 36). The DNFBPs AML/CFT guideline empower AMLC to be the supervisory authority for checking compliance of the non-casino DNFBPs.

455. Real estate agents/brokers are not covered persons in AMLA and there is no competent authority or SRB with powers to monitor its compliance. The Professional Regulatory Commission (PRC), through the Board of Real Estate Service, has the authority to issue licenses to real estate brokers. S.18 of RA9646 provides the fit-and-proper requirement for real estate brokers during the registration. S.19 provides the power to the Board to suspend a registration due to unethical conduct.

456. Jewellery dealers in precious stones and metals are governed by the Jewellery Industry Development Act of 1988 and are required to register their business with SEC (as the company registry) and the DTI. Rule 4 s.3.4 of 2018 IRR provides AMLC with the powers to act as competent authority to carry out the AML/CFT supervision on the sector, including preventing criminals influence in market entry.

457. The Supreme Court has the constitutional power "to promulgate rules concerning pleading, practice and procedure in all courts, and the admission to the practice of law under Section 5(5), Article VIII of the 1987 Constitution. Lawyers in the Philippines are under the supervision and regulation of the Supreme Court and the Integrated Bar of the Philippines (IBP) formed under PD 181. Republic Act No. 6397 confirmed the power of the Supreme Court to adopt rules of court to effect the integration of the Philippine Bar. Rule 138 s.2 of Rules of Court provides the fit-and-proper requirements prior to admission. AMLC has the authority to monitor the AML/CFT compliance of lawyers under the definition of AMLA. There is no SRO required to be appointed to oversee AML/CFT compliance. These parties can act on any complaints against any lawyer for violations of the Code of Professional Responsibility and laws, including AMLA.

458. The Board of Accountancy (BOA), under the supervision of Professional Regulatory Commission (PRC), has the authority to regulate accounting profession pursuant to RA 9298 Philippines Accountancy Act. S.23 of RA9298 prohibits individual with conviction of criminal offense (of moral turpitude), guilty of immoral and dishonourable conduct to register as an accounting professional. Under Section 24, existing registration can be suspended for the same causes in Section 23 and other accounting standards such as Code of Ethics. Under the AMLA, AMLC has the authority to monitor the AML/CFT compliance of lawyers.

459. Entities engaged in trust business (trust entities) are required to be licensed under the BSP pursuant to Section 79 of RA 8791. Trust entities within banks are subject to same fit and proper legal provisions apply for banks. MORNBFI s.4103T requires fit and proper of incorporators, subscribers and the management of (stand-alone) trust entities, and the incorporators and subscribers of those entities must not have involved in crimes of moral turpitude. There are TCSPs other than those trust entities supervised by the BSP, or those other than lawyers or accountants that participate in the creation administration and management of trust and corporate vehicles. S.53 of 2018 DNFBP Guideline provides AMLC with the power to act as competent authority to carry out the AML/CFT supervision of those entities, and Rule 4 s.3.4 of 2018 IRR provides AMLC the power in preventing criminals influence in market entry.

460. *Criterion 28.5* - Rule 7 s.5.2 requires supervision to covered persons to be on risk-sensitive basis. The PAGCOR approved a designated AML/CFT division in January 2018 in responsible for on-site and off-site examination. A gaming sector risk assessment was conducted in 2018 by PAGCOR and as at the time of the on-site PAGCOR was drafting a risk-based AML/CFT on-site examination manual. There is no AML/CFT risk-based supervision for CEZA and APECO.

461. AMLC Compliance and Supervision Manual (November 2018) set out the risk-based supervision that is applicable to other DNFBPs-covered persons. Part II.A of the manual requires AMLC to prepare an annual assessment plan that accounts risk factors ranging from those identified in the NRA, sectoral risk assessment and institutional risks of the covered persons to identify the covered persons that should be subject to on-site examinations. Part II.C also set out the procedures for AMLC to prioritise individual covered persons for off-site surveillance based on various high-risk triggers of non-compliance.

462. BSP's risk-based supervision framework exercised for banks (see c.26.5 and c.26.6) also applies to trust companies. Real estate agents are not subject to AML/CFT supervision.

Weighting and Conclusion

463. There are moderate shortcomings in R.28. The suitability procedures of PAGCOR licensees only cover board of directors and not shareholders or beneficial owners. No information was provided on the fit and proper framework for land-based casinos under the supervision of CEZA and APECO. Real estate agents are not covered persons subject to any AML/CFT requirements. A risk-based AML/CFT supervision framework is yet to be established for casinos.

464. **Recommendation 28 is rated partially compliant.**

Recommendation 29 - Financial intelligence units

465. The Philippines was rated partially compliant with the former R.26 in its previous MER. The deficiencies noted were that there was no formal TF mandate, insufficient resources were dedicated to provide feedback and guidance to reporting entities, insufficient resources were dedicated to the analysis function, the structure of AMLC and approval processes as prescribed under the AMLA impeded the Secretariat's full operational autonomy, access to relevant databases (police and others) were not timely, there was insufficient funding for the FIUs operating budget, the AMLA requirements on AMLC staff background affected overall effectiveness and there was insufficient sharing of financial intelligence with law enforcement.

466. *Criterion 29.1* - AMLC is the designated FIU for the Philippines (s.7 of the AMLA) to require and receive covered or suspicious transactions from covered persons (function of FIAG). As a hybrid FIU, AMLC also investigates ML/TF (undertaken by the FCIG). There is no

clear and explicit mandate provided in law that sets out the FIUs responsibility for the analysis of STRs and other relevant information, or for the dissemination of the results of that analysis, other than an indirect provision under s.7 (10) of the AMLA¹⁰⁰. Rule 6B of the 2018 IRR provides for the role of AMLC to analyse STR/ CTR and to disseminate financial intelligence arising for the analysis. AMLC's Financial Intelligence Manual – SOP states that AMLC's mandate and statutory duties are to receive and analyse reportable financial transactions, and disseminate financial intelligence to law enforcement agencies, other relevant government bodies and international counterparts to assist in combating ML and FT. Noting the hybrid structure of the FIU, there is no requirement for FIAG to disseminate information to FCIG.

467. AMLC is composed of the Governor of BSP as Chairman, and the Commissioner of the IC and the Chairman of the SEC as members. The Council is supported by a Secretariat. Under Section 7 of R.A. 9160, as amended, AMLC shall act unanimously to discharge its functions including dispensing approval or decision for disclosure on PEPs and banking enquiry.

468. *Criterion 29.2* - (a) AMLC has the sole authority to require and receive STRs from covered persons (s.7(1) of the AMLA). Rule 22 of the 2018 IRR states that covered persons shall file all STRs in accordance with the ARRG. The ARRG requires covered persons to report STRs to AMLC. (b) In addition to STRs, AMLC receives other information as required by national legislation, which includes covered transaction reports, cross-border currency declarations and reports on certain real estate transactions. S.9(c) of the AMLA, as amended, provides the obligation for covered persons to report CTRs and STRs. S.3(a)(8) and s.3b of the AMLA provide the definition of covered transaction and threshold for covered persons, including casino, jewellery dealers to reporting covered transaction. Cross-border currency declarations are reported to AMLC pursuant to Customs Memorandum Order No 33-2009 and all real estate transactions above PHP500,000, (approx. USD9500) are reported to AMLC pursuant to s.7 (12) of the AMLA.

Criterion 29.3

469. *29.3 (a)* - Section 7(2) of the AMLA gives AMLC the power to issue orders to covered persons to determine the true identity of the owner of any monetary instrument¹⁰¹ or property subject to a CTR or STR or request for assistance from a foreign state, or believed by the Council, on the basis of substantial evidence, to be, in whole or in part, wherever located, representing, involving, or related to, directly or indirectly, in any manner or by any means, the proceeds of an unlawful activity. In addition, for further requests on banking or investment transactions in relation to covered and suspicious transaction reports from banking and NBFIs, s.7(1) provides a basis for AMLC to require covered institutions to submit new STRs containing further information (including CDD data), analysis and transaction records needed for the purpose of FIU analysis.

470. *29.3 (b)* - Section 7(10) of the AMLA, provides AMLC the authority to enlist the assistance of any government office or government-owned and controlled corporations, in undertaking any and all AML operations. This may include the use of its personnel, facilities and resources. AMLC has signed MoAs with other government agencies which enable it to access

¹⁰⁰ Financial Intelligence Manual (Resolution 29 (2018)), stipulates that sharing of financial intelligence falls under the role set out in section 7 (10) of the AMLA, which enable AMLC to enlist the assistance of other government agencies for prevention, detection and investigation of ML offences.

Financial Intelligence Manual (Resolution 29 (2018)), stipulates that sharing of financial intelligence falls under the role set out in section 7 (10) of the AMLA, which enable AMLC to enlist the assistance of other government agencies for prevention, detection and investigation of ML offences.

cates, custodial receipts or deposit substitute instruments, trading orders, transaction tickets and confirmations of sale or investments and money market instruments; and (4) other similar instruments where title thereto passes to another by endorsement, assignment or delivery.

TECHNICAL COMPLIANCE

the information or databases of 25 other agencies, including online access of the SEC and DTI databases, which support its analyses.

471. *Criterion 29.4* - The Philippines demonstrated that it undertakes both operational and strategic analyses through its FIAG, as follows:

- *Operational analysis* – analysis of financial intelligence is conducted using AMLC’s database of STRs and CTR, closed source of information (which include SEC, DTI, Interpol, WorldCheck), and open source information. The process involves the assessment of a STR for profiling, determine the unlawful activity or suspicious circumstances based on STR narrative.
- *Strategic analysis* – analyses are undertaken to identify ML/FT trends and typologies for the purpose of distributing risk information (including statistics, trends and typologies) to government, covered persons, the general public and domestic and international AML/CFT counterparts. Such analysis also feeds into the NRA process.

472. *Criterion 29.5* - There is an implied mandate provided under the AMLA for the dissemination, spontaneously or upon request, of information and results of analysis related to ML to competent authorities under the s.7(10) provision for AMLC to ‘enlist’ the assistance of other governance agencies to undertake ML operations. This role is not clearly specified in the 2018 IRR, other than requirement for AMLC to develop mechanism for information dissemination which include to LEAs and covered persons¹⁰². However, the Financial Intelligence Manual SOP provides for work process for dissemination/disclosure to LEAs (see c. 29.1). AMLA is silent on disseminations in relation to TF and predicate offences. S.VI of AMLC Resolution No. 40 Series of 2018 decides that AMLC will not disclose information related to a PEP during an election period, however this does not prohibit internal sharing from FIAG to FCIG. This does however prevent AMLC from responding upon request to other authorities during an election period. For disclosures to foreign FIUs, paragraph 8 of AMLC Resolution no. 116, series of 2017, provides for AMLC to act on request for financial intelligence by foreign states. Disclosure of financial intelligence is mostly undertaken in secured manner, except for some urgent circumstances.

473. *Criterion 29.6* - Rule 6, s.1.6.8(a) of the 2018 IRR provides for the requirements for AMLC and its Secretariat to securely protect information received or processed and prohibit any revelation of the information. The confidentiality requirement continues to apply even after staff separation from AMLC. The IRR also provides for AMLC to formulate rules governing information exchange and dissemination, the security and confidentiality of such information, including procedures for handling, storage, and protection of, and access to, such information. Resolution No. 40 Series of 2018 out of AMLC Guidelines on Information Sharing and details the role of the AMLC Secretariat in the sharing of information, its scope, intended recipients, and conditions of sharing. A secure internet-based sharing of information between AMLCS, law enforcement and other government agencies was also approved by AMLC Resolution No. 140, however was not in place as at the time of the onsite. b) Rule 5, s.3.3 of the 2018 IRR states that the AMLC Secretariat staff are regular employees of the BSP and shall be entitled to such benefits and subject to such rules and regulations as are applicable to BSP employees of similar rank. As such, background investigation on potential AMLC officers and staff are conducted by the BSP’s Security, Investigation, and Transport Department. (c) AMLC has issued various information technology policies on access to confidential information, namely, the Policy on the Use of Information and Communications Technology Resources, Policy on Information and Communications Technology Security Systems, Password Policy, Physical Access to Servers and Other ICT Systems Policy and Remote Access to Servers and Other ICT Systems Policy. The

¹⁰² Rule 6 – para 1.6.7 of 2018 IRR

relevant policies set out protection of entry controls which include automatic door-locking. The Information and Communications Technology (ICT) Manual, approved through AMLC Resolution No. 78, Series of 2018, includes the requirement to perform regular audit.

474. *Criterion 29.7* - Section 7 of the AMLA, provides for the creation of AMLC which comprised of the Governor of the BSP as Chairman, the Commissioner of the IC and the Chairman of the SEC, as members. AMLC is an autonomous government agency, separate from the BSP, SEC or IC. The work of AMLC is not subject to the review of/approval by other government officials and it has a separate budget (capital outlay and maintenance and other operating expenses) under the General Appropriations Act (c.29.7(c and d)). AMLC may request information from domestic agencies and foreign jurisdictions. However, as noted above, AMLC cannot share information related to PEPs outside AMLC during election periods¹⁰³. Taking into account the risks and context of the country, this presents an impediment to AMLC's operational independence and autonomy (c.29.7 (a) and (b)).

475. *Criterion 29.8* - AMLC has been a member of the Egmont Group since June 2005.

Weighting and Conclusion

476. Philippines has functioning FIU with necessary powers and roles, including receipt of reports and information necessary to discharge its functions. There are some deficiencies in meeting R.29, in relation to and prohibition of sharing information on PEPs outside AMLC during an election period, which affect the FIUs autonomy and independence.

477. **Recommendation 29 is rated partially compliant.**

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

478. In its 2009 MER, the Philippines was rated partially compliant for the former R.27. The main deficiencies noted were the absence of a clear mandate to LEAs to investigate ML offences and substantial legislative changes were needed to provide the required powers to LEAs. The creation of a ML Investigation Coordination Group in order to have a coordinated and effective mechanism for AML/CFT was also recommended.

479. *Criterion 30.1* - AMLC is mandated to investigate all ML/TF offences and other violations of the AMLA and TFPSA (Rule 8, s.1 of the 2018 IRR). While AMLC does not enjoy all powers of an LEA, AMLC can enlist the assistance of any branch, department, bureau, office, agency or instrumentality of the government in investigating of ML or TF offences (s.7 of the AMLA).

480. The PNP is empowered to enforce all laws and ordinances, investigate and prevent crimes, arrest criminals and search and seizure (s.24 of RA 6975) under its general police powers. NBI is mandated to investigate a range of serious offences, including ML, TF and predicate offences based on s.1 of the RA 157 and s.5 of the RA 10867. PNP and NBI can investigate ML or TF offences in coordination with AMLC.

481. The PDEA can undertake the enforcement actions for drug related crimes and investigate all violators and other matters involved in the commission of any crime relative to the use, abuse or trafficking of any dangerous drug and/or controlled precursor and essential chemicals(s.84 of RA 9165), which would include related ML. The Office of the Ombudsman (OMB) can investigate and prosecute any act or omission of any public officer or employee, office or agency, when such act or omission appears to be illegal, unjust, improper or inefficient (s.15 of

¹⁰³ AMLC Resolution No. 40 Series of 2018

TECHNICAL COMPLIANCE

RA 6770). The Bureau of Customs (BOC) is mandated to prevent and suppress smuggling in the country (s.202 of RA 10863). The Securities and Exchange Commission (SEC) can investigate violations under the Securities Regulation Act (s.53).The Bureau of Fisheries (BFAR) to enforce all laws, formulate and enforce all rules and regulations governing the conservation and management of fishery resources(s.65(n) of RA 8550). Intellectual Property Office of the Philippines (IPOPhil) is authorised to enforce IP offences under s.7 (c) of RA 8293.

482. *Criterion 30.2* - AMLC is the primary LEA to designated to investigate ML and TF (s.7 AMLA, rules 7 and 19 of the 2016 RIRR, S. 36 of the CIRR and S.10 of the RA 10168). There is no legislative barrier for PNP and NBI to conduct parallel ML/TF investigations when predicate crimes are being investigated.

483. The MOAs between AMLC and LEAs which provide a framework of mutual information exchange and assistance in the conduct of investigations of ML and TF and predicate offences. In terms of MOAs, LEAs are required to report promptly to the AMLC any instances of ML and TF offences and related unlawful activities which enables referrals and coordinated investigations; thus satisfying the criterion.

484. There is no limitation for investigation of ML offences irrespective of where the predicate offence occurred. There is no limitation in LEAs referring to AMLC the elements of ML.

485. *Criterion 30.3* - Section 7(2) and s.11 of the AMLA empowers AMLC to expeditiously identify and trace property related to ML, TF and unlawful activity. AMLC, by s.10 of AMLA, can initiate freezing through OSG by a verified *ex parte* petition before the Court of Appeal and freeze for 20 days any monetary instrument or property, which period can be further extended via a summary hearing before the Court of Appeal. AMLC is unable to seize property subject to confiscation or suspected being proceeds of crime. It can request for assistance of LEAs with powers of seizure.

486. A number of LEAs are empowered to expeditiously identify, trace, and initiate freezing and seizing of property that is, or may become, subject to confiscation. Examples are; s.84(d) of the RA 9165 empowers PDEA to arrest and apprehend, as well as search all violators and exercise seizure and confiscation, the effects or proceeds of the crimes as provided by law and take custody thereof. S.54(5) of the Human Security Act (RA 9372) allows ATC the power of freezing of funds, property, bank deposits, placements, trust accounts, assets and records belonging to a person suspected of or charged with the crime of terrorism or conspiracy to commit terrorism. OMB does not have power to freeze or seize assets.

487. *Criterion 30.4* - There are no competent authorities, which are not an LEA, with responsibility for pursuing financial investigation of predicate offences.

488. *Criterion 30.5* - The OMB is the Philippines anti-corruption authority; but it is not able to conduct ML/TF investigations related to graft and corruption offences.

Weighting and Conclusion

489. **Recommendation 30 is rated compliant.**

Recommendation 31 – Powers of law enforcement and investigative authorities

490. In its 2009 MER, the Philippines was rated partially compliant with the former R.28. The main deficiencies noted were that the bank inquiry orders under AMLA cannot be issued unless a notice is given to the owner(s) of the accounts allowing them to contest the issuance of the order except where the predicate offence is kidnapping for ransom, drug offences, hijacking, destructive

arson and murder. In addition, the LEAs other than AMLC could not compel production of documents from financial institutions.

Criterion 31.1

491. *31.1 (a)* – Rule 8 of the 2018 IRR requires FIs and DNFBPs to provide AMLC full access to all information, documents or objects related to ML/TF and other violations of the AMLA and TFPSA immediately on receipt of an AMLC order. Rule 11 of the 2018 IRR provides authority to AMLC to conduct inquiries from bank and NBFIs with a court order and without a court order on specific predicate offenses. S.10 of the RA 10168 provides authority to obtain bank account details without a court order. S.33 of the CIRR provides authority to examine customer accounts in relation to casino issues. S.10 of the RA 10168 enables AMLC to access all necessary documents in respect of TF investigations.

492. Section 15(8) of the RA 6770 provides OMB to administer oaths, issue subpoena take testimony in any investigation or inquiry, including power to examine and have access to bank accounts and records. However, their scope of empowerment has been restricted by judicial pronouncement in *Marquez V. Desirto* whereby access to bank records are permitted only after the filing the relevant case and not during the investigation process. The SEC has powers to issue subpoena, summon witnesses to appear in any proceedings of the Commission and in appropriate cases, order the examination, search and seizure of all documents, papers, files and records, tax returns and books of accounts of any entity or person under investigation (s.5 (l) read together with s.53 of the RA 8799).

493. With the exception of AMLC, no other LEAs have powers to satisfy the requirement of criterion referred above and request the production of records held by financial institutions, DNFBPs and other natural or legal persons. However, AMLC, in terms of the MOAs with LEAs, can share such information obtained by it with OMB and other LEAs and these LEAs can use such information for their ongoing investigations and as evidence with concurrence of AMLC.

494. *31.1 (b)(c) & (d)* - the AMLA does not contain any provision in relation to the search of a person and premises and seizing and obtaining evidence. Rule 6, s.1.9.4 (a) of the 2018 IRR stipulates responsible officers and employees of covered persons and pertinent government agencies to give statements pertinent to the transactions, person or violation being investigated. This is limited to covered persons and government agencies. The Philippines indicates that in terms of s.7(10) of AMLA and s.10 of RA 10168 AMLC can enlist assistance of any state agencies including their personnel, facilities and resources in the detection and investigation of ML and TF offences in respect of criterion above.

495. LEAs responsible for associated predicate offences have wide range powers to search of persons and premises, taking witness statements and seizing and obtaining evidence. S.24 of the RA 6975 provides the PNP with general powers to make arrests, search and seizure, administer oaths and issue subpoena. S.4 of RA 10867, authorizes the NBI to issue subpoena for appearance of any person for investigation or production of documents; s.9 provides authority to conduct searches, arrests, seizure and take and require sworn statements of any persons summoned in relation to cases under investigation.

496. Section 84 of RA 9165 authorizes the PDEA to administer oaths, issue subpoena, arrest and apprehend, search, seizure and confiscate the effects or proceeds of crimes. S.15 of the RA 6770 provides OMB to administer oaths, issue subpoena, and take testimony, including a limited power to examine bank accounts and records where court proceedings are already underway.

497. Section 214 of the RA 10863 provides Bureau of Customs (BOC) to search, seizure and arrest for the implementation of the Act. S.5 of RA 8799 in relation to Rule 5 of the 2015 SRC IRR,

TECHNICAL COMPLIANCE

authorizes the SEC to issue subpoena and summon witnesses, order the examination, search and seizure of all documents, papers, files and records, tax returns, and books of accounts of any entity or person under investigation. The IPOPhil can undertake enforcement functions supported by concerned agencies (s.7 (c) of RA 8293, as amended). The BFAR is mandated to enforce all laws governing the conservation and management of fishery resources (s.65 (n) of RA 8550, as amended).

Criterion 31.2

498. 31.2 (a) - There is no legal provisions for the Philippines LEAs including AMLC to conduct undercover operations. However, PNP and NBI in their operational manuals have guidelines to conduct such operations.

499. 31.2 (b)&(c) - The LEAs ability to use investigative techniques such as intercepting communications and accessing computer systems is limited for specific offences (s.3 of the RA 4200) which does not include investigations of ML and TF offences.

500. 31.2 (d) - There are no legal provisions for the Philippines LEAs, including AMLC, to use controlled delivery as investigative techniques.

Criterion 31.3

501. 31.3 (a) - The AMLA (s.11) empowers AMLC to inquire into or examine any particular deposit or investment, including any related accounts held with any bank or NBF, upon order of any competent court based on *ex parte* application. In the meantime, no court order is required in cases involving kidnapping for ransom, violations of certain drug offences and hijacking. Further, Section 10 of the RA 10168 provides the AMLC to inquire into or examine deposits and investments with any bank or NBF and their subsidiaries and affiliates without a court order in respect of TF offences.

502. The AMLA (s.7(2)) authorises AMLC to issue orders to the appropriate supervising authority or covered institution to determine the true identity of the owner of any monetary instrument or property subject of a covered transaction or suspicious transaction report or request for international assistance from a foreign state to locate the proceeds of an unlawful activity. According to the Rule 2, s.1 (w) of the 2018 IRR "Covered transaction" refers a transaction in cash or other equivalent monetary instrument exceeding five hundred thousand pesos (US\$ 9350)and one million pesos (US\$ 18710) in case of jewellery dealers; dealers in precious metals and dealers in precious stones. S.9 of the AMLA requires covered persons to establish the true identity of their clients and, in case of corporate clients, require a system of verifying their legal existence and organizational structure, as well as the authority and identification of all persons purporting to act on their behalf. The Philippines clarified that using s.7(2) of AMLA, customer on boarding information and other information not covered by banking secrecy provisions of the RA 1405 can be accessed by AMLC.

503. OMB has limited authority including to examine and have access to bank accounts and records to cases with court proceedings underway (s.15(8) of the RA 6770).

504. The SEC has powers to issue subpoena, summon witnesses to appear in any proceedings of the Commission and in appropriate cases, order the examination, search and seizure of all documents, papers, files and records, tax returns and books of accounts of any entity or person under investigation(s.5 (l) of the RA 8799).

505. While other LEAs do not have powers to directly identify, whether natural or legal persons hold or control accounts, they are able to channel these inquiries through AMLC.

506. 31.3 (b) - AMLC has powers to examine assets without notification to the owner in respect of ML and TF offences (IRR Rule 6 (1.9)). With the exception of bank records, other LEAs can engage in the identification of assets without prior notification to the owner and can channel requests through AMLC when bank records are involved.

507. *Criterion 31.4* - AMLC is the FIU of the Philippines and a designated ML/TF investigation agency; therefore, they have direct access to relevant financial information held with the FIU. Other LEAs investigating ML, TF or predicates are able to request information held by the FIU under existing MOAs allowing exchange of information related to such investigations. These MOA are in place with twenty-eight (28) agencies including LEAs designated for predicate offenses. The Resolution No 40 of series 2018, s.IV allows AMLC to share information with domestic LEAs, supervising authorities, and competent authorities as well as foreign jurisdictions, with which AMLC has MOAs and MOUs.

Weighting and Conclusion

508. AMLC cannot directly seize assets or evidence or take witness statements, but these can be obtained with the cooperation of other LEAs. MOA and coordination structures are in place to facilitate these indirect arrangements for the exercise of compulsory measures. LEAs in the Philippines are not specifically empowered to engage in certain special investigative techniques.

509. **Recommendation 31 is rated largely compliant.**

Recommendation 32 – Cash Couriers

510. In its 2009 MER, the Philippines was rated largely compliant on Special Recommendation IX. The deficiencies noted were as follows; the postal stream and cargo streams were not covered by the declaration systems, there was very weak implementation of the cross border reporting requirement (due to a lack of clear policy to cover all entry points, and weak capacity to target and discover cash couriers), there was insufficient customs examiners at arrival and departure areas of international airports and seaports (except Manila) to enable the effective implementation of the Philippines' law relating to import and export of cash and BNI, no statistics were available relating to the cross border declaration of cash and BNI from international airports (except Manila) or seaports, and no information was available demonstrating safeguards to ensure the proper use of information and data provided pursuant to the currency declaration system.

511. *Criterion 32.1* - A declaration is required at the point of any import or export of any foreign currency or foreign currency-denominated BNI in excess of USD 10,000 or equivalent (s.4.2 of BSP Circular No.794 series of 2013 (amendment to foreign exchange regulations)). The declaration must include information on the source and the purpose of the transport of such currency and monetary instruments.

512. BSP Circular No. 922 series of 2016 (Amendment of the Rules on Cross-Border Transfer of Local Currency) sets up requirement for prior authorisation from the BSP for import or export of legal tender drawn in pesos for amounts above PHP50,000 (approx. USD 952). This is a defacto declaration obligation.

513. As required by the criterion, the generic application to all cross border transfers include transfers via travellers or through mail and cargo using different modes of transportation, and are covered by the words "import and export".

514. *Criterion 32.2* - The Philippine has a written declaration system for any person carrying currency or BNIs above the threshold of USD 10,000.

TECHNICAL COMPLIANCE

515. *Criterion 32.3* - The Philippine has a written declaration system.
516. *Criterion 32.4* - There is no designated competent authority that has the authority, in cases where there is a false declaration or a failure to declare, to request and obtain further information from the carrier with regard to the origin of the currency or BNIs, and their intended use.
517. *Criterion 32.5* - Section 36 of the RA 7653 provides that any violations of the Act or any order, instruction, rule or regulation issued by the BSP Monetary Board, such person or persons responsible for such violation shall unless otherwise provided in the Act, be punished by a fine of not less than PHP 50,000 [USD 952] nor more than PHP 200,000 [USD 3810] or by imprisonment of not less than two years nor more than 10 years, or both, at the discretion of the court. In terms of s.2530 of RA 1937, any vessel or aircraft, cargo, articles and other objects shall, under the listed conditions, be subject to forfeiture. These sanctions encompass false declarations as well. The penalties for the offence by way of imprisonment are dissuasive, however the imposed fixed amount fines are not proportionate and nor dissuasive.
518. *Criterion 32.6* - The MOA between BOC and AMLC provides for information exchange. According to the Customs Memorandum Order 33-2009 all foreign currency declarations of incoming and outgoing passengers must be submitted to AMLC.
519. *Criterion 32.7* - NALECC is the forum for coordination between LEAs including on matters related to customs and movement of currency. S.6 of Executive Order No. 41 stipulates that law enforcement coordinating committees at all level shall meet at least once a month to discuss, monitor and assess the law enforcement programs of the government. This coordination mechanism includes discussion of cross border currency transactions.
520. *Criterion 32.8* - The Supplemental Memorandum of Agreement for the Effective Implementation of BSP Rules on Physical Cross-Border Transport of Currencies provides that legal tender above the threshold can be restrained for initial investigation in instances of undeclared/under declared/ unauthorised currency are discovered, and will be handed over to BOC. There is no specific reference to restraint of currency or BNI where ML/TF or predicate offences are suspected. This gap was identified as a priority action in the NACS.
521. *Criterion 32.9* - BOC and AMLC retain copies of the written currency declaration. AMLC is required to retain all declarations for five years. S.13 (a) of the AMLA allows upon a request by foreign states for investigation or prosecution of an ML offence for AMLC to execute or refuse.
522. *Criterion 32.10* - There are legal protections to ensure proper use of information by officials under s.54 of the Data Privacy Act of 2012 with dissuasive sanctions for violations. Furthermore, s.9 of the AMLA provides for officers and employees of AMLC criminally liable for performance of any act contrary to their duty to act in good faith.
523. *Criterion 32.11* - Persons transporting funds or BNIs in relation to ML or TF may be subject to penalties for these offences as set out in R.3 and R.5. The sanctions for these offences are in addition to the possible penalties for providing a false declaration. The currency or BNIs would be subject to civil and criminal forfeiture as set out in R.4.

Weighting and Conclusion

524. The Philippines has a written declaration system for cross-border transportation of currency and BNIs. The cross-border transfers made via mail and cargo are covered by the words “import and export” in the BSP circular. No competent authority has the authority to request and obtain further information from the carrier in cases where there is a false declaration or a failure

to declare. The penalties for the offence by way of imprisonment are dissuasive however the fines are not proportionate and nor dissuasive. Competent authorities are not clearly empowered to restrain currency and BNI suspected of ML/TF or other predicate offences.

525. **Recommendation 32 is rated partially compliant.**

Recommendation 33 – Statistics

526. The Philippines was rated largely compliant with former Recommendation 32, which required maintenance of comprehensive statistics. The 2009 mutual evaluation concluded that that the Philippines had no practice of using statistics to undertake a review of the effectiveness of the regime as a whole and the statistics for customs were incomplete.

Criterion 33.1

527. Despite a clear legislative basis for relevant agencies to maintain comprehensive statistics on matters relevant to this criterion, there are some gaps in the application of this requirement in practice. Rule 32, Section 6 of the 2018 IRR requires competent authorities to maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML/CFT systems including (a) CTR, STR and other reports, received, analysed and shared; (b) ML/TF and associated unlawful activity investigations, prosecutions and convictions; (c) Monetary instruments and properties frozen and forfeited; and (d) Mutual legal assistance and other international requests for cooperation received and made.

528. *33.1 (a) - STRs:* AMLC maintains comprehensive statistics on STRs received, covered transaction reports, analysed reports and disseminated intelligences. The STRs are categorised as per the predicate offences and as per the general types of REs such as banking, insurance, securities, DNFBPs, STRs related with natural or legal persons, domestic and foreign persons, feed-backs on disseminated intelligences, etc.

529. *33.1 (b) - ML/TF investigations, prosecutions and convictions:* AMLC maintains statistics on ML/TF investigations, prosecutions and convictions. There is some scope for improvement with respect to the categorisation of an ‘investigation’ conducted by AMLC.

530. *33.1 (c) - Confiscations:* The Philippines has a regular mechanism to maintain statistics on frozen assets, petitions for civil forfeiture but not on seizure, actual confiscation and recovery. The statistics provided do not make it clear whether it was the proceeds of crimes and instrumentalities that were identified, seized, frozen, or confiscated, and whether such action or recovery was made in relation to predicate offence or ML offence. Statistics are not sufficiently detailed to aggregate them and are sometimes duplicated by different agencies with overlapping mandates.

531. *33.1 (d) - MLA/other international cooperation:* Statistics for MLA are well-managed between DOJ and AMLC. Reliable statistics in relation to other international cooperation are available in some instances, for example through the Egmont Secure Web, but are less formally maintained for other instances of international cooperation.

Weighting and Conclusion

532. There are minor shortcomings, particularly systems for maintaining statistics relating to confiscation and international cooperation requests outside MLA.

533. **Recommendation 33 is rated largely compliant.**

Recommendation 34 – Guidance and feedback

534. The Philippines was rated partially compliant with R.25 in its 2009 mutual evaluation. Feedback did not include statistics on the number of disclosures, with appropriate breakdowns, and on the results of the disclosures and no guidelines had been issued for DNFBPs as none of them were subject to AML/CFT requirements.

535. *Criterion 34.1* - The Philippines has a clear legislative basis to issue guidelines and provide feedback to assist covered persons in implementing the AMLA and TFPSA, their respective IRR and other AMLC issuances. Rule 32, Section 2.2 of the 2018 IRR requires AMLC and supervisory authorities to provide guidelines and feedback as set out in R.34.

536. The BSP MORB/MORNBFI, SEC Guidelines and IC Guidelines assist FIs to implement their obligations, while the AMLC DNFBP Guidelines assist DNFBPs to implement their obligations

537. The ARRG provides guidance on the online registration system, transaction security protocols, and reporting procedures. It further provides limited examples of alerts and red flag indicators, and typologies, which can help reporting entities in the submission of reports. TF is briefly included in the ARRG. Other guidance is limited with respect to TF.

538. In practice, limited feedback has been given to FIs and DNFBPs. However, AMLC produced STR reporting guidelines in response to a STR quality review and conducted engagement with compliance officers to improve STR reporting. .

539. More broadly, the AMLC Secretariat also provides email and phone support to assist FIs and DNFBPs in completing CTRs and STRs. AMLC and financial sector regulators have conducted numbers of awareness programs and trainings to covered persons, provided feedbacks on their activities in general.

Weighting and Conclusion

540. Philippines has a strong legal mandate to provide guidance and feedback and has issued guidance material, however the provision of feedback to FIs and DNFBPs has been limited.

541. **Recommendation 34 is largely compliant.**

Recommendation 35 – Sanctions

542. In its 2009 MER, the Philippines was rated partial compliant with former R.17. The civil monetary sanctions were insufficient and rarely imposed.

543. *Criterion 35.1* - There is a broad range of mostly proportionate and dissuasive sanctions (criminal, civil and administrative) available against both natural persons and legal persons that fail to comply with AML/CFT requirements.

544. If failures to apply AML/CFT measures are wilful and directly associated with ML/TF, there are criminal offences under the AMLA. S.4(e) is the offence of aiding, abetting or assisting the commission of ML/TF offences, whereas s.4(f) is the offence of performing or failing to perform any act as a result of which ML/TF is facilitated. The penalty is imprisonment from between four and seven years or a fine of between P1.5 million (approx. USD28,000) and P3 million (approx. USD56,000).

545. Specific to TF, s.8 of the TF Law prohibits any person from making available any property or funds, or financial or other related service to a designated person or entity. S.16 of the TF Law requires covered persons or relevant government agencies to freeze without delay, the funds or other assets of designated persons and entities upon receipt of a freeze order. The penalty for failing to follow these orders is a fine from P500,000 (approx. USD9,300) to P1 million (approx. USD18,600).

546. AMLA includes a criminal penalty for any FIs/DNFBPs who, knowing that a covered or suspicious transaction is required under the act to be filed with AMLC, fails to do so. Such covered persons are liable for imprisonment from six months to four years or a fine of not less than 100,000 Php (approx. USD 1,900) but not more than 500,000 Php (approx. USD 9,500) or both (s.14(a)(3)). The fines available are not dissuasive.

547. There are further criminal offences in sections 9 and 14 of the AMLA that relate to AML/CFT failures (regardless of whether ML/TF occurs). This includes failing to report covered or suspicious transactions (R. 20), failing to keep records (R.11), malicious reporting and breach of confidentiality (R.21). Depending on the offence, the penalties range from imprisonment for periods from six months to 8 years and fines from P100,000 (approx. USD1,860) to P1 million [USD18,600]. There is no specific offence for failing to conduct CDD (R.10), although if CDD failures were directly associated with ML, the offences above under s.4(e) and (f) of the AMLA could apply.

548. In addition to the criminal offence provisions, s.7(11) of the AMLA and Rule 26 of the IRR enables AMLC to impose administrative sanctions for the violations of laws, rules, regulations, orders and resolutions. This is without prejudice to the filing of criminal charges against the persons responsible for the violation. Rule 26 of the IRR applies to all FIs and DNFBPs (other than casinos - see below) that are covered persons. Rule 26(6) of the IRR enables BSP, SEC or IC to also impose enforcement actions on their supervised entities for violations of their respective circulars and orders. Alternatively, Rules 7(2) and 26(6) of the IRR enables BSP, SEC or IC to escalate any adverse AML/CFT findings to AMLC for possible administrative sanctions. Administrative fines can be issued up to P500,000 (approx. USD9,300), but this is per violation, which is not dissuasive for individual failings.

549. AMLC's Rules on Imposition of Administrative Sanctions (RIAS) provide administrative sanctions that may be imposed for violation of the AMLA, its IRR or other orders or issuances. There is a matrix of violations with corresponding penalties, which are dependent on the asset size of the covered person and severity of the violation. Violations are classified from light to grave and may be imposed per violation, transaction or customer. Penalties range from P5,000 (approx. USD93) for a light violation by a micro entity to P500,000 (approx. USD9,300) for a grave violation by a large entity. For light or first time failures, violations may be dealt with by written warning or reprimand. These sanctions apply across all the AML/CFT requirements of R.10 to R.23. For R.6, there are administrative sanctions available under Rule 26 of the IRR of the TF Law for persons who violate the TF Law. Penalties range from a reprimand up to P500,000 (approx. USD9,300) per violation. Overall the maximum available monetary penalty are not proportionate or dissuasive for an individual failing, but could be multiplied with repeated violations. Unlike the SEC's powers, there is not a multiplier of fines per day for persistent violations.

550. For BSP, s.X811/4811Q of the MORB/MORNBFI state that administrative sanctions are based on an overall assessment of a FI's AML risk management system. Depending on the severity of the non-compliance, these range from written reprimands, restrictions on licenses and products that can be provided and corrective plans. Monetary penalties exist for serious non-compliance or if corrective plans are not complied with. These sanctions apply across R.6 and R.10- 21, and relevant elements of R.8. The sanctions also apply if a bank engages with or fails to conduct CDD on an unregistered NPO.

551. For SEC, s.12 of the 2018 AML Guidelines contains provisions for sanctions and penalties. These include revocation or suspension of registration, cease and desist orders pursuant to s.64 of the SRC or administrative sanctions pursuant to s.53.4 of not less than PHP 10,000 (approx. USD 190) and not more than PHP 1,000,000 (approx. USD 19,000) per violation. These sanctions apply to R.6, R.10, R.12, R.15, R.17 and R.21. For R.8, as per criterion 8.4b above, non-compliance with SEC Rules by a NPO may result in a fine of no less than PHP 10,000 (approx. USD 190) and not more than PHP1,000,000 (approx. USD 19,000), which can be extended by PHP2,000 (approx. USD 38) per day of violation, or disqualification from registration.

552. For IC, s.62 and 63 of CL. No. 2018-48 contains provisions for sanctions for non-compliance with AML/CFT requirements. This includes written reprimands, suspension, removal or disqualification from office (for officers of covered persons) and monetary penalties. Penalties range from PHP 5,000 (approx. 95) for a light violation to PHP200,000 (approx. USD 3800) for a grave violation. Fines may be imposed per violation, transaction or customer, but the aggregated fine must not exceed 1% of the total asset base. These sanctions apply across R.6, R.10, R.12, R.15, R.17 and R.21.

553. For casinos, s.37 of the CIRR states that non-compliance with the provisions of the CIRR shall be subject to such penalties and sanctions as may be imposed under the AMLA and PAGCOR, CEZA and APECO's respective charters or AML/CFT guidelines (issued pursuant to s9 of the CIRR). For AMLC, s.37 of the CIRR states that the RIAS shall apply to covered persons that are casinos. This applies to R.10, R.12, R.15, R.17 and R.23. For R.6, there are also administrative sanctions available under Rule 26 of the IRR of the TF Law for persons who violate the TF Law.

554. *Criterion 35.2* - Section 14 of the AMLA (sanction for ML) and Section 16 of TFP/RA 10168 (sanctions for failure to freeze) defines that where the offense is committed by any corporations or any legal persons, the criminal penalty will apply to the "responsible officers" who participated in or allowed by their gross negligence for the commission of the ML crime, or who fail to comply with a freeze order. Guidelines of the FIs require the appointment of compliance officers to be responsible for AML/CFT program for financial institutions (see Criterion 18.1), the BSP, SEC, and IC define the compliance officers shall be reporting to the board of directors who will ultimately be responsible for the AML/CFT implementation. S.10 of the CIRR for casinos and Section 7 of the AML/CFT guideline of the DNFBPs stipulate that the board of directors/partners/sole proprietors have the ultimate responsibility of the AML/CFT compliance.

555. AMLA empowers AMLC to impose administrative sanctions on covered persons, their directors, officers or employees for the violation of the AML requirements under the legal framework, without prejudice to administrative sanctions to the filing of any criminal charges against the persons (s. 14 (f)). The AMLC Rules on Imposition of Administrative Sanctions do not align with the AMLA with respect to sanctions for non-compliance by directors or management of covered persons that are legal persons, however the AMLA prevails. AML/CFT administrative sanctions applicable for BSP-regulated covered persons (per MORB Section X811) and IC-covered persons (s.62 of IC Circular 2018-48) include removal from the office and disqualification from holding any position in any covered institutions. S.12.2 of the SEC Revised AML/CFT Guidelines 2018 contain provisions for criminal charges against persons responsible that includes board of directors, who can be subject a fine of no less than PHP 5 million (approx. USD 95,250) or imprisonment of 7 to 21 years upon conviction. The provision is only for covered persons subject to the SRC. Directors and senior management of investment houses, investment companies financing and lending companies that are governed by other acts are not included. It is not explicit that administrative sanctions are applicable and can be imposed by supervisory authorities over directors or management for DNFBPs that are legal persons pursuant to CIRR (s.37), the gaming regime of casinos nor AML/CFT guideline of the DNFBPs (s. 57).

Weighting and Conclusion

556. There are minor deficiencies in meeting R.35, including administrative fines that are not dissuasive for individual failings, gaps with the administrative liability of directors and management of DNFBPs and SEC regulated institutions that are legal persons.

557. **Recommendation 35 is rated largely compliant.**

Recommendation 36 – International instruments

558. In its 2009 MER Philippines was rated partly compliant with former Recommendation 35 and non-compliant with former Special Recommendation I. The main deficiencies noted were the inadequate definition of ML, missing predicate offences and lack of criminalisation of TF. In the Philippines' 2012 APG follow-up report, Special Recommendation I was found to be at a level equivalent to largely compliant, following the enactment of R.A. 10168.

559. *Criterion 36.1* - Philippines has ratified all of the relevant treaties. The Senate of the Republic of the Philippines ratified the Vienna Convention on 26 February 1996; the Palermo Convention on 24 October 2001; the Merida Convention on 08 November 2006; and the Terrorist Financing Convention on 14 October 2003.

560. *Criterion 36.2* - A treaty, once signed, is forwarded to the Philippine Senate for a vote by at least two-thirds of its members, for concurrence. In accordance with Section 21 Art 7 of the 1987 Philippines Constitution once concurrence is received from the Senate the contents of the treaty automatically become an enforceable part of Philippines law. All treaties relevant to R.36 have received a concurrence vote.

561. In February 2013 legislation was passed to redefined ML according to be in keeping with the Vienna and Palermo Conventions, with the exception of minor technical deficiencies including tax offences not being captured as a predicate for ML.

562. In June 2012 legislation was passed which criminalises TF mostly in keeping with UN TF Convention.

563. Philippines implemented many aspects of the relevant articles¹⁰⁴ of the Vienna Convention, the Palermo Convention, the Merida Convention and the TF Convention. However some gaps remain with STR reporting and regulation and supervision of DNFBPs.

Weighting and Conclusion

564. Philippines has ratified all the relevant conventions and implemented most of their obligations. Minor deficiencies remain, including the lack of coverage of tax offences as a predicate for ML.

565. **Recommendation 36 is rated largely compliant.**

Recommendation 37 - Mutual legal assistance

566. In its 2009 MER Philippines was rated largely compliant with former Recommendation 36 and partly compliant with former Special Recommendation V. The main deficiency noted was the absence of TF criminalisation as a possible impediment to MLA. With the enactment of R.A.

¹⁰⁴ With the exception of Articles 8 and 17 Vienna Convention; Articles 15, 20, 26, 27, 28 29, 30, 31, Palermo Convention; and Article 16, Merida Convention.

TECHNICAL COMPLIANCE

10168, the rating of Special Recommendation V was amended to a level equivalent to largely compliant in 2012.

567. *Criterion 37.1* - Section 2 of Article II of the Constitution provides that the Philippines adopts the generally accepted principles of international law as part of the law of the land and adheres to the policy of peace, equality, justice, freedom, cooperation, and amity with all nations. Likewise, the Philippines has signed and ratified MLATs with Australia, China, Hong Kong, China, Korea, Russia, Spain, Switzerland, United Kingdom, United States and ASEAN (incorporating Brunei Darussalam, Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, Singapore, Thailand and Vietnam). These MLATs as well as bilateral tax treaties and the relevant multilateral treaties that the Philippines has joined provide the legal basis for the 'prompt' provision of widest possible assistance in relation to investigations, prosecutions and related proceedings.

568. For countries that have no existing MLA treaty with the Philippines or who have not joined the Palermo, Merida or TF conventions, cooperation can be extended on the basis of mutuality and reciprocity (s.13 of the AMLA). For MLA requests relating specifically to ML offences, the MOA between the DOJ and AMLC requires DOJ to endorse the request to AMLC to action appropriately. The IRR provides a legal basis for the AMLC to give timely prioritisation and execution of MLA (Rule 29 s.7).

569. *Criterion 37.2* - In the MLATs entered into by the Philippines, the DOJ, the Secretary of Justice or his duly authorised representative, is designated as the central authority on all MLA matters.

570. In line with Philippines' tax treaties, BIR is the central authority for MLA request and other request for information from other countries with regard to tax offences or other matters relating to taxation.

571. Outside of MLATs, the MOA between the DOJ and AMLC permits AMLC to request assistance and provide assistance directly to the appropriate authority of the foreign state. This is supported by the IRR which provides that MLA requests from foreign States will be filed with the DOJ, as the central authority on all MLA matters, and that the AMLC may directly receive and act on MLA requests made on the basis of reciprocity provided that all actions taken on such requests shall be transmitted to the DOJ for formal response to the requesting state (IRR Section 4 of Rule 29).

572. AMLC is required to formulate processes for the timely prioritisation and execution of MLA requests as explicitly provided under Rule 29 Section 7 of IRR 2018. Philippines asserted that requests requiring urgent action or requests involving certain types of offences (e.g. terrorism, drug-related offences or corruption) where given priority. The formulation of clear processes for the timely prioritisation and execution of MLA requests is not established.

573. Under the 2018 IRR (Rule 30, s.7), AMLC is required to maintain a case management system to monitor progress of MLA requests. AMLC utilises a document management system as well as a manual system for this purpose. In addition, DOJ maintains a manual case management system which stores the date of receipt of MLA requests, the requesting State, name/nationality of the subject of the matter, assistance sought, name of case officer appointed, competent authority for the request, date of referral to the competent authority and status of the request. In relation to requests directly received by AMLC, a record is not created in the DOJ case management system. Rather it is recorded by AMLC into AMLC's system.

574. *Criterion 37.3* - MLA is not prohibited nor subjected to unreasonable or unduly restrictive conditions in the Philippines. Under the MLATs, the Philippines may refuse to provide assistance if it were to impair the Philippines sovereignty or security, where the offence is

political or military in nature and not under criminal law, or if it is in contravention of human rights. MLA may also be refused if the request relates to an offence for which the sentence has been served or an acquittal has been granted. Under s.13(d) of the AMLA, AMLC can assist with MLA requests on the condition that the request is not prejudicial to the interest of the Philippines. Further, under s.2 of the AMLA, the extension of cooperation in transnational investigations and prosecutions of ML offenses should be consistent with the Philippine foreign policy.

Criterion 37.4

575. *37.4(a)* - Article 3(1)(a) of the Switzerland MLAT indicated that MLA may be refused if in connection with a fiscal offence. The other MLATs, multilateral conventions and tax treaties that the Philippines has joined do not restrict MLA on the grounds that the criminal offence also involves fiscal matters.

576. *37.4(b)* - The MLATs, multilateral conventions and tax treaties that which the Philippines has entered into do not permit the refusal to provide assistance on the basis of bank secrecy.

577. *Criterion 37.5* - The MLATs, multilateral conventions and tax treaties that entered into by the Philippines include provisions on the protection of confidentiality of the requests (for example, art.9 of the ASEAN MLAT and art.7 of the US MLAT), including the information contained therein. Disclosure is limited to the use of the information contained therein for purposes of supporting the allegations made by the government agencies in order to achieve the assistance requested.

578. *Criterion 37.6* - Dual criminality is not a strict requirement for the provision of MLA under Philippines' law. Further, its inclusion in the Philippines' MLATs is discretionary, i.e. a state *may* provide assistance in the absence of dual criminality if permitted by its domestic laws. However, some MLATs (Spain, United Kingdom and United States) require dual criminality in the context of coercive actions such as search, seizure, restraint or confiscation requests.

579. *Criterion 37.7* - For the MLATs, multilateral conventions and tax treaties that require dual criminality, reference is made to the act or omission, or underlying conduct, that has occurred constituting an offence in both jurisdictions (see art.3 (1)(e) of the ASEAN MLAT and art.1 (3) of the UK MLAT). The AMLA, as amended, lists as one of the unlawful activities/predicate offenses those "felonies or offenses of a similar nature that are punishable under the penal laws of other countries" (s.3(i) (34), AMLA). As long as the offence is of the same nature as those of the predicate offense then the requirement is satisfied. Predicate offenses are material in the pursuit of applications for bank inquiry, petitions for freeze order, petitions for civil forfeiture, and complaints for money laundering.

580. *Criterion 37.8* - The MLATs to which the Philippines is a party and the IRR provide specific reference to the types of assistance that may be afforded, such as the production of records, searches of premises, and the seizing and obtaining of evidence. Not all MLATs provide specific reference to searches of persons nor the taking of witness statements, which may be captured by the commonly referenced "other assistance" included in these MLATs (see art.1(2)(k) of the Hong Kong, China MLAT). In extending MLA, AMLC can use all powers and legal remedies under the AMLA, IRR and TFPSA, including authority to investigate and determine the true identity of persons, enlisting the assistance of other government agencies, freeze order, bank inquiry and civil forfeiture. AMLC is empowered to seek assistance from any other domestic authority, so can (see c31.1.), which can overcome the limits and allow for broad assistance to be rendered to foreign counterparts. However, the powers of AMLC are supplemented by the powers exercised by other LEAs such NBI and PNP in relation to the response prepared by the DOJ.

Weighting and Conclusion

TECHNICAL COMPLIANCE

581. There are minor shortcomings in relation to clear processes for the timely prioritisation and execution of MLA requests.

582. **Recommendation 37 is rated largely compliant.**

Recommendation 38 – Mutual legal assistance: freezing and confiscation

583. In its 2009 MER Philippines was rated largely compliant with former Recommendation 38. The two main deficiencies were that there were no arrangements for coordinating seizure and confiscation and no consideration of asset forfeiture fund.

584. *Criterion 38.1* - The Philippines has provisions in its model MLAT and IRR to take prompt action in response to requests from foreign countries covered by a MLAT to identify, freeze, seize or confiscate property, proceeds and instrumentalities (e.g. art.1(2)(i) of the China MLAT). The petition for civil forfeiture includes other monetary instrument or property of equal value in cases where the monetary instrument or property that should be subject of forfeiture (s.1, IRR of AMLA). The Hong Kong, China (art.18(5)(c)) and Korea (art.17(4)) MLATs which define property to also include “property which represents the value of benefits derived from the commission of an offence”. Some MLATs reference assistance to be provided in seizing property in relation to restitution (e.g. art.1(2)(g) of the US MLAT) or to satisfy the imposition of a pecuniary penalty (art.1(2)(f) of the Australia MLAT).

585. For countries that have no existing MLA treaty with the Philippines, cooperation with respect to freezing and confiscation may be extended as per the analysis in criterion 37.1. However, there is no specific process guaranteeing expeditious action for MLA requests for freezing and confiscation for jurisdictions without MLATs.

586. AMLC has the authority to freeze assets related to ML (s.10, AMLA) and TF (s.11, RA 10168) and forfeit proceeds of crimes (s.12, AMLA) and TF (s.18, RA 10168). The provisions on AMLC investigation, and freeze order, bank inquiry and civil forfeiture, shall apply to MLA requests when necessary to affect the assistance to be extended.

587. *Criterion 38.2* - As the Philippine system utilises a civil forfeiture regime, MLA relating to non-conviction based forfeiture orders would be recognised. Under Section 13 of the AMLA, as amended, AMLC has authority to apply for forfeiture in relation to a request made by a foreign state. Civil forfeiture under the AMLA applies in relation to non-conviction based confiscation proceedings. The related provisional remedies of bank inquiry and freeze order are available to AMLC in the preparation of a civil forfeiture case. The provisional remedy of asset preservation order is available during the pendency of the civil forfeiture case.

Criterion 38.3

588. *38.3 (a)* - Under 2018 IRR Rule 29 Section 4.3 (Investigation, Freeze Order, Bank Inquiry and Civil Forfeiture, AMLC shall adopt a flexible mechanism for coordinating with other States regarding requests for freezing and forfeiture of assets.

589. *38.3 (b)* - An asset management system on the maintenance and disposal of frozen and forfeited assets was established by AMLC pursuant to AMLC Resolution No. 22 of 2018. This allows AMLC to ensure that during the pendency of cases and after its forfeiture, the assets do not diminish in value and that it would be converted into cash before its transmittal to the National Treasury or repatriation to the requesting State.

590. Remedies under Section 39 of the Rules of Court on “Execution” are available in disposing of confiscated properties. Further 2018 IRR Rule 32 Section 1 Management of Frozen,

Preserved and Forfeited Assets) requires AMLC to establish mechanisms for managing and/or disposing preserved and forfeited assets.

591. *Criterion 38.4* - The ASEAN MLAT includes the provision for the Philippines to share confiscated property with other parties to the Treaty. Similarly, the UK MLAT includes explicit provisions for the sharing of assets (Articles 20-24). Other MLATs allow for sharing through the provision for the transfer or some or all of the proceeds of crime, instrumentalities or proceeds from the sale of these assets between Parties (art.15(3) of the China MLAT, art.17(3) of the Korea MLAT, art.18(3) of the Spain MLAT, and art.16(30) of the US MLAT).

592. Monetary instruments or properties forfeited in favour of the Government of the Philippines are considered revenue to be deposited with the National Treasury as income of the General Fund. The Philippines may share confiscated property relating to a criminal prosecution for ML offences with other countries, subject to the filing of a claim on the forfeited assets by said country with the Regional Trial Court which ordered the forfeiture (s.12(b) of the AMLA).

593. As explicitly provided under Rule 29 Section 4 of the IRR of AMLA, AMLC shall coordinate, if necessary, with the requesting State on the, procedure for, and mode of, turnover of the portion of the forfeited assets that belongs to the relevant persons in the requesting State.

Weighting and Conclusion

594. **Recommendation 38 is rated compliant.**

Recommendation 39 - Extradition

595. In its 2009 MER the Philippines was rated partly compliant with former Recommendation 39. The main deficiencies related to the lack of a process by which extradition took place.

596. *Criterion 39.1* - The Philippines is able to execute extradition requests, however there is no guarantee of execution without 'undue delay'.

597. *39.1 (a)* - ML and TF are extraditable offences under Section 13 (g) of the AMLA, as amended, and Section 20 of TFPSA, respectively. However, extradition is only pursuant to a treaty or convention, and is therefore not universally available. The Philippines has extradition treaties with Australia, Canada, China, Hong Kong, China India, Indonesia, Korea, Micronesia, Russia, Spain, Switzerland, Thailand, UK and US. Extradition is also supported by various international conventions that the Philippines has joined. The IRR explicitly confirms that the UN TF Convention is a basis for requesting or granting extradition relating to relevant offices (Rule 30 s.3).

598. *39.1 (b)* - Presidential Decree No. 1069 (*Prescribing the Procedure for the Extradition of Persons Who Have Committed Crimes in a Foreign Country*) governs extradition proceedings in the Philippines, but does not address case management or clear processes for prioritisation. Under Section 5 of the 2018 IRR Rule 30 (Extradition), DOJ and AMLC are required adopt a case management system, and clear processes for prioritisation and timely execution of extradition requests. The DOJ has a manual case management system (using Microsoft Excel), which allows them to easily search and retrieve information on requests for extradition. No information was provided on processes for the timely execution of extradition requests including prioritisation.

599. *39.1 (c)* - Presidential Decree No. 1069 (s.3), requires the existence of dual criminality in extradition cases. The requirements for execution of extradition requests are not unreasonable or unduly restrictive. A majority of the bilateral extradition treaties allow extradition as long as

TECHNICAL COMPLIANCE

an offence is punishable under the laws of Philippines and the requesting country, and the penalty imposed for the offence is imprisonment for at least one year. Some treaties dispel that requirement at the discretion of the jurisdiction that receives an extradition request. Some treaties give the requested State the discretion to consider a request for extradition even if the offence subject of the request, having been committed outside of its territory, would not be punishable in its jurisdiction.

600. Section 4 of the AMLA requires provision by the jurisdiction requesting extradition of documents relating to criminal offence, the decision or sentence or the criminal charge and the warrant of arrest.

601. *Criterion 39.2* - Most of the Philippines' treaties allow the refusal of an extradition request on the basis of nationality.¹⁰⁵ Philippines' treaties with India and United States are an exception and contain an explicit provision that extradition shall not be refused on the basis that the person sought is a citizen of the requested jurisdiction.

602. Only some of the Philippines' treaties contain a provision that codifies the principle that where extradition is refused, the person must be prosecuted.

603. *Criterion 39.3* - Presidential Decree No. 1069 (s.3), requires the existence of dual criminality in extradition cases. The test for dual criminality is "actual conduct", not terminology.

604. *Criterion 39.4* - There are no simplified extradition mechanisms in place in the Philippines.

Weighting and Conclusion

605. There are moderate shortcomings given that extradition is not available except pursuant to a treaty or convention. Further, there is no guarantee of execution without undue delay and most of treaties allow for the refusal of an extradition request on the basis of nationality, with only some treaties containing a provision that codifies the principle that where extradition is refused, the person must be prosecuted. There is also no evidence of a specific simplified process for extradition.

606. **Recommendation 39 is rated partially compliant.**

Recommendation 40 – Other forms of international cooperation

607. In its 2009 MER Philippines was rated largely compliant with former Recommendations 40 and SR. V. The requirements of R.40 have been revised significantly since the 2009 MER.

608. *Criterion 40.1* - Philippines provides a wide range of avenues for international cooperation in line with its policy that Philippines should not be used as a site to launder proceeds of crime (see Section 2 AMLA).

609. The range of mechanisms for international cooperation includes participation in international frameworks such as Egmont, INTERPOL, World Customs Organisation, IOSCO and International Association of Insurance Supervisors. Agencies are able to conclude and utilise MOAs with foreign counterparts to cooperate internationally. Lastly, the establishment of the Philippine Centre on Transnational Crime (PCTC) creates a focal point for competent authorities'

¹⁰⁵ Eleven of the fourteen bilateral extradition treaties of the Philippines allow refusal on the basis of nationality. These are with Australia (Art. 4[2][a]), Canada (Art. 4[1]), China (Art. 3[1]), HKSAR (Art. 3[1]), Indonesia (Art. VI[A]), Korea (Art. 6[1]), Micronesia (Art. 4[2][a]), Russia (Art. 3[1][g]), Spain (Art. 4[1][a]), Switzerland (Art. 3[2][b]) and Thailand (Art. VI[2]),

international cooperation on combatting transnational crime. This diversity of mechanisms for international cooperation provides Philippines' competent authorities with the ability to cooperate spontaneously or upon request. However, rapid provision of assistance was not demonstrated.

Criterion 40.2

610. *40.2 (a)* - AMLC's legal basis for providing cooperation is provided under Section 2 of the AMLA. PCTC's basis under Section 3 of the EO 62, and BSP's basis under R.A 7653. IC issued a Circular in November 2018 setting out that it shall provide cooperation to its foreign counterparts (s.1, IC CL No.61 2018). IC is also an active member of the IAIS and has been actively coordinating with other IAIS members.

611. The PCTC is the focal point for INTERPOL and is involved in international cooperation on transnational crimes. It also provides a mechanism for all competent authorities to cooperate through a shared central database for governmental agencies.

612. *40.2 (b)* - The range of mechanisms for international cooperation provides Philippines' competent authorities with options to use the most efficient means. There are no explicit restrictions on agencies with respect to the means for cooperation.

613. *40.2 (c)* - AMLC, as a member of the Egmont Group, has access to the ESW, within which it transmits and executes requests for information. AMLC can also exchange information with other FIUs by virtue of a Memorandum of Understanding (MOU). The Philippines have guidelines available to competent authorities for the exchange of information such as BSP Guidelines for the Exchange of Information. PNP is a member of INTERPOL and can use their gateways for information exchange. Customs is a WCO members and can use RILO.

614. *40.2 (d)* - AMLC has a Quality Management System (QMS) which outlines the processes for the prioritization and timely execution of requests for information. A Standard Operating Procedure for the Financial Intelligence Unit was also approved on 9 March 2018.

615. For BSP, prioritisation is based on the urgency and importance of the request. To ensure timeliness of response to request for information from the public (external stakeholders), the committed processing time, submitted in compliance with Monetary Board Resolution No. 1324.C, is fifteen (15) banking days (for simple request); and sixty (60) banking days (for requests requiring approval). Compliance with this timeline is monitored quarterly and submitted to BSP management.

616. The IC is mandated to respond for requests within fifteen (15) working days from receipt. However, timeliness of the response/reply is also relative to the intricacy and availability of the requested data or information. Although, upon evaluation of the request, if the request necessitates prioritization, the same is given preferential time for the action officer to act upon.

617. Specific processes for prioritisation and timely execution of international cooperation requests were not provided with respect to other competent authorities, in particular law enforcement agencies.

618. *40.2 (e)* - Rule 22.B of the 2018 IRR requires that AMLC, and its officers and staff are must securely protect information received or processed and shall not reveal, in any manner, any information known to them by reason of their office (see also Rule 6, s.1.4.3 and Rule 31, s.9 of the 2018 IRR to AMLA). The AMLC Guidelines on Information Sharing was also issued to serve as internal guidelines for the AMLC Secretariat is handling requests for information. Similar

TECHNICAL COMPLIANCE

provisions apply to the BSP under RA 7653 such that criminal and administrative sanctions attach to disclosure of any information of a confidential nature.

619. Specific processes for safeguarding information related to international cooperation were not provided with respect to other competent authorities, in particular LEAs.

620. *Criterion 40.3* - AMLC has a wide range of MOUs to exchange information with 39 foreign counterparts. From 2013-2017, AMLC was unable to sign any MOU with foreign counterparts due to a query/clarification with the Office of the President regarding the authority of AMLC, through the Executive Director, to enter into an MOU. Since then the DFA has clarified that AMLC need not obtain special authority from the President to enter into MOUs with counterpart FIUs in other countries.

621. The BSP has signed MOUs with counterpart regulators for all foreign banks that have a presence in the Philippines. If an MOU is to be concluded it must be with the authority of the Monetary Board granted to the Governor. BSP has MOUs with banking regulators in China, UK, Chinese Taipei, Hong Kong, China, Germany, Australia, Thailand and Indonesia.

622. PNP has bilateral agreements with foreign police forces (covering ML, financial or economic crimes, but not specifically TF) of Sweden, Korea, Qatar, Cambodia, Indonesia, and New Zealand. This is not a wide range of counterparts; however the police network through INTERPOL is also available to the PNP.

623. *Criterion 40.4* - Under Section 2.1 of the 2018 IRR Rule 32 Section 2 (Guidelines and Feedback Mechanism), AMLC, and the relevant supervisory authorities, LEAs and OGAs shall, as far as practicable, monitor and assess the quality, timeliness and usefulness of the assistance, cooperation or information obtained, including responses to requests for basic and beneficial ownership information or requests for assistance in locating beneficial owners residing abroad, they receive from the requested parties. AMLC and the relevant supervisory authorities, LEAs and OGAs, are compelled by 2018 IRR Rule 32 Section 2 to, whenever required, provide feedback to the requested parties, including foreign counterparts and non-counterparts, on the quality, timeliness and usefulness of the assistance, cooperation or information obtained.

624. *Criterion 40.5* - The sole grounds for refusal by AMLC, to providing information relates to the provision of financial intelligence where the release of information or documents may unduly prejudice an investigation or proceeding in the requested jurisdiction. Or if judicial proceedings concerning the same facts have been initiated. Or if the provision of the relevant information would prejudice the sovereignty, security, national or essential interest of the requested country

625. BSP may refuse sharing of information particular to customer account information, unless this is of particular relevance to the supervisory concern prompting the request.

626. These types of limitations to provision of information are not unduly restrictive or unreasonable.

627. *Criterion 40.6* - For information dissemination with counterpart FIUs, IRR Rule 31 Section 7 requires AMLC to establish controls and safeguards to ensure that information exchanged is used only for the purpose for, and by the authorities, for which the information was requested or provided. However, no information has been provided on controls established under that section. Various MOUs with foreign partners include controls on use of information.

628. The MOUs entered into by BSP with foreign counterparts contain a provision on the use of information, including limiting the subsequent use.

629. Further, the supervisory authorities (BSP, IC, SEC) are required under 2018 IRR Rule 31 Section 7 (Controls and Safeguards) s.7.2 to ensure that they have prior authorization from the requested foreign counterpart for any dissemination of information exchanged, or use of that information for supervisory and non-supervisory purposes, unless the concerned supervisor is under obligation to disclose or report the information. In such cases, at a minimum, the requesting supervisor shall promptly inform the requested foreign counterpart of this obligation as explicitly provided under Rule 31 Section 7 of the IRR of AMLA.

630. *Criterion 40.7* - AMLC staff are required to securely protect information received or processed and are prohibited to reveal, in any manner, any information known to them by reason of their office. This confidentiality of information is expressly provided under Rule 22 of the 2018 IRR, as amended. Likewise, both the Egmont Charter and the MOUs of AMLC with other FIUs provide provisions on the confidentiality of the requests for information and the information shared.

631. Obligation of confidentiality and information sharing apply to BSP staff under RA 7653 such that criminal and administrative sanctions attach to disclosure of any information of a confidential nature. Further, MOUs concluded by BSP contain provision as regards protection of information and parties' obligations concerning privacy and data protection.

632. Section 8 of Insurance Commission Circular Letter No. 2018-61 (23 November 2018) provides that the IC shall maintain the confidentiality of requests for information it receives and the information exchanged, in the same manner as it would protect similar request or information received from domestic sources. Further, under Section 64 of IC CL NO. 2018-48 and IC CL NO. 2018-60 (both 2018), the provisions of the 2018 IRR of the AMLA, as amended, apply where there is an insufficiency in IC Circular Letters.

633. No information was provided on other competent authorities.

634. *Criterion 40.8* - AMLC is authorised to make inquiries on behalf of foreign counterparts per Section 7 of the AMLA, as amended. The information that may be provided can be found in the AMLC database. For inquiries on identity, AMLC may issue orders to either the supervising authorities or covered persons to determine the true identity of the owner of any monetary instrument or property subject, among others, of a request for assistance from a foreign State as provided under s.7 (2) of the AMLA, as amended.

635. Section 8 of Insurance Commission Circular Letter No. 2018-61 (23 November 2018) provides that the IC shall, consistent with existing laws, conduct inquiries on behalf of their foreign counterparts, and, as appropriate, to authorise or facilitate the ability of foreign counterparts to conduct inquiries themselves in the Philippines, in order to facilitate effective group supervision.

636. There is no specific provision guaranteeing equivalence of information access between foreign and domestic counterparts. However the Philippines assert that the broad policy statement under s.2 AMLA which supports transnational cooperation for AML/CFT purposes is supportive of such a practice.

637. Limited information was provided on other competent authorities.

Exchange of Information Between FIUs

638. *Criterion 40.9* - Item 7 of AMLC Resolution no. 116, series of 2017, provides for AMLC to act on request for, or spontaneously disclose, financial intelligence to member FIUs of the Egmont Group and other non-Egmont member FIUs which it has an existing MOU. The 2018 IRR further

TECHNICAL COMPLIANCE

provides for AMLC to receive and take action in respect of any request from foreign states for assistance in their own AML operations as provided in the AMLA (Rule 6, s.1.4, 2018 IRR). S.2 of the AMLA provides for cooperation in transnational investigations and prosecutions of persons involved in ML. The instruments provide for legal basis for cooperation in relation to cooperation in information exchange in relation to ML, TF and predicate offences (Rule 6 s.1.4. of the RIR 2018).

639. *Criterion 40.10* - Rule 32 (s.2.4) of the 2018 IRR, provides for AMLC, when required, to provide foreign counterparts feedbacks on quality, timeliness and usefulness of the assistance, cooperation or information obtained.

640. *Criterion 40.11* - Section 2 (Declaration of Policy) of the AMLA, states that there are no legal limitations to the sharing of intelligence with foreign counterparts, pursuant to the power of AMLC under S.7 which is “to implement such measures as may be necessary and justified under this Act to counteract money laundering.” AMLC Resolution No. 125 AMLC Resolution No. 40 (Guidelines on Information Sharing) provide for AMLC to provide to foreign FIUs all information accessible to or obtainable by it, for intelligence purposes. This includes STRs/CTRs and its analysis, KYC documents, strategic and operational analysis, other types of intelligence information including from other domestic information received, gathered or analysed by AMLC (also in Rule 6, S.1.6 of the 2018 IRR).

Exchange of Information Between Financial Supervisors

641. *Criterion 40.12* - S.2 (2.4) of Rule 31 of the 2018 IRR permits supervisors to provide international cooperation based on their respective charters and laws. The BSP has established international cooperation through MOUs signed with foreign supervisory bodies. Nine MOU have been signed with overseas bank supervisors. S.5 and S.18 of the New Central Bank Act provides the legal basis for BSP to conduct international cooperation and to enter into contracts. The Monetary Board of the BSP has developed an internal procedure manual “Ground Rules for Information Sharing Between Home and Host Supervisors” to govern the framework of the MOUs. S.66.5 of the SRC permits the SEC to provide assistance to foreign enforcement authority of any country whose law grant reciprocal assistance if the requesting party is conducting investigation of the potential violation of any laws related to securities or commodities in the financial markets.

642. IC issued Circular Letter No.2018-61 to establish the international cooperation framework pursuant to 2018 IRR

643. *Criterion 40.13* - Rule 31 (s.2.5) of the 2018 IRR permits supervisors to exchange information with foreign counterparts within their legal power. BSP also has the power to obtain any data from local government bodies for the proper discharge of its functions and responsibilities (RA 7653 S.23), and to demand any documents, books and records from FI necessary for its supervision (RA 7653, s.25). S.16 and 27 of RA7653 provides BSP some legal grounds to permit disclosure of information of confidential nature or about the confidential operation when there is prior authorization of the Monetary Board or the Governor of the BSP. The power applies to existing MOUs that provide the BSP the authority to disclose information to the extent reasonable and permitted by law that will include those related to internal supervision and licensing documents domestically available to them.

644. Section 66.5 of the SRC permits the SEC to provide assistance to foreign enforcement authorities including the disclosure of information filed or transmitted to the SEC.

645. Section 1 of IC Circular Letter No.2018-61 permits IC, consistent with its existing laws, to exchange with foreign counterparts information domestically available to them, including information held by IC regulated entities, in a manner proportionate to their needs.

646. *Criterion 40.14* - Section 2 (2.6) of Rule 31 of the 2018 IRR permits supervisors to exchange information with foreign counterparts for group supervision purpose within their legal power. S.16 and 27 of RA7653 provides the BSP some legal grounds to permit disclosure of information of confidential nature when there is prior authorisation of the Monetary Board or the Governor of the BSP. Under its MOUs, BSP can exchange information of licensing process and on-going supervision that includes the regulatory information and prudential information of fit and proper of directors, senior offices and relevant shareholders. The information does not limit exchange of beneficial ownership information as permitted under s.17 of RA7653. S.66.5 of the SRC (RA 8799) permits the SEC to disclose any information available to foreign enforcement authority, including regulatory information, prudential information and required AML/CFT information.

647. Both the BSP and the SEC have the ability to request AML/CFT information that may relate to specific bank accounts through the MOUs/MOAs that the two supervisors signed with AMLC (see c.40.15).

648. Section 1 of IC Circular Letter No.2018-61 permits IC, consistent with its existing laws, to exchange regulatory information, prudential information and AML/CFT information.

649. *Criterion 40.15* - Section 2 (2.7) of Rule 31 of the 2018 IRR permits supervisors within their legal power to conduct inquiries on behalf of their foreign counterparts or to facilitate the foreign counter parts to conduct inquiries themselves. BSP has the power to authorise home jurisdiction authorities of the FIs to conduct on-site examination in the Philippines for the purpose of consolidated supervision, either by themselves or accompanied by the BSP, based on the Ground Rules for Information Sharing Between Home and Host Supervisors” and also in Paragraph 8 of the MOA with the Bank of Thailand.

650. The three FI supervisors have entered into MOU/MOAs individually with AMLC for the domestic information exchange that allow the FIs supervisors to obtain information available with AMLC, including information of bank accounts and investment accounts that are protected by secrecy provision (RA1405).

651. Prior consent of AMLC is required if the information requested by the FI supervisor is to be released to any other party (s.VI-A of the AMLC/BSP MOU; and art.III of the AMLC/IC MOA), which includes counterparties outside the Philippines.

652. Under s.66.5 of the SRC, SEC can provide assistance to foreign counter parts, including through inquiry on their behalf. It does not have the power to permit the foreign counterparts to conduct inquiry themselves.

653. Section 1 of IC Circular Letter No.2018-61 permits IC, consistent with its existing laws, to conduct inquires on behalf of foreign counterparties or allowing those parties to conduct inquiries themselves.

654. *Criterion 40.16* - MOU signed by BSP with foreign regulators include provisions to maintain confidentiality of information in the request (s.14 to 17 MOU with Bank of Thailand). Prior consent of the requested party must be obtained if the information is to be disclosed to a third party. The requesting party is obliged to promptly notify the foreign counterpart that the information obtained will be legally compelled to disclosure, and use all reasonable means to resist such demand or to protect the confidentiality.

655. Rule 66.5 of the RIRR of the SRC provides the power for the SEC to formulate rules governing information exchange including dissemination, safeguard and confidentiality of the

TECHNICAL COMPLIANCE

information. There is no further reference that prior authorisation shall be obtained from the requested counterparts when the information they provided have to be disseminated by the SEC.

656. S.6 of IC Circular Letter No.2018-61 set out the obligation to safeguard information and for IC to obtain prior approval from foreign counterparts for any disclosure of information exchanged.

Exchange of Information Between Law Enforcement Authorities

657. *Criterion 40.17* - AMLC Resolution (no. 116 of 2017) provides for AMLC, as the primary investigative agency for ML/TF, to receive and take action in respect of any request from foreign states for assistance in their own AML operations as provided in the AMLA (Rule 6, s.1.4, 2018 IRR). S.2 of the AMLA provides for cooperation in transnational investigations and prosecutions of persons involved in ML. The instruments provide for legal basis for cooperation in relation to cooperation in information exchange in relation to ML, TF and predicate offences (Rule 6 S.1.4. of the RIR 2018).

658. PCTC, (EO 62, 1999) is mandated to explore and coordinate information exchanges and training with other government agencies, foreign countries and international organizations involved in the combat against transnational crime. PNP serves as the National Central Bureau of the INTERPOL in the Philippines (s.1, MO 92 of 1993). Relevant LEAs have been designated by Section 5, EO 62, to assist the PCTC in its functions, and they can supply information through PCTC to foreign counterparts. However, there is no specific provision ensuring that the information exchanged is as broad as domestically available information.

659. *Criterion 40.18* - Philippine LEAs are able to investigate and obtain information on matters within their respective jurisdiction, and share these with their foreign counterparts. This is usually done through networks such as ASEANAPOL or INTERPOL.

660. 2018 IRR Rule 31.5.3 extends application of AMLC's financial analysis, investigations, and bank inquiries provision to instances where it is responding to requests for information and gathering information requested. LEAs may obtain bank information from AMLC, provided there is an existing MOU between the requesting LEA and the AMLC. This bank information may then be shared to the LEA's foreign counterpart for intelligence purposes.

661. *Criterion 40.19* - LEAs are not prohibited from conducting joint investigations. While there is no explicit provision permitting joint investigations, there is practice that demonstrates this is possible. For instance, in May 2014, the Joint Terrorist Financing Investigation Group (JTFIG) was formed by members of the anti- terrorism group of LEAs, such as the PNP, NBI and AMLC which has collaborated with the US FBI in joint investigations.

Exchange of Information Between Non-Counterparts

662. *Criterion 40.20* - There is no specific enabling provisions for competent authorities to exchange information indirectly with non-counterparts. AMLC provides a focal point for Philippines agencies seeking financial intelligence from other countries.

Weighting and Conclusion

663. Philippines' competent authorities have a wide range of mechanisms by which they can cooperate with foreign counterparts, in most, but not all, circumstances.

664. **Recommendation 40 is rated largely compliant.**

Summary of Technical Compliance – Key Deficiencies

Compliance with FATF Recommendations		
Recommendation	Rating	Factors underlying the rating
1. Assessing risks & applying a risk-based approach	LC	<ul style="list-style-type: none"> ▪ The understanding of external threats/ foreign proceeds is weak and vulnerabilities of related to the cash economy are not well understood. ▪ The vulnerabilities of legal persons/ legal arrangements in posing ML/TF risk, inter- linkages between covered persons and crimes.
2. National cooperation and coordination	C	<ul style="list-style-type: none"> ▪ The Recommendation is fully met
3. Money laundering offence	LC	<ul style="list-style-type: none"> ▪ Tax crimes are not a predicate offence; ▪ There is a lack specific inclusion of “association” in the definition of ancillary offences.
4. Confiscation and provisional measures	PC	<ul style="list-style-type: none"> ▪ There is a gap with respect to authorities’ ability to seize a wide range of property that is subject to confiscation. ▪ There is a lack of provisions to enable authorities to void or prevent actions that prejudice the ability to restrain or recover property subject to confiscation. ▪ There are practical impediments to LEAs other than AMLC directly accessing bank records to trace assets. ▪ There are minor gaps with mechanisms for the preservation and management of assets.
5. Terrorist financing offence	LC	<ul style="list-style-type: none"> ▪ There are gaps in coverage of the financing of travel of individuals for the purpose of terrorist acts and the providing or receiving of terrorist training.
6. Targeted financial sanctions related to terrorism & TF	PC	<ul style="list-style-type: none"> ▪ There are shortcomings relating to the evidentiary standard of proof for making a UNSCR 1267 proposal to the UN for designation as well as for domestic designations under UNSCR 1373. ▪ For UNSCR 1373 designations, authorities cannot operate <i>ex parte</i> against an entity proposed for designation and there is no mechanism to operate against an individual.
7. Targeted financial sanctions related to proliferation	NC	<ul style="list-style-type: none"> ▪ The Philippines lacks specific measures to implement TFS related to proliferation of WMD.
8. Non-profit organisations	LC	<ul style="list-style-type: none"> ▪ There are knowledge gaps regarding the composition of the NPO sector, relating to both registered and unregistered NPOs. ▪ The Philippines is yet to fully implement targeted risk based supervision or monitoring.
9. Financial institution secrecy laws	LC	<ul style="list-style-type: none"> ▪ The power to inquire into bank deposits is solely vested with AMLC, which results in delays with some competent authorities obtaining CDD information to

Compliance with FATF Recommendations		
Recommendation	Rating	Factors underlying the rating
		<p>understand beneficial ownership in keeping with R.24.6</p> <ul style="list-style-type: none"> AMLC does not share PEP-related bank account information to other competent authorities or foreign counterparts during an election period.
10. Customer due diligence	LC	<ul style="list-style-type: none"> For some types of legal person or legal arrangement, there is not a clear requirement for ownership structures to be examined, and beneficial owners or persons acting on behalf of the customer be identified and their identities verified.
11. Record keeping	C	<ul style="list-style-type: none"> The Recommendation is fully met
12. Politically exposed persons	LC	<ul style="list-style-type: none"> PEP requirements set out by BSP are only applicable to close associates in restricted circumstances.
13. Correspondent banking	C	<ul style="list-style-type: none"> The Recommendation is fully met
14. Money or value transfer services	LC	<ul style="list-style-type: none"> There are shortcomings with the actions taken by the Philippines to identify and apply sanctions to unregistered RTCs.
15. New technologies	C	<ul style="list-style-type: none"> The Recommendation is fully met
16. Wire transfers	LC	<ul style="list-style-type: none"> There is a gap with the timeframe by which information must be made available by ordering institutions to beneficiary institutions for domestic wire transfers. There is a gap with the requirement that CDD and wire transfer transaction records will be made available swiftly to competent authorities. The wire transfer provisions do not apply to FIs supervised by SEC or IC.
17. Reliance on third parties	C	<ul style="list-style-type: none"> The Recommendation is fully met
18. Internal controls and foreign branches and subsidiaries	LC	<ul style="list-style-type: none"> Financing and lending companies that are not captured as covered persons or required to implement internal controls.
19. Higher-risk countries	LC	<ul style="list-style-type: none"> There is no requirement for EDD to be applied to customers from higher risk countries when called upon to do so by the FATF. There is no requirement that customers that are legal persons from higher risk countries be subject to EDD. AMLC, BSP, SEC and IC do not provide regular updates to FIs on countries that have AML/CFT deficiencies.

Compliance with FATF Recommendations		
Recommendation	Rating	Factors underlying the rating
20. Reporting of suspicious transaction	PC	<ul style="list-style-type: none"> ▪ Obligations to report attempted transactions are not directly covered in law or regulation. ▪ The requirement to report STRs related to tax offences is not clear as tax offences are not a predicate to ML. ▪ The five working day timeframe to report STRs does not fulfil the 'promptly' requirement.
21. Tipping-off and confidentiality	C	<ul style="list-style-type: none"> ▪ The Recommendation is fully met
22. DNFBPs: Customer due diligence	PC	<ul style="list-style-type: none"> ▪ There are gaps with the coverage of CDD and record keeping by casinos ▪ There are scope deficiencies in relation to third party reliance. ▪ The real-estate sector is not covered for AML/CFT requirements ▪ There is inconsistency of the definition of lawyers-/accountants-covered persons with FATF standards ▪ DNFBPs are not required to apply additional measures to the family members and associate of PEPs
23. DNFBPs: Other measures	PC	<ul style="list-style-type: none"> ▪ STRs: tax crimes are not predicate offences, attempted transactions not being subject to STRs and the timeframe for reporting is not 'prompt'. ▪ Real estate agents are not covered persons under AMLA and there are, scope deficiencies related to lawyers and accountants. ▪ There is an absence of supervisory measures imposed on casinos for high risk countries that warrant attention by the FATF or by the supervisory authorities.
24. Transparency and beneficial ownership of legal persons	PC	<ul style="list-style-type: none"> ▪ Basic information on cooperatives is only available through an FOI request. ▪ There are no measures in place to mitigate the risk associated with bearer share warrants nor to address the risks relating to nominee shareholders and nominee directors. ▪ The power to inquire into bank deposits is solely vested with AMLC, which results in delays with some competent authorities obtaining CDD information to understand beneficial ownership.
25. Transparency and beneficial ownership of legal arrangements	PC	<ul style="list-style-type: none"> ▪ There are no obligations on trustees of non-business trusts (private trusts) to obtain and hold adequate, accurate, and current information on the identity of the settlor, the trustees, the protector (if any), the beneficiaries or class of beneficiaries, and any other

Technical compliance

Compliance with FATF Recommendations		
Recommendation	Rating	Factors underlying the rating
		<p>natural person exercising ultimate effective control over the trust</p> <ul style="list-style-type: none"> There are no obligations on private trustees to disclose their status to financial institutions and DNFBPs when forming a business relationship or carrying out an occasional transaction above the threshold Beneficial ownership information for private trusts (whether chartable, foreign or other) is not available. The penalties available if the trustee entity fails to provide timely access to information regarding the trust are not proportionate or dissuasive.
26. Regulation and supervision of financial institutions	LC	<ul style="list-style-type: none"> SEC lacks fit and proper requirements to prevent criminals and their associates from holding significant control (or being shareholder or beneficiary owner) of its covered persons IC lacks fit and proper requirements for HMOs beyond directors and officers. Financing and lending companies are not subject to AML/CFT regulation and supervision. BSP's risk-based model does not explicitly take account the broader ML/TF risks presented in its on-site supervision.
27. Powers of supervisors	LC	<ul style="list-style-type: none"> There are gaps with the administrative liability of directors and management of SEC regulated institutions that are legal persons.
28. Regulation and supervision of DNFBPs	PC	<ul style="list-style-type: none"> The suitability procedures of PAGCOR licensees only cover the board of directors and not shareholders or beneficial owners. Gaps with the fit and proper framework for land-based casinos supervised by CEZA and APECO. A risk-based AML/CFT supervision framework is yet to be established for casinos. Real estate agents are not covered persons subject to any AML/CFT requirements.
29. Financial intelligence units	PC	<ul style="list-style-type: none"> There is only an implied mandate for AMLC's dissemination of ML-related financial analysis to other authorities, but no explicit provision to that effect. AMLC cannot share information related to PEPs outside AMLC during election periods, which is an impediment to operational independence and autonomy.
30. Responsibilities of law enforcement and investigative authorities	C	<ul style="list-style-type: none"> The Recommendation is fully met

Compliance with FATF Recommendations		
Recommendation	Rating	Factors underlying the rating
31. Powers of law enforcement and investigative authorities	LC	<ul style="list-style-type: none"> LEAs in the Philippines are not specifically empowered to engage in special investigative techniques.
32. Cash couriers	PC	<ul style="list-style-type: none"> No competent authority has the authority to request and obtain further information from the carrier in cases of a false declaration or a failure to declare. Fines are not proportionate or dissuasive. Competent authorities are not empowered to restrain currency and BNI suspected of ML/TF or other predicate offences.
33. Statistics	LC	<ul style="list-style-type: none"> Shortcomings in the systems for maintaining statistics relating to confiscation and non-MLA international cooperation requests.
34. Guidance and feedback	LC	<ul style="list-style-type: none"> Only limited feedback has been given to FIs and DNFBPs.
35. Sanctions	LC	<ul style="list-style-type: none"> Administrative fines available for individual failings are not dissuasive. There are gaps with the administrative liability of directors and management of DNFBPs and SEC regulated institutions that are legal persons.
36. International instruments	LC	<ul style="list-style-type: none"> Tax offences are not covered as predicate offences for ML.
37. Mutual legal assistance	LC	<ul style="list-style-type: none"> Shortcomings with processes for the timely prioritisation and execution of MLA requests.
38. Mutual legal assistance: freezing and confiscation	C	<ul style="list-style-type: none"> The Recommendation is fully met
39. Extradition	PC	<ul style="list-style-type: none"> Extradition is not available except pursuant to a treaty or convention. No guarantee of execution without undue delay. Most of treaties allow for the refusal of an extradition request on the basis of nationality, with only some treaties containing a provision that codifies the principle that where extradition is refused, the person must be prosecuted. There is no evidence of a specific simplified process for extradition.
40. Other forms of international cooperation	LC	<ul style="list-style-type: none"> Shortcomings in the range of mechanisms by which authorities can cooperate with foreign counterparts.

Glossary of Terms

AFP	Armed Forces of the Philippines
AMLA	Anti-Money Laundering Act
AMLC	Anti-Money Laundering Council
APECO	Aurora Pacific Economic Zone and Freeport Authority
APO	Asset Preservation Order
ARRG	AMLC Registration and Reporting Guidelines
ARRS	AML Risk Rating System
ATC	Anti-Terrorism Council
BIR	Bureau of Internal Revenue
BNI	Bearer-negotiated instrument
BOC	Bureau of Customs
BSP	Bangko Sentral Pilipinas (the Central Bank of the Philippines)
CDA	Cooperative Development Authority
CDD	Customer Due Diligence
CEZA	Cagayan Economic Zone Authority
CIDG	Criminal Investigation and Detection Group
CIRR	Casino Implementing Rules and Regulations
CMIC	Capital Markets Integrity Corporation
CSEZFP	Cagayan Special Economic Zone and Freeport
CSP	Corporate Service Provider
CSR	Company Registration System
CTR	Covered Transaction Report
DFA	Department of Foreign Affairs
DOJ	Department of Justice
DSWD	Department of Social Welfare and Development
DTI	Department of Trade and Industry
STMO	Strategic Trade & Management Office (DTI)
EDD	Enhanced Due Diligence
EMI	E-Money Issuer
ESW	Egmont Secure Web
FCIG	Financial Crimes Investigation Group
FIAG	Financial Intelligence Analysis Group
FSID	Financial System Integrity Department
FTF	Foreign terrorist fighters
GIS	General Information Sheet
HSA	Human Security Act
IC	Insurance Commission
IOSCO	International Organization of Securities Commissions
IRR	Implementing Rules and Regulations
ISIL	Islamic State of Iraq and the Levant
JTFIG	Joint Terrorism Financing Intelligence Group
KYC	Know Your Customer
LEA	Law enforcement agency
LEG	Litigation and Evaluation Group
LGU	Local Government Unit
LRA	Land Registration Authority
MLA	Mutual Legal Assistance
MLAT	Mutual Legal Assistance Treaty
MLPP	Money Laundering Prevention Program
MOA	Memorandum of Agreement
MORB	Manual of Regulations for Banks
MSB	Money Service Business

MVTS	Money Value Transfer Service
NACC	National AML/CFT Coordination Committee
NACS	National AML/CFT Strategy
NALECC	National Law Enforcement Coordinating Committee
NATS	National Anti-Terrorism Strategy
NBI	National Bureau of Investigation
NICA	National Intelligence Coordinating Agency
NPO	Not-for-profit organisation
NPS	National Prosecution Service
NRA	National Risk Assessment
NSC	National Security Council
NSSLA	Non-stock savings and loan associations
OFAC	Office of Foreign Assets Control
OMB	Office of the Ombudsman
OSG	Office of the Solicitor General
PAGCOR	Philippine Amusement Gaming Corporation
PAOCC	Presidential Anti-Organized Crime Commission
PCNC	Philippine Council for NGO Certification
PCTC	Philippine Centre for Transnational Crime
PDEA	Philippine Drug Enforcement Agency
PDS	Personal Disclosure Statement
PEP	Politically Exposed Person
PF	Proliferation financing
PHP	Philippine peso
PNP	Philippine National Police
PNP-ACG	Philippine National Police – Anti-Cybercrime Group
PNP-AKG	Philippine National Police – Anti-Kidnapping Group
PNP-IG	Philippine National Police – Intelligence Group
PNP-SAF	Philippine National Police – Special Action Force
POGO	Philippine Offshore Gaming Operator
RBA	Risk-based approach
RIAS	Rules on Imposition of Administrative Sanctions
RIRR	Revised Implementing Rules and Regulations
RSA	Remittance sub-agent
RTC	Regional Trial Court
RTC	Remittance Transfer Company
SCAML/CFT	NALECC Sub-Committee on AML/CFT
SCOC	NALECC – Sub-Committee on Organised Crime
SEC	Securities and Exchange Commission
SOCTA	Serious and Organized Crimes Threat Assessment
STR	Suspicious Transaction Report
TBML	Trade-based money laundering
TFPSA	Terrorism Financing Prevention and Suppression Act of 2012
TFS	Targeted financial sanctions
TFTF	Task Force on Terrorism and Terrorism Financing
TSCP	Trust or Company Service Provider
UNSCR	United Nations Security Council Resolution
WMD	Weapons of Mass Destruction