FATF

APG

Anti-money laundering and counter-terrorist financing measures

Singapore

Mutual Evaluation Report

September 2016

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

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

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

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

This assessment was adopted by the FATF at its June 2016 Plenary meeting.

Citing reference:

FATF and APG (2016), *Anti-money laundering and counter-terrorist financing measures - Singapore,* Fourth Round Mutual Evaluation Report, FATF, Paris and APG, Sydney
www.fatf-gafi.org/publications/mutualevaluations/documents/mer-singapore-2016.html

CONTENTS

Executive Summary

1. This report provides a summary of the anti-money laundering and combating the financing of terrorism (AML/CFT) measures in place in Singapore as at the date of the on-site visit (17 November 2015 to 3 December 2015). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Singapore's AML/CFT system, and provides recommendations on how the system could be strengthened.

Key Findings

- Singapore's AML/CFT coordination is highly sophisticated and inclusive of all relevant competent authorities. Driven by the AML/CFT Steering Committee and the Inter-Agency Committee, the coordination mechanism in Singapore is a very valuable tool in AML/CFT policy development. This proved to be true in the development of the National Risk Assessment (NRA) and the cooperation and organisation associated with this mutual evaluation exercise. Singapore has a strong focus on law and order and enforcement, which often result in dissuasive penalties.

- Singapore has a reasonable understanding of its ML risks and has taken steps to mitigate them. Nevertheless, moderate gaps remain. In particular the nexus between transnational threats, the inherent risks faced by Singapore as one of the world's largest financial centres, and vulnerabilities within the system is not sufficiently reflected in Singapore's NRA.

- Singapore's ability to proactively identify and address serious foreign predicate ML, and transnational ML networks will be strengthened with moderate improvements in Singapore's understanding of its foreign predicate ML risks. Singapore provided information that it was pursuing some complex cases involving transnational fraud and corruption. However, Singapore has prosecuted few foreign predicate ML cases outside of wire transfer frauds involving money mules/shell companies, and has confiscated low amounts of proceeds of crime. Singapore has demonstrated that it has a general understanding of its TF risks. But the weighting placed in the risk methodology on indicators derived from reported incidences in Singapore has somewhat hindered Singapore's ability to appreciate the inherent TF risks associated to its geographical location and its status as a global financial centre.

- Singapore's FIU, the Suspicious Transactions Reporting Office (STRO), uses well-functioning systems and coordination mechanisms to integrate FIU information into LEA processes. Singapore's primary investigative agencies routinely make significant use of STRs at early stages of ML and predicate investigations. While financial intelligence information is provided to other agencies, they are yet to make significant use of such information to support investigation. STRs relating to TF, while routinely disclosed to the Internal Security Department (ISD), have not resulted in any criminal investigations.

- Singapore's FIs generally demonstrated a reasonably good understanding of ML risks impacting Singapore domestic clients, but a less developed understanding of the risk of illicit flows into and out of Singapore. FIs and especially DNFBPs had a less mature understanding of TF risks, and often failed to distinguish between terrorism and TF risks. Overall, there is a significant difference in the level of understanding of the ML/TF risks between the financial sector and DNFBP sector, therefore limiting DNFBPs' ability to develop a comprehensive risk understanding.

- For most FIs, AML/CFT supervision appears robust, with a variety of off-site factors examined and comprehensive on-site examinations/follow-up being conducted. Singapore has recently extended AML/CFT supervision to most types of DNFBPs, but there are significant differences in effective supervision of AML/CFT requirements between relevant supervisory bodies. While Singapore has a range of remedial measures that it can impose on FIs, the financial penalty structure across the DNFBP sector is quite diverse and concerns exist about the differences in approach in terms of dissuasiveness and proportionality. Apart from the casino and TSP sectors, sanctions for non-compliance by DNFBPs have not been tested.

- Singapore has not undertaken an adequate ML/TF risk assessment of all forms of legal persons and legal arrangements. Authorities however acknowledge that legal persons and arrangements created in Singapore, and those registered or operating in Singapore from foreign jurisdictions, can be used to facilitate predicate crimes and ML/TF offences. Singapore has implemented some preventive measures designed to prevent the misuse of legal persons and arrangements for ML and TF, including the collection of beneficial ownership information by FIs and DNFBPs. However, in practice, some DNFPBs do face challenges in obtaining beneficial ownership information.

- On international cooperation, Singapore provides constructive and high quality information and assistance when requested, but faced occasional challenges executing some MLA requests in a timely manner. Although few outgoing MLA requests were made prior to 2015, Singapore has taken steps to increase outgoing MLA requests in 2015, more than doubling the entire number of MLA requests in the previous 3 years. Singapore also uses informal channels and the LEAs, FIU and financial supervisors are generally well engaged in making and receiving requests where permitted. Singapore shares domestically available beneficial ownership information for legal persons and legal arrangements, however there is limited information available under the domestic framework.

Risks and General Situation

2. Singapore maintains one of the lowest domestic crime rates in the world,1 and therefore, the bulk of Singapore's exposure to ML risks arises from offences committed overseas. In particular, Singapore's status as both a major global financial centre and an international trade/transportation hub makes it vulnerable to becoming a transit point for illicit funds from abroad. According to Singaporean authorities, foreign predicate offences constituted 66% of all ML investigations and 27% of all ML convictions in Singapore between 2008 and 2014. Singapore's NRA published in January 2014 identifies common predicate offences committed in Singapore (e.g. cheating (the term which Singapore uses for fraud), unlicensed money lending (UML) and criminal breach of trust (CBT), as well as foreign predicate cheating offences and proceeds of overseas corruption as posing relatively higher ML threats to Singapore.

3. The main conduits of ML identified in the NRA are banks, remittance agents, shell companies and individual money mules. Around 77% of the funds managed in Singapore are foreign sourced, with the majority of assets under management coming from the Asia-Pacific region. The size and foreign exposure of Singapore's private banking and asset management industry increases Singapore's ML/TF vulnerabilities. In addition, Singapore's position as an international trade/transportation hub also increases its ML/TF vulnerabilities. Given the complexity and large volume of trade financing services offered in Singapore, this banking sub-sector is also exposed to a higher level of ML/TF risk. Moreover, legal persons and arrangements also remain vulnerable to misuse given the broad range of financial services available.

4. Singapore is situated in a region where several terrorist groups operate actively and have carried out attacks in the last 10 years. Singapore's NRA report highlights that "there has been no evidence of TF being committed in Singapore or terrorist funds flowing into or through Singapore." An assessment of the TF threat posed by ISIL was subsequently conducted, and the findings were communicated to all FI, DNFBP and NPO supervisors.

Overall Level of Effectiveness and Technical Compliance

5. Singapore's AML/CFT regime has undergone significant reform since the last assessment in 2008. Singapore has a strong legal and institutional framework for combating ML, TF, and PF. Technical deficiencies identified in Singapore's ML offence were addressed in 2010, and more recently the crime of ML was extended to cover more predicate offences, such as serious tax offences. The technical compliance framework is particularly strong regarding law enforcement, confiscation, targeted financial sanctions, preventive measures for and the supervision of FIs, and international cooperation but less so regarding transparency of legal persons and arrangements, and preventive measures and sanctions for non-compliance for DNFBPs.

6. In terms of effectiveness, Singapore achieves substantial results in risk understanding and mitigation, international cooperation, collection and use of financial intelligence, and proliferation financing, and only moderate improvements are needed in these areas. More significant improvements are needed in other areas as indicated below.

---

[1] According to data presented in the United Nations Office on Drugs and Crime (UNODC)'s report on International Statistics on Crime and Justice. See also: www.unodc.org/documents/data-and-analysis/Crime-statistics/International_Statistics_on_Crime_and_Justice.pdf

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

7. Singapore's AML/CFT coordination at the operational level is highly effective and inclusive of all relevant competent authorities. The Inter-Agency Committee coordinated the development of the National Risk Assessment (NRA) and the cooperation and organisation associated with the mutual evaluation. Singapore authorities consult across the private sector in AML/CFT policy development including the development of the NRA. Operational activities of authorities are targeted towards identified risk and resources are allocated accordingly both in terms of quantity and quality.

8. The NRA process has established a basis for the private sector and government agencies to understand Singapore's ML/TF risks. However, there remain moderate gaps in Singapore's overall understanding of risk. While Singapore has taken mitigation efforts to address the transnational risks that it has identified (such as from shell companies, trade based money laundering, as well as laundering of proceeds of corruption and tax evasion), some other forms of ML and TF relevant to Singapore's context should have been given greater attention. In particular the nexus between transnational threats and specific vulnerabilities in Singapore could be better articulated to in order to promote a deeper understanding of how the ML/TF risks can materialize in the Singapore context. Singapore's risk assessments take into account indicators such as STRs filed, incoming formal and informal requests for information, interaction with foreign counterparts and international reports. However, the national risk understanding reflects a disproportionate focus on domestic predicate ML and smaller-scale forms of transnational ML.

9. Singapore in its NRA identifies domestic source TF as a low to medium threat and foreign source TF as a medium threat. While Singapore has a Strategic understanding of TF risk to a certain extent, in particular foreign sources of funding, they should further focus on factors such as geographical factors, level and extent of terrorism activity in the region and inherent risks such as Singapore being a financial, transport and people hub. The private sector's tactical level understanding of 'risk' is too focused on screening databases and adverse news rather than TF risk factors, and financial institutions' and DNFPBs' understanding of TF risk is often conflated with terrorist threat.

10. Private sector entities report that the NRA has been useful. Beyond the NRA, authorities had issued additional guidance and red flag indicators to the private sector, but key information on transnational threats is not made public, including information on jurisdictions assessed to be high-risk As far as the financial sector is concerned, foreign FIs (banks in particular) have a good understanding of ML risks, while FIs with a domestic focus demonstrated a less sophisticated understanding of ML and, in particular TF risks facing them. All DNFBPs demonstrated a basic level awareness of risks but the risk mitigating measures significantly vary within the sector.

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

11. Singapore has a strong legal and institutional framework for domestic ML investigation and prosecution. This has been enhanced through legislative changes, ML-focused investigation policies and increased resources in key LEAs. LEAs have access to a wide range of information for the purposes of their investigations, including financial intelligence, information from public databases and police records such as criminal history and police intelligence, however have limited access to tax and trade information.

12. Financial intelligence is stored in STRO's database and includes STRs, Cash Movement Reports (CMRs), and threshold Cash Transaction Reports (CTRs). STRO has direct access to law enforcement information and relevant police units have direct access to STRO information. STRO can also request further information from financial institutions to support its enquiries. STRO makes use of liaison officers from various investigative agencies and this has contributed to the dissemination of STRs that are relevant to LEAs and generally of high quality.

13. The primary ML investigative authorities (CAD and CPIB) routinely make significant use of STRs at early stages of ML and predicate investigations with the majority of asset seizures and ML investigations, relating to both domestic and foreign predicate offences, being supported by STRs. Other investigative and regulatory agencies have made limited use of STRs in predicate offence investigations. STRs relating to TF, while routinely disclosed to ISD, have led only to false positives name matches and have not resulted in any criminal investigations.

14. Singapore has significantly increased the number of ML investigations, prosecutions and convictions since its last mutual evaluation, and this is commendable. In particular, Singapore has targeted key domestic ML threats, such as UML, through the effective use of its ML offences. However, limitations in Singapore's understanding of its nexus with foreign ML risks may have some ramifications for Singapore's ability to proactively identify and address serious foreign predicate ML and transnational ML networks. This has led to most of Singapore's transnational ML cases so far relating to offenders involved in smaller-scale and less complex forms of ML offending (e.g. UML and money mules), whereas Singapore should also more aggressively target the more complex cases expected of a sophisticated financial centre such as Singapore (while continuing to successfully target UML and money mules).

15. While Singapore has a comprehensive legal framework for seizing and confiscating criminal proceeds, Singapore did not demonstrate that confiscation is a strategic priority in Singapore's criminal justice regime and there is a lack of emphasis on the pursuit of confiscation of proceeds of crime as a goal in its own right. Nevertheless, Singapore has made some good operational and policy changes to promote asset seizure and confiscation since 2013. This has not yet provided tangible results, but should do so in the future.

16. While there is a strong framework in place to detect the illicit cross-border movement of cash and bearer negotiable instruments, Singapore pursues criminal prosecutions for more serious cases of offending (which ordinarily result in a fine), but does not pursue confiscation as a sanction for breaches of its cross-border reporting regime.

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

17. Singapore has a strong legal framework for the criminalisation of TF. While Singapore has a general understanding of its TF risks, it is not clear that Singapore's risk assessment has fully taken into consideration the TF vulnerabilities associated with its geographical location and its position as a financial hub. . While Singapore has taken preventative actions against a number of individuals and organisations in relation to terrorism, Singapore does not consider criminal investigations of TF an appropriate response within its national security framework. Consequently there have been no separate and independent TF criminal investigations. Instead, preventive and other powers are used by Singapore's ISD to address TF. Despite a total number of 780 potential TF case leads dealt with by

the ISD, other than clearing false positive name matches, it does not appear that financial investigations have ever been undertaken in relation to TF.

18. Singapore has effectively implemented TFS. Listing in Singapore is automatic after UN designation and without delay. The financial supervisor has created an e-mail alert system for FIs and the broader public, including DNFBPs, to receive updates to various UN sanctions list. This has been proven effective and FIs and the majority of DNFBPs are well aware of their TF freezing obligations. While Singapore's competent authorities have appropriate regulations and enforcement powers in place to safeguard NPOs from TF abuse, Singapore has not implemented a targeted approach in doing so. Oversight of NPOs is restricted to good governance reviews with a lack of targeted reviews based on any assessment of TF abuse risks.

19. Singapore actively mitigates the PF risk through TFS and controls on dual-use goods under the relevant international agreements. Singapore demonstrated a robust information sharing mechanism among relevant authorities in charge of export control, financial supervision, intelligence and law enforcement. This has resulted in FIs and DNFBPs (except for PSMDs which are not supervised) being well aware of the targeted financial PF-related sanctions against Iran and the DPRK.

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

20. FIs and DNFBPs demonstrated a fair understanding of ML risks impacting Singapore domestic clients, but a less developed understanding of the risk of illicit flows into and out of Singapore. The understanding of TF risk by FIs was less current but in line with the limited findings of the published NRA report. DNFBPs' understanding of TF risk is poor.

21. The requirements for CDD, record-keeping and PEP clients were well understood by FIs, however there are gaps in their understanding of geographical risks relating to the proceeds of corruption entering Singapore. Overall, DNFBPs' implementation of CDD and PEP requirements is rather basic and this seems to be due to the fact that AML/CFT preventive measures were recently introduced for most of them. The STR reporting obligation is overall well understood by FIs. Within the financial sector, the banking sector has submitted the most number of STRs but the number of STRs filed by DNFBPs, except casinos, is low. It was notable that most FIs which the assessment team spoke to had not filed STRs related to TF, however, reporting entities did file targeted financial sanctions name matches as STRs.

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

22. Singapore has a generally robust system for ensuring that criminals or their associates do not misuse FIs. For most FIs, AML/CFT supervision by the Monetary Authority of Singapore (MAS) appears robust, with a variety of off-site factors examined and comprehensive on-site examinations/follow-up being conducted. Supervision is based on the individual risk profile for each FI, however given the inconsistencies identified in both the NRA and the individual assessments of risk in FIs, targeting on the basis of ML/TF risks is not optimal. Supervision only recently included SVFs and non-bank credit and debit card issuers. There is a wide range of sanctioning tools available for the financial sector, ranging from warnings/reprimands to criminal prosecution/removal of

licences and these have been used. No direct enforcement action has been taken in relation to the senior management of FIs.

23. Singapore has recently developed and extended its AML/CFT supervision to most types of DNFBPs. There are significant differences in effective supervision of AML/CFT requirements across relevant supervisory bodies. The majority of PSMDs are not subject to AML/CFT supervision. In contrast with the financial sector, the financial penalty structure across the DNFBP sector is quite diverse and enforcement of the sanctioning regime for non-compliance with AML/CFT measures is at an early stage.

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

24. Singapore has not undertaken a ML/TF risk assessment of all forms of legal persons and legal arrangements. Authorities acknowledge that legal persons and arrangements created in Singapore, and registered or operating in Singapore from foreign jurisdictions, can be used to facilitate predicate crimes and ML/TF offences. However, there is an uneven understanding within the government and the private sector of the inherent and residual risks associated with legal persons and arrangements.

25. Basic information on legal persons and arrangements is readily available. However, the existing measures and mechanisms are not sufficient to ensure that accurate and up-to-date information on beneficial owners is available in a timely manner. While Singapore has put CDD measures in place requiring FIs and CSPs (including lawyers and accountants) to collect beneficial ownership information, in practice the collection of beneficial ownership information is not always possible given deficiencies in the implementation of preventive measures within the DNFBP sector.

26. Stronger enforcement of existing obligations would contribute to dissuading the misuse of legal persons and arrangements. Sanctions for failure to comply with the beneficial ownership requirements are available but have rarely been used in practice.

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

27. Singapore provides a range of international cooperation, including MLA, extradition, intelligence/information, and beneficial ownership information. The feedback indicates that the quality of assistance is generally high, often supporting complex investigations and helping to secure convictions. However the feedback also suggests that there were occasional delays in the execution of requests. Singapore indicates that since the 3rd round mutual evaluation, it has adopted a policy of positively responding to requests as far as possible; time is often taken to seek clarifications to facilitate the processing of requests which do not contain sufficient information. However, delays can also be caused by strict interpretation of the MACMA or a lack of resources to deal with an increasingly complex caseload. Asset restraint can be conducted quickly using domestic LEA powers; however this channel requires that LEAs conduct a domestic ML investigation. Using the MACMA restraint provisions is an alternative, a process that takes longer because of the requirement for an order of the High Court.

28. Few outgoing MLA requests are made, although Singapore has increased efforts since 2015. With respect to other forms of cooperation, the LEAs, FIU and financial supervisors are generally well engaged in making and receiving requests where permitted.

29. Singapore shares domestically available beneficial ownership information for legal persons and legal arrangements, however there is limited information available under the domestic framework.

Priority Actions

30. The prioritised recommended actions for Singapore, based on these findings, are:

- Singapore should conduct comprehensive ML and TF risk assessments for all types of legal persons (private companies, public companies, foreign companies, etc.) to identify where the risks are and develop policy to address those risks.
- Singapore should ensure effective supervision for AML/CFT across all categories of DNFBPs through risk-based, targeted and prioritised outreach to and inspections of the non-financial professions, and extend AML/CFT supervision to all PSMDs. Singapore should also increase the level of communication and information sharing by competent authorities and SRBs to ensure a better understanding of the ML/TF risks by the DNFBP sector.
- Financial sector supervisors should continue dialogue with the FIs to promote a better understanding of ML and TF risks, and more closely target supervisory activity to ML/TF risks.
- Singapore should take steps to improve the capability of its LEAs to proactively identify and investigate ML, particularly complex and foreign predicate ML. Singapore should pursue more offenders involved in the laundering of foreign proceeds of crime in addition to the current focus on pursuing money mules and shell companies.
- LEAs should more proactively pursue the confiscation of proceeds of crime and make greater use of the seizure and confiscation powers in the Corruption, Drug Trafficking and other Serious Crimes (Confiscation of Benefits) Act (CDSA) to pursue proceeds of crime that are not directly linked to offences being prosecuted.
- The next round of Singapore's NRA should better articulate the nexus between key threats and vulnerabilities to promote a deeper understanding of how the ML/TF risks faced by Singapore will materialise in Singapore's context. In particular, this analysis should take into consideration Singapore's geographic location and role in the international economy, and deal more specifically with the ML threats to the financial sector in the context of Singapore's position as a financial centre.
- Singapore should conduct a comprehensive sector review to better understand the types of organisations within the NPO sector that are

inherently vulnerable to TF abuse and continue outreach to NPOs to raise awareness of specific TF abuse risks.

- Singapore should continue to use MLA to follow and restrain assets that have moved to other jurisdictions, and to pursue the people involved and improve response times in responding to foreign requests.
- Given Singapore's status as a global trade, finance and transportation hub, the FIU should seek to obtain additional strategic information sources, such as international electronic fund transfer reports and trade data, to complement existing reports that provide insight into international ML/TF threats.

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

Technical Compliance Ratings

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

C = Compliant
LC = Largely compliant
PC = Partially compliant
NC = Non-compliant

.

MUTUAL EVALUATION REPORT

Preface

This report summarises the AML/CFT measures in place in Singapore as at the date of the on-site visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Singapore'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 Singapore, and information obtained by the evaluation team during its on-site visit to Singapore from 17 November 2015 to 3 December 2015.

The evaluation was conducted by an assessment team consisting of:

- Mr. Ian Matthews, Financial Conduct Authority, U.K (financial expert)
- Mr. Shunichi Fukushima, Ministry of Finance, Japan (financial and targeted financial sanctions expert)
- Mr. Alastair Bland, Charities Directorate, Canada (risk and NPO expert)
- Mr. Ken Menz, Attorney-General's Department, Australia (legal expert)
- Mr Andrew Hill, Financial Intelligence Unit, New Zealand (law enforcement expert)
- Mrs. Larissa Alanna Gray, World Bank (international cooperation expert)

The assessment process was lead and supported by Mr. Richard Berkhout, senior policy analyst and assessment co-led, Ms. Lia Umans and Ms. Masha Rechova, policy analysts, and Ms. Ailsa Hart, research assistant (all FATF Secretariat) and Mr. Gordon Hook, Executive Secretary of Asia/Pacific Group on Money Laundering and assessment co-lead.

The report was reviewed by Ms. Kellie Bailey, Financial Intelligence Unit, Belize; Dk. Nurul Ehsani Binti Pg Mohammad, Financial Intelligence Unit, Brunei Darussalam; Mr. Gajanan Nabar, Securities and Exchange Board, India; Mr. Emmanuel Mathias, International Monetary Fund.

Singapore previously underwent a FATF Mutual Evaluation in 2008, conducted according to the 2004 FATF Methodology. The 2008 Mutual Evaluation and 2011 follow-up report have been published and are available at: www.fatf-gafi.org/countries/s-t/singapore/.

Singapore's 2008 Mutual Evaluation concluded that the country was compliant with 11 Recommendations; largely compliant with 32; partially compliant with 4; and non-compliant with 2. Singapore was rated compliant or largely compliant with 15 of the 16 Core and Key Recommendations. Singapore was placed under the regular follow-up process immediately after the adoption of its 3rd round Mutual Evaluation Report. Following additional steps taken to address deficiencies in Recommendation 1, Singapore in February 2011 moved from regular follow-up to biennial updates.

CHAPTER 1. ML/TF RISKS AND CONTEXT

31. The Republic of Singapore is an island country off the southern tip of the Malay Peninsula, in Southeast Asia. The city state is separated from Malaysia to the north by the narrow Johore Strait and from Indonesia to the south by the wider Singapore Strait. Singapore has a land area of 718 square kilometres, and a total coastline of 193 kilometres (120 miles). The population stands at about 5.470 million,[2] of which 3.870 million are Singapore citizens and permanent residents. The remaining 1.60 million are non-residents working, studying or living in Singapore on a non-permanent basis. The three largest ethnic groups are the Chinese, the Malays, and the Indians.

32. A sovereign state since 1965, Singapore is a republic operating on a Westminster system of unicameral parliamentary government. Parliament is elected by general election every five years. The Singapore Parliament consists of both elected and non-elected Members of Parliament (MPs). Elected MPs are drawn from candidates who have won the general elections, while non-elected MPs are appointed by Parliament and may be non-politicians nominated to provide a greater variety of nonpartisan views. The Cabinet, chaired by the Prime Minister, is collectively responsible to the Parliament.

33. Singapore's legal system is rooted in the English common law tradition and characterised by the doctrine of judicial precedent (or stare decisis). The judiciary is one of the three constitutional pillars of government along with the legislative and the executive. The full Judicial power in Singapore is vested in the Supreme Court (the Court of Appeal and High Court) as well as subordinate courts (Magistrate and District Courts) by the Constitution of Singapore. The highest court is the Court of Appeal, which hears both civil and criminal appeals from the High Court and the State Courts. Decisions of the Court of Appeal are binding on lower courts. There is a single nationa law.

34. Singapore is a wealthy ASEAN member state with the world's 36th largest economy (GDP was about USD 307.87 billion in 2014[3]) and 16th highest gross national income per capita (about USD 55 150). The national currency is the Singapore dollar (SGD), which is also accepted as customary tender in Brunei Darussalam.

ML/TF Risks and Scoping of Higher-Risk Issues

Overview of ML/TF Risks

35. While Singapore maintains one of the lowest domestic crime rates in the world,[4] its status as a major global financial centre inevitably exposes it to ML/TF risks disproportionate to its domestic criminal environment. Singapore's National Risk Assessment (NRA) report was published in January 2014 and identifies common predicate offences committed in Singapore (e.g.

[2] Singapore Ministry of Trade & Industry – as of June 2015 (Available at: www.singstat.gov.sg/docs/default-source/default-document-library/publications/publications_and_papers/reference/sib2015.pdf).

[3] World Bank (nd), World Bank Data: Singapore , http://data.worldbank.org/country/singapore.

[4] According to data presented in the United Nations Office on Drugs and Crime (UNODC)'s report on International Statistics on Crime and Justice, Singapore's crime rate is one of the lowest in the world. See also: www.unodc.org/documents/data-and-analysis/Crime-statistics/International_Statistics_on_Crime_and_Justice.pdf

1

cheating[5]/fraud, unlicensed money lending (UML) and criminal breach of trust (CBT)), as well as foreign predicate cheating offences and proceeds of overseas corruption as posing relatively higher ML threats to Singapore. According to the NRA, cheating generates the highest amount of criminal proceeds among all domestic and foreign predicate offences. The main conduits of ML identified in the NRA are banks, remittance agents, shell companies and individual money mules.

36. In 2014, Singapore recorded 32 196 cases of crime. While slightly higher than 2013 (28 984 recorded cases), the 2013 crime rate was the lowest registered in 30 years. Approximately 72% of the recorded cases in 2014 are potential proceeds-generating crimes (23 297) representing four main categories of crimes (commercial crimes, housebreaking and related crimes, theft and related crimes and violent/serious property crimes).

37. The bulk of Singapore's exposure to ML risks arises from offences committed overseas. In particular, Singapore's status as both a major global financial centre and an international transport hub makes it vulnerable to becoming a transit point for illicit funds generated throughout East and South East Asia. Notably, UNODC in April 2013 estimated that proceeds of crime within the Asia Pacific amount to as much as USD 90 billion, with drug trafficking and timber smuggling representing the two largest sources of illicit funds.[6] According to Singaporean authorities, foreign predicate offences constituted 66% of all ML investigations and 27% of all ML convictions in Singapore between 2008 and 2014. Meanwhile, the amount of foreign criminal proceeds seized amounted to USD 230 million.

38. The size and foreign exposure of Singapore's private banking and asset management industry increases Singapore's ML/TF vulnerabilities. Between 2012 and 2013, total assets managed by Singapore-based asset managers grew by 11.8% to SGD 1.82 trillion (approx. EUR 1.2 trillion / USD 1.28 trillion[7]).[8] Furthermore, around 77% of the funds managed in Singapore are foreign sourced, with the majority of assets under management coming from the Asia Pacific region. The high-value and bespoke service that can be offered in these sub-sectors, exposes the private banking and asset management industry in Singapore to significant ML/TF risks, including from PEPs.

39. Singapore's position as an international trade and transportation hub also increases its ML/TF vulnerabilities. Given the complexity and large volume of trade financing services offered in Singapore, this banking sub-sector is exposed to a higher level of ML/TF risk. Singapore's NRA report also identifies that *"weaknesses have been observed in AML/CFT controls of trade finance (…) such as inadequate policies and procedures, and insufficient transaction monitoring"*. In addition, Singapore currently has 8 Free Trade Zones (FTZs) which pose inherent ML/FT risks, as FTZs are generally characterised by relaxed oversight and an absence of trade data and systems integration.

40. Singapore's NRA report identifies an increase in the number of ML cases involving shell companies established by non-residents based overseas. Given the tax incentives for foreign trusts in

---

[5] Cheating is defined in art. 415 of the Criminal Code and corresponds to the predicate offence of fraud, as referred to in the FATF standards.

[6] UNODC (2013), Transnational Organized Crime in East Asia and the Pacific – A Threat Assessment, www.unodc.org/documents/data-and-analysis/Studies/TOCTA_EAP_web.pdf

[7] Conversion rates as of 17 November 2015 (start of the on-site visit): 1 SGD = 0.6596 EUR and 1 SGD = 0.7021 USD.

[8] MAS (2013), Singapore Asset Management Industry Survey 2013, www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Surveys/Asset%20Management/2013%20AM%20Survey%20Public%20Report_25072014_Final%20revised.pdf.

Singapore and the broad range of financial services available, legal arrangements in Singapore remain vulnerable to misuse for ML/TF purposes. While professional trust service providers are regulated for AML/CFT requirements, including the conduct of CDD and holding of beneficial ownership (BO) information, the understanding of risk within the sector is limited. There is currently no estimate of the size and/or foreign exposure of Singapore's trust industry. Notably, Singapore criminalised the laundering of proceeds of serious tax offences on 1 July 2013, bringing it in line with FATF requirements.

41. Singapore is situated in a region where several terrorist groups operate actively and have carried out attacks in the last 10 years. Nevertheless, Singapore states that it has not detected any evidence of any TF cases since the disruption of Singapore's Jemaah Islamiyah (JI) in December 2001. Singapore's NRA report highlights that "there has been no evidence of TF being committed in Singapore or terrorist funds flowing into or through Singapore." An assessment of the TF threat posed by ISIL was subsequently conducted.

Country's risk assessment & Scoping of Higher Risk Issues

Country's risk assessment

42. In January 2014, Singapore published its first NRA report following a two-year government-wide ML/TF risk assessment exercise. The NRA was conducted under the ambit of the AML/CFT Steering Committee with participation of over 15 government agencies. The NRA analysed national ML and TF risks, and covered 14 financial sub-sectors and 8 non-financial sectors. The report identifies three higher risk financial sectors, namely full banks, remittance agents and money changers, and internet-based stored value facility (SVF) holders. For the non-financial sector, the NRA report identifies company service providers (CSP), the casino sector and the pawnbrokers sector as having a higher ML/TF risk. The NRA report identifies sectors requiring further study, in which emerging risks may manifest. Specifically, Singapore identified virtual currencies, precious stones and metals dealers (PSMDs), and the Singapore Freeport as topics for further study. The NRA report also identifies tax offences and trade-based money laundering (TBML) as foreign criminal threats of interest, although, the NRA report does not provide an analysis of TBML or tax offences beyond stating that *"it is noted that there are reports internationally that have cited these crime types as risk areas for Singapore but the number of cases investigated, foreign requests for assistance received and seizures relating to these offences is very low"*. Nonetheless, the authorities have disseminated red flag indicators, conducted outreach and issued guidance in order to sensitise reporting entities to the elevated threat level posed by these crime types. Singapore identified domestic source TF as a low to medium threat and foreign source TF as a medium threat.

43. Singapore has since used the results of the NRA to help shape aspects of how it combats ML. In particular, the report identifies a few sectors where the controls were relatively less robust, and authorities have since put in place measures to better mitigate the ML/TF risks. These include additional measures for money-changers and remittance agents, and new measures for PSMDs, CSPs and pawnbrokers. In the more vulnerable areas identified in the NRA, law enforcement agencies and the STRO, Singapore's FIU, have worked with relevant domestic authorities to develop red flag indicators to improve the detection of ML/TF in their respective sectors. These lists of red flag indicators, which are disseminated to the regulated entities via their sector supervisors, are also publicly available on STRO's webpage.

1

44. Generally, Singapore has a reasonable understanding of its risks. However, while Singapore identifies an increase in the number of ML cases involving shell companies established by non-residents based overseas to launder proceeds of cheating, all forms of legal persons and legal arrangements have not been adequately assessed. Individual departmental assessments of certain forms of legal persons were conducted prior to the NRA and based on previous identified incidences, media reporting and discussions with LEA. However, the results of these assessments were not subsequently included in the NRA report for consideration by other agencies and the private sector. The analysis appears to have drawn the conclusion that legal entities providing professional services are inherently low risk, overlooking the risk of ML through services. In the NRA report, the focus of risks relating to legal arrangements is on the risk of TSPs, rather than legal persons/arrangements themselves or the nexus between legal persons/arrangements abuse.

45. While risks related to proceeds of overseas corruption and trade-based money laundering are mentioned in official assessments such as the NRA report, assessors are of the view that more could be done to understand these risks. Similarly, moderate improvements are needed in terms of understanding of the threats posed by large-scale international ML networks, with cases cited by the Singapore authorities relating more to smaller scale transnational offending.

46. Within the context of Singapore's national security strategy, combatting terrorism and combatting TF are from a policy perspective considered equivalent. This approach risks conflating terrorism threat with TF risk, although officials actively seek to understand international experience of TF to maintain awareness. Assessors found the awareness of the distinction between terrorism and TF risk within the financial sector and DNFPBs more limited.

Scoping of Higher Risk Issues

47. In deciding what issues to prioritise, the assessment team reviewed material provided by Singapore on national ML/TF risks, and information from reliable third party sources (e.g., reports of other international organisations). The issues listed present not only the areas of higher ML/TF risks (including threats and vulnerabilities), but also contain issues that were of significant concern to the assessment team based on material provided before the on-site visit.

i. Legal/ operational and international cooperation issues

   a. Foreign predicate offences**.** The risk and/or magnitude of foreign proceeds of crime laundered through Singapore, in particular stemming from fraud (a.k.a. "cheating" in Singapore), drug trafficking, environmental crime, tax crime and corruption in the region. Singapore's geographic location and the large size and international reach of its financial sector make Singapore vulnerable to being a transit point for illicit funds both ML/TF-related through South East Asia, and other foreign jurisdictions. Additionally, the lack of evidence of TF flows may be caused by an absence of such flows (low risk), or by a lack of focus (higher risk).

   b. Misuse of corporate vehicles, trusts for ML/TF purposes. Singapore is particularly vulnerable to the misuse of legal persons due to its low tax regime, which raises the risk of attracting funds generated from tax crimes, and the relative ease of starting a business. In addition, the lack of available data on the size and scope of Singapore's trust industry, with the exception of trusts administered by licensed trust companies, makes it difficult to accurately assess the scale of ML/TF risk for legal arrangements.

ii. Vulnerabilities in financial and DNFBP sectors

a. Trade finance. The growth in the trade finance industry poses a number of ML/TF risks for Singapore. Singapore's NRA report identifies that "*weaknesses have been observed in AML/CFT controls of trade finance (…) such as inadequate policies and procedures, and insufficient transaction monitoring.*" Given that TBML necessarily requires intermingling of the trade sector with the finance sector, the assessment looked in more detail at the application of CDD and other preventive measures in trade finance transactions (in particular regarding due diligence on the source of funds and identification of beneficial ownership.). Moreover, Singapore's status as a hub of international trade also increases its vulnerability to PF. The NRA contains an in-depth analysis on how the current AML/CFT system works effectively to detect and prevent trade and financial transactions involving Iran and the DPRK that could be made in a disguised manner.

b. Private banking and asset management industry. Singapore's private banking and asset management industry has seen significant growth in recent years. As indicated above, between 2012 and 2013, total assets managed by Singapore-based asset managers grew by 11.8% to SGD 1.82 trillion. Furthermore, around 77% of the funds managed in Singapore are foreign sourced, with the majority of assets under management coming from the Asia Pacific region. The assessment also considered this issue in relation to customer due diligence, in particular regarding PEPs, the source of funds, ongoing transaction monitoring, and identification of beneficial ownership and the extent to which the private banks and asset management firms in Singapore are effectively complying with the existing AML/CFT obligations.

c. Gatekeepers and other DNFBPs (in particular, lawyers, accountants and CSPs): The sector presents higher ML/ TF vulnerability given that AML/CFT measures and their implementation are not as strong as those in the financial sector. A significant amount of AML/CFT legislation for DNFBPs (CSPs, accountants, real estate agents, and pawnbrokers) has also been enacted in the last twelve months requiring further examination into the level of implementation and the enforcement of the new legislation, including outreach activities to DNFBPs.

Materiality

48. Singapore has a highly developed, trade-oriented market economy. Situated along the vital shipping lanes of the Straits of Malacca, Singapore is one of the busiest ports in the world, connected to more than 600 ports in over 120 countries.[9] With an airport serving some 110 airlines flying to over 240 cities in about 60 countries and territories worldwide, Singapore serves as a major gateway to Southeast Asia.[10] Singapore's GDP was SGD 390.1 billion (approx. EUR 257.3 billion / USD 273.9 billion) in 2014, with a per capita GNI of SGD 69 168 (approx. EUR 45 623 / USD 48 563). Total trade amounted to SGD 982.7 billion (approx. EUR 648.2 billion / USD 690 billion), of which SGD 518.9 billion (EUR 342.3 billion / USD 364.3 billion) were from exports. Singapore's top five trading partners are China, Malaysia, the European Union, the United States and Indonesia.

[9] MPA (nd), Global Hub Port, www.mpa.gov.sg/web/portal/home/maritime-singapore/what-maritime-singapore-offers/global-connectivity/global-hub-port

[10] Changi Airport Group (nd), Parnering Us, www.changiairportgroup.com/cag/html/business-partners/.

1

49. Manufacturing is a pillar of Singapore's economy. Singapore's skilled workforce and strong business environment, which includes political stability and a robust legal framework, have rightfully drawn thousands of multinational corporations to invest and establish a wide range of businesses centred on petrochemicals, pharmaceuticals and electronics. In recent decades, the relative importance of services to the Singapore economy has grown substantially. As at the end of 2014, the services industry contributed nearly two-thirds of the GDP and employed 70% of the workforce.

50. The finance and insurance sub-sector is the fourth largest sub-sector by GDP. Singapore's financial sector had about SGD 2.7 trillion (approx. EUR 1.78 trillion / USD 1.90 trillion) in assets in 2013 (amounting to 73.7% of GDP). The IMF's 2013 Financial Sector Assessment Program (FSAP) found Singapore's financial system to be highly developed, and well regulated and supervised, with Singaporean authorities giving a strong emphasis to integrity and stability in finance and to compliance with international standards. According to the Financial Stability Board, shadow banking assets in Singapore were worth 30 billion in 2014.[11]

51. Singapore's economy contracted 0.6% in 2009 as a result of the global financial crisis, but rebounded 15.1% in 2010, on the strength of renewed exports, before slowing in 2011-14, largely as a result of the European recession and China's slowdown.[12] Future growth is forecast to remain at a moderate 2–4% rate for 2015.[13] Unemployment remains low, at just under 2%, and prices are subdued without stoking worries about deflation.[14]

Structural Elements

52. The key structural elements for effective AML/CFT control appear to be present in Singapore. Political and institutional stability, accountability and rule of law are all present. There also exists a high level of political commitment to tackling domestic corruption, as evidenced by the ongoing work of the Corrupt Practices Investigation Bureau (CPIB). In 2013, there was a 96% conviction rate with respect to the corruption cases that went to trial.[15] In addition, Singapore consistently ranks in the top five countries on the Transparency International Corruption Perception Index meaning that it is perceived to be one of the least corrupt countries in the world. Singapore also has a capable and independent judiciary, headed by the Supreme Court of Singapore.

53. Singapore's institutional structure provides it with the necessary framework to implement its AML/CFT regime. The institutional AML/CFT framework in Singapore is centred around the AML/CFT Steering Committee, which acts as the national AML/CFT coordination authority. For a full overview of the institutional framework see Section 1.4 (b).

---

[11] Based on the FSB report, the size of Singapore's shadow banking sector is as follows: End-2013 – USD 31.9 billion and End-2014 – USD 30.0 billion. (FSB (2015), Global Shadow Banking Monitoring Report 2015, www.fsb.org/2015/11/global-shadow-banking-monitoring-report-2015).

[12] Know Your Country (December 2014), Singapore: Risk & Compliance Report, www.knowyourcountry.com/singapore1111.html

[13] MAS (2015), Macroeconomic Review, April 2015 (MAS), www.mas.gov.sg/~/media/resource/publications/macro_review/2015/Chpt%202%20Apr%2015.pdf].

[14] Ibid.

[15] Clifford Chance (2014), A Guide to Anti-corruption legislation in Asia Pacific 2014, http://globalmandatoolkit.cliffordchance.com/downloads/Anti_corruption_Guide_nov_2014.pdf.

Background and other Contextual Factors

Overview of AML/CFT strategy

54. Singapore's AML/CFT Steering Committee published a national AML/CFT Policy Statement on 8 June 2015.[16] According to Singapore authorities, the Statement reflected long-standing policy objectives. The Policy Statement is posted on the websites of MHA, MOF and MAS.

55. Singapore's AML/CFT policy objectives are to: i) detect, deter and prevent money laundering, associated predicate offences and terrorism financing; and ii) protect the integrity of its financial system from illegal activities and illicit fund flows. To achieve these policy objectives, Singapore has identified the following eight principles: "(*i) allocate resources on a risk-sensitive basis; (ii) maintain close policy and operational coordination and cooperation across the Government; (iii) take a preventive approach that combines tough licensing and comprehensive reporting requirements, strict AML/CFT regulations, and risk-based supervision of the relevant financial and non-financial sectors; (iv) enhance private sector stakeholders' understanding of ML/TF risks and promote a culture of compliance; (v) take decisive and deterrent law enforcement action against ML/TF activity, including that relating to foreign crimes; (vi) disrupt drug dealing and other serious offences early to prevent proceeds from being laundered; (vii) provide assistance to other jurisdictions through formal and informal channels spontaneously and on request; (viii) rigorously implement and contribute to the development of international standards[…]*".[17]

Overview of the legal & institutional framework

56. The following are the main ministries, and authorities responsible for formulating and implementing the government's AML/CFT and proliferation financing policies:

i. Ministries and coordinating committees

- AML/CFT Steering Committee: The Steering Committee is the national AML/CFT coordination authority, comprising the Permanent Secretary of the Ministry of Home Affairs, Permanent Secretary of the Ministry of Finance (MOF) and Managing Director of the Monetary Authority of Singapore (MAS).
- Inter-Agency Committee (IAC): The IAC supports the AML/CFT Steering Committee as the main operational body that coordinates the implementation of the national AML/CFT policy. The IAC comprises Singapore's key AML/CFT agencies, including policy makers, the financial intelligence unit, law enforcement authorities, supervisors, customs and tax authorities, intelligence services, and the Attorney General's Chambers.
- Inter-Ministry Committee on Counter Terrorism (IMC-CT): The IMC-CT was set up in 2001 under the auspices of the Attorney-General's Chambers

[16] MOF (nd), Singapore's AML/CFT Policy Statement, www.mof.gov.sg/Policies/Anti-Money-Laundering-Countering-the-Financing-of-Terrorism-AML-CFT/Singapores-AML-CFT-Policy-Statement

[17] MOF (nd), Singapore's AML/CFT Policy Statement,www.mof.gov.sg/Policies/Anti-Money-Laundering-Countering-the-Financing-of-Terrorism-AML-CFT/Singapores-AML-CFT-Policy-Statement

(AGC) and the Ministries of Foreign Affairs and Law to ensure Singapore's full compliance with its international obligations and to strengthen its national capacity to implement measures to combat international terrorism. The members of the IAC and the IMC-CT work together to ensure a consistent and coherent approach in Singapore's counter terrorism and CFT strategy.

- Inter-Ministry Committee on Export Controls (IMC-EC): The IMC-EC provides a whole-of-government policy oversight of all export control matters and serves as Singapore's policy and operational coordination mechanism for implementation of UNSCRs pertaining to WMD-proliferation and related issues.
- Ministry of Home Affairs (MHA): MHA is in charge of maintaining law and order as well as internal security in Singapore. In respect of the AML policy/regime, the Ministry has responsibility for the relevant legislation, chiefly the Corruption, Drug Trafficking and other Serious Crimes (Confiscation of Benefits) Act (CDSA), as well as the Terrorism (Suppression of Financing) Act (TSOFA).
- Ministry of Finance (MOF): The main regulatory statutes under the MOF are the Companies Act, Business Registration Act and Accountants Act. MOF is the parent ministry to the Inland Revenue Authority of Singapore, the Accounting and Corporate Regulatory Authority, the Singapore Customs and the Singapore Totalisator Board.
- Ministry of Law (MinLaw): MinLaw is responsible for advancing access to justice, the rule of law, the economy and society through policy, law and services. In the area of international cooperation to combat ML/TF, MinLaw is the parent ministry for the Mutual Assistance in Criminal Matters Act, the Extradition Act and the United Nations Act.
- Attorney-General's Chambers (AGC): The AGC is the independent Organ of State responsible for legislative drafting and reform; advising the Government on all domestic and international legal matters; prosecution of offenders and making applications to prevent dissipation of proceeds of crime. The AGC is also Singapore's Central Authority for mutual legal assistance in criminal matters, and is also in charge of processing extradition requests.

ii. Criminal justice and operational agencies

- Commercial Affairs Department (CAD): The CAD is a specialist department of the Singapore Police Force (SPF), which focuses on matters related to commercial crime. The expertise of ML/TF investigations lies within the CAD, under the Financial Investigation Group (FIG). The key role of the FIG

is to ensure that all ML and TF cases are properly investigated and to provide cross-jurisdictional assistance relating to ML and TF.

- Internal Security Department (ISD): ISD of the Ministry of Home Affairs has a specialised and dedicated team of investigators that collects and analyses intelligence in relation to all terrorism-related activities, including TF activities. ISD's team of investigators works closely with the Counter-Financing of Terrorism Branch (CFTB) of CAD with respect to TF investigations. Moreover, ISD will propose individuals/entities found to be involved in terrorism activities to the IMC-TD for designation as terrorists under the First Schedule to the TSOFA.
- Central Narcotics Bureau (CNB): CNB is responsible for enforcing the CDSA in relation to seizure of drug assets. CNB's Financial Investigation Team investigates into the financial affairs of drug traffickers, with a view to confiscating all benefits derived from drug trafficking.
- Corrupt Practices Investigation Bureau (CPIB): CPIB, a department under the Prime Minister's Office, is responsible for enforcing the CDSA in relation to bribery offences and investigating related ML.
- Suspicious Transaction Reporting Office (STRO): STRO is Singapore's financial intelligence unit (FIU). The establishment and the functions of the STRO are expressly provided for in section 3A of the CDSA. STRO is currently housed under the Intelligence Group (ING) in CAD following a re-organisation in 2013.

iii. Financial Sector Supervisors

- Monetary Authority of Singapore (MAS): MAS is the integrated regulator and supervisor of the financial sector (including Licensed Trust Companies).
- Insolvency and Public Trustee's Office (IPTO) - Moneylenders: IPTO is a department under MinLaw which handles matters relating to insolvency, public trust, moneylending and pawnbroking. More specifically, IPTO licenses and regulates moneylenders, who are required to fulfil their AMLCFT obligations under the Moneylenders (Prevention of Money Laundering and Financing of Terrorism) Rules 2009.

iv. DNFBP Supervisors and Self-Regulatory Bodies

- Casino Regulatory Authority (CRA): CRA is a statutory board established under the Casino Control Act to regulate Singapore's casinos.
- Accounting and Corporate Regulatory Authority (ACRA): ACRA is the national regulator of business entities and public accountants in Singapore,

as well as the facilitator for the development of business entities and the public accountancy profession.

- Institute of Singapore Chartered Accountants (ISCA): ISCA is the national accountancy body of Singapore. It is mandatory for all public accountants regulated by ACRA to be ISCA members. Professional accountants not registered as public accountants may also be members of ISCA.
- The Law Society (LawSoc): LawSoc is the statutory entity responsible for regulating the Singapore legal profession.
- Council for Estate Agencies (CEA): CEA is a statutory board established under the Estate Agents Act 2010 to administer the enhanced regulatory framework for the real estate agency industry. Commencing its operations from 22 October 2010, CEA's principal functions are to license the estate agents (referring to the estate agencies) and register salespersons (referring to the property agents), promote the integrity and competence of estate agents and salespersons and engage in public education efforts to help consumers in property transactions.
- Insolvency and Public Trustee's Office (IPTO) - Pawnbrokers: IPTO is a department under Ministry of Law that handles matters relating to insolvency, public trust, moneylending and pawnbroking. More specifically, IPTO licenses and regulates pawnbrokers, who are required to fulfil their AML/CFT obligations under the Pawnbrokers Act 2015.
- Office of the Commissioner of Charities: The Office of the COC (set up in 2006) is the supervisory authority appointed to provide regulatory oversight of the charity sector.
- Majlis Ugama Islam Singapura (MUIS): MUIS is the supervisory authority appointed to provide regulatory oversight of Singapore's mosques.
- Notably, there have been several changes to Singapore's institutional framework since the last assessment in 2008. For example, the CAD underwent a reorganisation in October 2013 where the functions of each branch and division within CAD have been more clearly defined so as to enable its investigators to specialise and become more adept in their area of work. There are now distinct branches within the CAD's FIG for ML investigations, TF investigations and the fostering of international cooperation related to ML/TF. CPIB also set up a Financial Investigations Branch in 2011 to specifically conduct ML investigations.

Overview of the financial sector and DNFBPs

57. Singapore is ranked by the IMF as one of 29 systemically important financial centres in the world. As of 31 December 2014, there were more than 1 000 financial institutions in Singapore (see table below). They provide a wide range of financial services including trade financing, foreign

exchange, derivatives products, capital markets activities, loan syndication, underwriting, mergers and acquisitions, asset management, securities trading, financial advisory services and insurance services. In 2014, financial services accounted for 11.8% of Singapore's GDP and 5.4% of total employment in the economy.

58. Singapore's financial sector is dominated by banks and mainly intermediates financial flows with East Asia and Europe. Total banking sector assets amounted to USD 2 trillion as of December 2013.[18] Commercial banks make up 78% of the financial system, of which two-thirds are attributable to foreign banks. The latest Financial Sector Assessment Program (FSAP) assessment in 2013 found that "foreign banks represent about 65% of assets in Singapore." The insurance sector is the second largest component of Singapore's financial system, although amounting to only about 6% of the financial system.

59. Singapore is one of the world's fastest growing asset management centres, due to the large range of financial services offered and the jurisdiction's attractive tax regime. As of 2014, there were more than 600 fund management firms, with SGD 880 billion (approx. EUR 580 billion or USD 617 billion) in assets under management (AUM), of which approximately 77% come from sources outside Singapore. Assets booked in Singapore and Hong Kong, China are expected to account collectively for 20% of global offshore assets by 2018.[19]

Table 1. **Number and Size of Financial Institutions registered with MAS/IPTO**

Type of Financial Institution	Number of licensed/approved institutions *as of 31 December 2014*	Total Assets *as of 31 December 2014* (in SGD billions, unless otherwise specified)
Full Banks	33	1 623
Wholesale Banks	55	527
Offshore Banks	37	122
Merchant Banks	38	96
Non-Bank Credit Card Issuers	2	6.7[20]
Finance Companies	3	16
Direct Life and Composite Insurers	21	155[21]
Insurance Brokers	70[22]	2.0
Fund Management Companies	589	1 031
Licensed broker-dealers	116	51
Corporate Finance Advisory Firms	42[23]	28
Approved Trustees	13	155

[18] MAS (nd), Banking Sector, www.mas.gov.sg/singapore-financial-centre/overview/asian-dollar-market.aspx

[19] Private Banker International, www.privatebankerinternational.com/.

[20] Total billings for all card issuers (including banks) was SGD 44.6b in 2014, of which Amex and Diners accounted for a total of SGD 6.7b.

[21] This refers to the total life insurance assets of direct life and composite insurers.

[22] Of which 36 are also exempt financial advisers providing financial advisory services.

[23] This includes licensed broker-dealers who also provide corporate finance advisory services.

Type of Financial Institution	Number of licensed/approved institutions *as of 31 December 2014*	Total Assets *as of 31 December 2014* (in SGD billions, unless otherwise specified)
Securities Depository	1	13[24]
Financial Advisers	61	0.3
Money-changers	381	40[25]
Remittance Agents	72	30[26]
Multi-purpose Stored Value Facilities	4	-
Financial Holding Companies	2	-
Moneylenders	179	0.6

60. Full banks generally face higher inherent risks, owing to their larger customer base, higher transaction volume and the international nature of their transactions. These banks offer a wide range of products and services and serve a broad spectrum of corporate and individual customers, including higher risk customers such as PEPs.

61. The private banking industry in Singapore has also grown significantly over the past decade, as indicated above, boosted by the rising wealth in Asia. Private banking is traditionally associated with higher ML risk factors due to the more high-value and bespoke services that can be offered, including to wealthy PEPs.

62. Money-changers and remittance agents are cash-intensive sectors and have been identified by Singapore as having characteristics that may heighten the ML/TF risk. In addition to the inherent risks in this sector, Singapore's peculiar position (e.g. a host of a high number of migrant workers from neighbouring countries with poor formal banking systems; and a hub of international trade and travellers) contributes to higher ML/TF risks. The NRA also acknowledges that smaller remittance agents may not have adequate resources and systems to put in place additional risk mitigation measures. The implementation of the AML/CFT obligations and control measures in these sub-sectors is not as robust as in banks.

63. With the increased use of online payments, internet-based stored value facility (SVF) holders have also been identified in the NRA as one of the higher risk sub-sectors. Singapore has identified that the cross-border nature of most transactions and the challenges faced by internet-based SVF holders in verifying customer identities are clear red flags. Consequently, Singapore enhanced the scope of its AML/CFT requirements to cover internet-based SVFs that do not demonstrate sufficient low risk characteristics. Nevertheless, the AML/CFT regulations, supervisory regime and control measures in this sub-sector are relatively nascent, and global best practices and standards are still being developed.

64. The DNFBP sectors are relatively small in terms of the number and financial volume of transactions in comparison to the financial sector. Given that, aside from trust companies, casinos and lawyers, AML/CFT measures in the remaining DNFBP sectors are recent and their implementation is not as strong as those in the financial sector, the DNFBP sector presents a potential ML/TF risk. With the exception of accountants, there are legally enforceable AML/CFT

[24] This refers to off-market securities transfers.

[25] This refers to transaction volume.

[26] This refers to inward and outward remittances.

preventive measures for all categories of DNFBPs. Preventive measures for accountants are set out in the ISCA Ethics Pronouncement-200 (EP-200). While the document is issued by a competent authority (the ISCA) and uses mandatory language, there is no clear link to proportionate and dissuasive sanctions in case of non-compliance with these AML/CFT requirements. While Singapore refers to disciplinary sanctions in s.53 of the Accountants Act, these sanctions relate to breach of professional standards of conduct and are not clearly linked to AML/CFT requirements, including on CDD. The following table illustrates an overview of the DNFBPs in Singapore, followed by a brief description of three DNFBP sectors which presents higher risks than others.

Table 2. **Number and Size of DNFBPs**

Type of DNFBP entities	Number of Entities (as of 31 Dec 2014)	Size of Sector (in billions of SDG)
Casinos	2[1]	Gross gaming revenue (2013): 7.6[2]
Pawnbrokers	227	Value of outstanding loans (2014): 5.4
Precious Stones and Metals Dealers (PSMD)	Over 800[3]	Operating receipts of jewellery retailers (2013): 2.5
Company Service Providers (CSPs)	2 687[4]	-
Licensed Trust Companies	54	Total Assets Under Management: 240
Real Estate Agents	licensed estate agents: 1 369 registered salespersons: 30 830	Value of private property transactions (2014): 35[5]
Lawyers	Lawyers: Over 5 000 Law firms: Over 800	-
Professional Accountants (of which: Public Accountants)	Over 28 000 (1 051)	-

Table Notes:

[1] The number of casinos is limited to 2 for a period of 10 years from 1 March 2007 by the Casino Control Act (Article 41(1)).

[2] USD 6 billion.

[3] There were 856 Jewellery Retailers in 2013 - Singapore Department of Statistics (2016), Services Survey Series – Retail Trade 2013

[4] As of 15 May 2015, when the regulations for CSPs took effect.

[5] Of which SGD 20b is for residential properties and SGD 15b is for non-residential properties.

65. Company service providers (CSPs) have been identified by Singapore as a sector with a higher level of risk owing to the companies that CSPs help to incorporate for international customers. While CSPs generally do not handle large amounts of cash, Singapore recognises the risk that the companies that they help to incorporate may be abused by criminals to set up complex and opaque structures for illicit purposes. The regulatory framework for CSPs was strengthened with the introduction of AML/CFT requirements in May 2015 to mitigate the ML/TF risks.

66. The casino sector is relatively new in Singapore. Only two licensed casinos were established in 2010, before which casinos were not allowed. The gross gaming revenue in 2013 was about USD 6 billion, ranking Singapore third after Macau and Las Vegas. The casino sector's cash-intensive business exposes it to a higher level of inherent risk.

1

67. Singapore identified that the fast-growing pawnbrokers sector is another risk area where controls can be improved. Transactions in this sector are mainly cash-based and gold items make up 90% of all pledges. Although this sector is domestically focused and the individual loan amounts are generally small, debt repayment using illicit funds and pawning of stolen goods are channels of risk. The Insolvency and Public Trustee's Office (IPTO) introduced an AML/CFT regime to this sector in 2015.

Overview of preventive measures

68. Singapore's AML/CFT regime has undergone significant reform since the last assessment in 2008. The MAS (Amendment) Act was adopted and entered into force in June 2015, and the MAS Notices and Directives were recently amended (reflecting changes made to the FATF Standards in 2012.) Meanwhile, the Moneylenders (Prevention of Money Laundering and Financing of Terrorism) Rules 2009 ("PMFTR") have also been recently amended.[27] The MAS Notices and Directives, and the PMFTR for moneylenders that impose obligations on financial institutions use almost identical language to that used by the FATF. This means that, overall, preventative measures for the financial sector generally meet a high level of technical compliance with the detailed provisions of the FATF Recommendations.

69. Within the DNFBP sector, Singapore at the time of the 3rd round mutual evaluation applied AML/CFT preventive measures only to trust companies (that are regulated as financial institutions) and lawyers. Since that time, AML/CFT requirements were extended to casinos when they were opened in 2010 (amended in June 2015), real estate agents (November 2013; updated February and September 2015), accountants (November 2014 but these are not enforceable), CSPs (May 2015), and pawnbrokers (April 2015). Nevertheless, a large portion of Precious Stones and Metals Dealers (PSMDs) are still not subject to the full range of AML/CFT obligations as required by the FATF Recommendations, including the Singapore Precious Metals Exchange (SGPMX). The late introduction of AML/CFT measures for the various components of the DNFBP sector (this is a FATF requirement since 2003) has its impact on this assessment, most notably on IO.3 and IO.4.

70. In addition, under the Corruption, Drug Trafficking and other Serious Crimes (Confiscation of Benefits) Act (CDSA) of 2000, any person, including financial institutions and DNFBPs, is obliged to file an STR to the STRO in the CAD in the course of trade, profession, business or employment when he/she suspects any property may constitute proceeds of drug dealing or criminal conduct, including TF.

Risk-based exemptions or extensions of preventative measures

71. Singapore has applied AML/CFT exemptions in several areas identified to be low risk. In particular, MAS assessed that the widely-used physical SVF holders, given their usage and form, present a low risk for ML and TF. However, internet-based SVF have been identified in the NRA as being higher risk. Initially, all SVF holders which issued SVFs with load limits of less than SGD 1 000 (approx. EUR 659 / USD 702) were exempted from AML/CFT measures. On 30 November 2015, amendments to the MAS Notice PSOA-N02 came into force and additional conditions for SVFs to be exempted from AML/CFT measures were introduced. On that basis, 58 out of a total of 69 SVF

[27] The amendments to the PMFTR took effect on 1 September 2015.

holders are currently exempted from preventive AML/CFT measures, with the exception of record keeping and suspicious transaction reporting requirements under the CDSA and the TSOFA. All 6 internet-based SVF holders are now subject to the full range of AML/CFT requirements.

72. MAS has also exempted FIs from the requirement to make inquiries into beneficial ownership in specific lower risk situations. These exemptions, which relate to particular types of financial institutions and activities, are consistent with the example in footnote 31 to c.10.10 of the FATF Methodology.

73. The NRA identified the Singapore Freeport, which is a storage and logistics facility for high value goods, as an emerging risk to consider. Following further analysis, Singapore placed AML/CFT obligations (e.g. CDD, record-keeping) on Zero GST warehouse licensees in Singapore on 1 October 2015, including those located within the Singapore Freeport. Such obligations may be justified by the inherent risks posed by the high value goods held in the facility, and appear to be in line with Singapore's assessment that the Singapore Freeport presents a medium-high ML/TF risk. The relevant authorities however did not demonstrate a comprehensive understanding of what activities were being undertaken in the Singapore Freeport, which raised concerns with the assessors.

Overview of legal persons and arrangements

i. Legal persons

74. The types of legal persons that can be established or created in Singapore are: local companies (including public companies) foreign companies, and limited liability partnerships (LLPs). Other business entities exist in Singapore (general partnerships and limited partnerships, and sole proprietorships) but they are not legal persons.

75. The Accounting and Corporate Regulatory Authority (ACRA) is the central registration authority in Singapore for business entities. The process for the creation of legal persons and for obtaining and recording basic ownership information is set out in the Companies Act and the Limited Liability Partnership Act. Under the Companies Act, anyone wishing to set up a company must provide: the company name, address of the registered office, memorandum and articles of association, as well as the names and details of directors, managers, secretaries and auditors. The information held by ACRA in relation to companies and LLPs is available to the public for a small fee, depending on the information purchased. Government agencies can obtain the same information free of charge.

76. Singapore does not have a central beneficial ownership (BO) information registry, which is not an FATF requirement but one of the options to comply with Recommendation 24. However, under the Companies Act, public and private companies are required to maintain a shareholders' register containing the name and address of each shareholder; date shares were acquired; number and classes of shares held. Listed companies are required to keep a register of substantial shareholders at the registered office. BO information of legal persons can also be obtained through other means, namely through CSPs and FIs. The table below shows the number of legal persons registered with ACRA between 2010 and 2014.

Table 3. **Legal Persons registered with ACRA**

	2010	2011	2012	2013	2014
Local Companies (public and private)	216 566	229 371	242 604	261 047	281 982
Foreign Companies	1 776	1 842	1 947	2 011	2 012
Limited Liability Partnerships	8 173	9 607	10 720	12 024	13 971

77. Singapore authorities advise that the majority of legal persons in Singapore are registered through Company Service Providers (CSPs) and CSPs file the majority of documents with ACRA to register legal persons. CSPs have to register with ACRA as filing agents and employ qualified individuals and must use their professional filing numbers issued by ACRA to access ACRA's electronic transaction system. As of May 2015 there were about 2 600 CSPs registered with ACRA (pursuant to the ACRA Act and ACRA (Filing Agents and Qualified Individuals) Regulations 2015 ("ACRA Regulations").

78. Companies and LLPs must comply with the requirement to file annual returns and annual declarations respectively. The annual return for companies updates ACRA on any changes to basic company information including names and addresses of company directors and the registered office. ACRA may undertake enforcement action against companies and LLPs that fail to file annual returns/declarations. Penalties for non-compliance include fines when breaches are addressed or court enforcement action when they are not.

ii. Legal arrangements

79. Trusts in Singapore are governed by both common law and statute. Unlike companies and other business entities, there is no central or other registry for the registration of trusts. There is no estimate of the total number of trusts existing in Singapore.

80. Complex legal arrangements including trusts are usually established through professional intermediaries, such as licensed trust companies (LTCs), lawyers, or accountants. There are no general obligations in Singapore for all trustees to keep accurate and up to date information in relation to trusts; however professional trustees including LTCs, lawyers and accountants, when acting in that capacity are regulated for AML/CFT purposes (by MAS, the Law Society of Singapore and ACRA respectively).

81. In particular, under MAS Notice TCA-N03, LTCs are required to conduct CDD on "trust relevant parties", which includes the settlor, the beneficiaries, protector and the trustee. Lawyers are required, under the Legal Profession (PMLFT) Rules Part 2, to conduct CDD in relation to their clients and where the client is a legal arrangement in relation to trust relevant parties, including any beneficiaries - CDD includes verification of identity. While accountants are also required to conduct CDD in relation to their clients who are trustees, including beneficiaries (EP-200 s.4.12), these requirements do not qualify as law or enforceable means, as explained above. The Singaporean competent authorities, including law enforcement (CAD, Corrupt Practices Investigation Bureau), STRO and tax authorities, have powers to obtain information relating to trustees, beneficiaries, trustee residence and assets managed under a trust.

82. As at 31 December 2014, there were 54 licensed trust companies (LTCs) in Singapore, over 5 000 lawyers, 1 051 public accountants, and over 28 000 professional accountants (regulated by the Institute of Singapore Chartered Accountants (ISCA)).

iii. International context for legal persons and arrangements

83. Legal persons, including foreign companies registered in Singapore, are vulnerable to criminal misuse. Since 2012, the CAD has observed an increase in the number of ML cases involving shell companies established by non-residents based overseas.

84. In addition, Singapore is rapidly emerging as a premier jurisdiction for establishing and operating various types of trusts. Singapore trust law permits the operation of foreign trusts, which under specified conditions qualify for tax benefits, including tax exemption on a wide range of trust income as well as exemption from tax on the distributions to beneficiaries of such trusts (under section 13G of the Singapore Income Tax Act, chapter 134). Singapore trust law also permits the formation of domestic trusts governed by the laws of a foreign country.

Overview of supervisory arrangements

85. The Monetary Authority of Singapore (MAS) is the consolidated financial sector regulator that supervises the following financial institutions for AML/CFT: banks, merchant banks, finance companies, direct life insurers, money-changers, remittance agents, financial advisers, capital markets intermediaries, SVF holders, non-bank credit card issuers, the central depository (CDP) and financial holding companies.

86. MAS has a broad range of powers to supervise and monitor compliance of FIs with AML/CFT requirements, including powers of off-site surveillance, auditing and on-site visits and inspections. The various classes of FIs are subject to similar obligations on CDD, record keeping, suspicious transaction reporting, internal control policies and procedures, the need for management-level compliance function, audit and staff training in AML/CFT measures. IPTO also has powers to supervise money lenders.

87. Each DNFBP sector is regulated for AML/CFT by its licensing/registration authority or self-regulatory body, with the exception of PSMDs other than pawnbrokers, which are only subject to a cash reporting regime. The table below shows the authorities responsible for AML/CFT supervision of the various DNFBPs.

Table 4. **DNFBP Supervisors and Self-regulatory bodies**

Type of DNFBP	Supervisor/ SRB	Applicable Law/ regulation
Casinos	Casino Regulatory Authority (CRA)	• Casino Control Act (CCA) • Casino Control (Prevention of Money Laundering and Terrorism Financing) Regulations 2009 • Internal Controls Code (Prevention of Money Laundering and Terrorism Financing) • Internal Controls Code (Treasury) • CDSA • TSOFA
Pawnbrokers	Insolvency & Public Trustee's Office (IPTO)	• Pawnbrokers Act 2015 • Pawnbrokers Rules 2015 • CDSA (including section 48H-48K on cash transaction reporting) • Corruption, Drug Trafficking and other Serious Crimes (Cash Transaction Reports) Regulations 2014 • TSOFA
Other Precious Stones and Metals Dealers	[The cash transaction reporting regime is enforced by CAD]	• CDSA (including section 48H-48K on cash transaction reporting) • Corruption, Drug Trafficking and other Serious Crimes (Cash Transaction Reports) Regulations 2014 • TSOFA
Company Service Providers	The Accounting and Corporate Regulatory Authority (ACRA)	• ACRA Act • ACRA (Filing Agents and Qualified Individuals) Regulations 2015 • CDSA • TSOFA
Licensed Trust Companies	The Monetary Authority of Singapore (MAS)	• MAS Act • Trust Companies Act • MAS Notice TCA-N03 • CDSA • TSOFA
Real Estate Agents	Council for Estate Agencies (CEA)	• CEA Practice Circular on the Prevention of Money Laundering and Countering the Financing of Terrorism • CDSA • TSOFA
Lawyers	The Law Society of Singapore (MinLaw, Law Society)	• Legal Profession Act • Legal Profession (Prevention of Money Laundering and Financing of Terrorism) Rules 2015 • Prevention of Money Laundering and Financing of Terrorism Practice Direction (PDR 2015 Paragraph 1) • CDSA • TSOFA

Type of DNFBP	Supervisor/ SRB	Applicable Law/ regulation
Public Accountants	The Accounting and Corporate Regulatory Authority (ACRA)	• Accountants Act • Accountants (Public Accountants) Rules • Ethics Pronouncement 200, AML/CFT Requirements and Guidelines for Professional Accountants in Singapore ("EP200") • ISCA (Proceedings of Council) Rules • ISCA Membership and Fees Rules • CDSA • TSOFA
Professional Accountants	Institute of Singapore Chartered Accountants (ISCA)	• EP200 • ISCA (Proceedings of Council) Rules • ISCA Membership and Fees Rules • CDSA • SOFA

International Cooperation

88. International cooperation is an important issue in the context of AML/CFT in Singapore. Singapore is exposed to ML risks from foreign criminals seeking to launder the proceeds of foreign offences in the country. Singapore's status as a major global financial centre and international transit hub makes it vulnerable as a transit point for illicit proceeds through South East Asia and other foreign jurisdictions. Singapore employs both formal and informal means of international cooperation, taking into account the nature of offences involved and the requirements of speed and efficiency. The top ten jurisdictions that Singapore cooperates most regularly with are the U.S, China; Hong Kong, China; Malaysia, United Kingdom, India, Australia, France, Indonesia and Canada.

89. The legal framework for MLA is set out in the Mutual Assistance in Criminal Matters Act (MACMA). The Central Authority for mutual legal assistance and extradition is the International Affairs Department (IAD) of the Attorney-General's Chambers (AGC).

Terrorist Financing and Financing of Proliferation

90. Between December 2001 and June 2015, Singapore dealt with 93 persons under the Internal Security Act (ISA) for involvement in terrorism-related activities. Of these 93 persons, 17 were involved in terrorism cases which included elements of TF activities (all prior to 2008). All 17 persons had links to Jemaah Islamiyah (JI) and Moro Islamic Liberation Front (MILF), and had made financial contributions towards the JI and/or MILF, mostly through their personal donations and funds solicited from their associates. The amounts contributed were not fixed and while some made one-off contributions, others contributed more regularly. In some cases, the individuals handed over donations and funds raised to foreign JI/MILF leaders and members for activities overseas, e.g. funding of MILF to fight against the Philippines' government and funding of JI/MILF-run madrasahs in the region. Some of the individuals were also involved in and contributed funds towards join business ventures with the JI/MILF.

1

91. Between 2008 and 2014, Singapore advises that there have been 413 TF investigations undertaken by CAD in support of ISD investigations but Singapore has yet to detect any confirmed case resulting in prosecution.

92. In the same period, between 2008 and 2014 up to 780 terrorism-related leads were generated from ISD and other Singaporean agencies, and from foreign partners. These covered all aspects of terrorism-related activities including operational, financial, ideological and other leads. The leads came from different sources including reports from the public, to Police, directly to ISD, and referrals from other LEAs, STRS, leads generated from ISD's CT investigations, intelligence shared by local sources as well as foreign intelligence agencies. Of these 780 leads, a total of 87 TF inquiries were undertaken by ISD, however these "inquiries" related solely to false positive name matches on STRs. There are no real investigations beyond these inquiries.

93. Between January 2014 and June 2015, Singapore detected and investigated over 10 Singaporeans who had been radicalised by ISIL propaganda. One individual was subsequently detained and another was issued with a Restriction Order under the ISA. Both had been radicalised by online ISIL propaganda with intention to travel to Syria to fight with ISIL. The Singaporean who was detained had been prepared to carry out terrorist attacks in Singapore. There is no evidence that financial investigations were undertaken with respect to these cases.

94. Singapore acknowledges that there is a large foreign community in Singapore which could encourage foreign terrorist groups to use Singapore as a base for terrorism fund raising amongst their own nationals. Since June 2015, three individuals had been detained under the ISA after investigations showed that they had been radicalised by the ISIL propaganda and wanted to join and fight with ISIL. Authorities are also aware that Singapore continues to be a potential target for terrorism.

CHAPTER 2. NATIONAL AML/CFT POLICIES AND COORDINATION

Key Findings and Recommended Actions

Key Findings

1. Singapore's AML/CFT coordination is highly sophisticated and inclusive of all relevant competent authorities. Driven by the AML/CFT Steering Committee and the Inter-Agency Committee, the coordination mechanism in Singapore is a valuable tool in AML/CFT policy development. This proved to be true in the development of the National Risk Assessment (NRA) and the cooperation and organisation associated with this mutual evaluation exercise.
2. Singapore consults with private sector entities in policy development and in initiatives such as the NRA process. This consultative process has ensured a broad and uniform understanding of the government's initiatives and concerns with respect to ML/TF issues. However more needs to be done to ensure that private sector understanding of risk is further strengthened.
3. Singapore has a strong domestic culture of law and order, and crimes committed in Singapore are investigated and prosecuted, and often result in dissuasive penalties. Singapore has a reasonable understanding of its ML/TF risks. Nevertheless, this understanding is shaped mainly by visible factors such as ML/TF caseloads, feedback from foreign counterparts, international reports, reported transactions and international requests as indicators of its overall ML/TF risks. Legal persons and arrangements have yet to be comprehensively assessed limiting the scope of Singapore's understanding of risk.
4. Taking into consideration Singapore's position one of the world's largest financial centres, moderate gaps remain in Singapore's understanding of the nexuses between transnational threats and vulnerabilities in the system and how transnational risks will materialise in a Singapore context. Singapore has taken steps to mitigate the transnational risks that it has identified (such as from shell companies, trade based money laundering, as well as laundering of proceeds of corruption and tax evasion). Still, some other forms of ML and TF relevant to Singapore's context should have been given greater attention.

Recommended Actions

1. The next round of Singapore's NRA should better articulate the nexus between key threats and vulnerabilities to promote a deeper understanding of how the ML/TF risks faced by Singapore will materialise in Singapore's context. This analysis should take into consideration Singapore's geographic location and role in the international economy.
2. The next NRA should better anticipate dynamic and hidden risk, and include comprehensive risk assessments of the different types of legal persons and arrangements, especially those associated with transnational activities such as trade, investment, and wealth management.
3. Singapore should consider setting out a formal national strategy following the next NRA, in order to coordinate prioritisation of key risks through prevention, avoidance and mitigation measures.
4. Singapore should take steps to improve the level of private sector awareness of the results of the national assessments of ML/TF.

95. The relevant Immediate Outcome considered and assessed in this chapter is IO1. The recommendations relevant for the assessment of effectiveness under this section are R1-2.

Immediate Outcome 1 (Risk, Policy and Coordination)

Overview of the risk assessment

96. Singapore conducted a National Risk Assessment (NRA) exercise during 2012-13, based on a modified version of the Asia/Pacific Group on Money Laundering (APG) and World Bank's Strategic Implementation Planning (SIP) Planning Framework. Singapore was one of the first countries to produce its formal risk assessment document, which was published in January 2014. Fifteen government agencies were involved in the process and private sector consultation was conducted. At a high level, the NRA report acknowledges that Singapore's openness as an international transportation hub and financial centre exposes it to inherent cross-border ML/TF risks. Analysis was conducted on 14 financial sub-sectors and 8 non-financial sectors.

97. The NRA concluded that the sectors most vulnerable to ML and TF are those that are internationally-oriented and cash-intensive. The assessment also concluded that AML/CFT measures have generally mitigated the ML/TF risks. Many higher risk sectors, such as banks and casinos, already have AML/CFT controls in place. Remittance agents (RAs), money-changers, internet-based SVF holders, CSPs and pawnbrokers were identified as sectors where AML/CFT controls were relatively less robust.

98. A threat assessment was conducted considering domestic offences and 30 predicate offences in 136 foreign jurisdictions. The threat assessment used an approach of considering determining factors[28] and validating factors.[29] Unlicensed Money Lending (UML) was identified as one of the most prevalent domestic predicate offences for ML. The assessment identified overseas cheating (fraud) and corruption as the major predicate offences for transnational ML. Assessment of the TF threat considered Singapore's investigations and TF-related intelligence or information received, including from foreign counterparts. The assessment found that since the disruption of the Jemaah Islamiyah network, there has been no evidence of TF being committed in Singapore since 2008.

99. Higher risk countries are not listed in the NRA report. Authorities indicated that they applied the same determining factors used in the assessment of overseas predicate threats, while the validation factors were modified to take into account factors such as whether the jurisdiction is a neighbouring country. However, the prominence of requests for international cooperation and previous investigations potentially leads to identifying countries with strong international cooperation with Singapore as being higher risk. Assessors indeed noted correlation between high threat ratings and higher capacity countries. Nevertheless, Singapore has continued to refine this assessment and assessors noted that in the most recent assessment the threat rating for some lower capacity countries was elevated.

[28] Incidence of predicate offences and propensity to laundering in relation to domestic offences; and MLA, LEA and FIU requests and STR referred to domestic LEAs in relation to foreign predicates.

[29] Number of ML investigations, prosecutions and convictions, amount of proceeds seized, indication of threat from international reports, and consequences in relation to both domestic and foreign predicates; as well as estimated losses in relation to domestic offences; and amount of proceeds confiscated and other qualitative factors including information exchanges with foreign counterparts.

Overview of coordination arrangements

100. The main national AML/CFT policy coordination mechanism is the AML/CFT Steering Committee. The Committee is led by the Permanent Secretaries of MHA and MOF and the Managing Director of MAS.[30] Working level coordination to implement policy is managed through the Inter-Agency Committee comprising AML/CFT agencies, including policy makers, the FIU, law enforcement authorities, supervisors, customs and tax authorities, intelligence services, and the Attorney-General's Chambers.

Understanding of risk

101. The NRA process has established a basis for the private sector and government agencies to understand Singapore's ML/TF risks. The NRA report is an accurate reflection of Singapore's understanding of its ML/TF risks and in the assessment team's view it encompasses Singapore's national understanding of risk. The primary purpose of the NRA report is to highlight key risks areas to the private sector that require vigilance and articulate residual risks taking into account control measures in place. As the NRA document is public, the scope of the document and the degree of detail of analysis is limited. Nonetheless, Singapore describes the NRA as being comprehensive and all agencies and private sector representatives consistently reported that it is all-inclusive and accurate representation of Singapore's ML and TF risks. The NRA is only one part of what this mutual evaluation looked at, because this exercise assesses Singapore's broader risk understanding. Singapore officials report that a more comprehensive analysis was conducted, underpinning the assessment. Other documents describing reviews of risk areas were produced to demonstrate risk understanding to assessors. However, it was not clear to the assessors how this analysis had fed into national processes such as the NRA exercise, and therefore national risk understanding.

102. Singapore has demonstrated risk understandings outside of the information presented in the NRA report although there remain moderate gaps in Singapore's understanding of risk particularly in regards to transnational threats. There has been analysis of transnational threats, in the NRA and STRO's strategic products. However, this analysis could be further improved by placing more weight on methods associated with main threats, especially transnational ML of grand corruption, tax and other predicates proceeds, and ML by sophisticated international networks associated with these predicates. For example, although the NRA identifies past instances of ML of proceeds of overseas corruption by self-launderers and close associates, Singapore's understanding does not draw out the nexus between international exposure and the propensity for proceeds for grand corruption to be laundered through legal structures. Similarly, although relatively high vulnerability was found in regards to property development, the potential nexus between that sector and ML of grand corruption has not been tested.

103. Since the NRA report was published, Singapore officials have made considerable efforts to leverage overseas experiences of TBML. Resulting guidance was issued to banks in 2015 highlighting red-flags for trade financing associated with ML in merchandise trade based ML based on international experience. However, risks relating to the types of TBML that are likely to materialise in Singapore are yet to be well elaborated in the NRA. Additionally, assessors found that Customs in particular had limited understanding of the TBML risks and that Customs' guidance is high level and

[30] In Singapore's context, the Permanent Secretary of MHA and MOF, and the Managing Director of MAS, are the heads of their respective agencies.

does not highlight specific risks to Singapore (although red flag indicators were issued relevant to TBML). Additionally, no assessment has been conducted on trade in services vulnerability to ML and tax evasion, which is likely to be high risk given Singapore's role as a financial hub, the ease of establishing companies, exposure to international laundering and the risks from ACRA resourcing identified in the NRA analysis.

104. MAS initiated a tax review by financial institutions to identify assets held in institutions, reviewed red flags used to detect tax crimes, and actively followed up with institutions to track the fund flows. This process led to guidance on tax crimes, related ML and red flags. However, this review stopped short of a comprehensive risk assessment as the review did not analyse vulnerabilities likely to be abused by transnational tax crime. Additionally DNFBPs were not covered by the review sectors, and therefore CSPs which are likely to be relevant to tax offending were excluded.

105. Not all forms of legal persons and arrangements, and their adverse relationship to transnational threats, have been assessed. With respect to legal persons in particular, an assessment of public companies, foreign companies and limited liability partnerships was not included in the NRA report. As for private or closely held companies Singapore assessed only shell companies. Although some risks associated with legal persons and arrangements are discussed in the NRA report (shell companies abused by transnational cheating), risks associated with other forms were only examined in a departmental analysis which was presented to the assessors on-site. The results of the examination were also not shared with other departments nor were they subject to consultation with the private sector during the NRA process. The documentation produced for assessors on the internal methodology used to assess legal persons and arrangements indicated that the assessment was based on previous identified incidences, media reporting and discussions with LEAs and not on current, operative factors and evidence. The analysis appears to have drawn the conclusion that legal entities providing professional services are inherently lower risk, overlooking the risk of ML through services, which is associated with significant ML and tax predicate threats active in the international environment.

106. The focus of risks relating to legal persons and arrangements in the NRA is on the risk of the CSP and TSP sector rather than legal persons/arrangements themselves or the nexus between legal person/arrangement abuse and the significant ML and tax predicate threats active in the international environment (with the exception of shell companies used in cheating cases). As a result, there is no consistent and coherent understanding within the government and the private sector of the inherent and residual risks associated with the various forms of legal persons and arrangements; compounded by these risks not being included in the NRA report except as relates to ML of cheating and the use of TSPs to form express trusts. Risks associated with gatekeeper professionals (both as a vulnerability and as a threat) have only received a cursory high level of analysis, which seems to have primarily drawn on detected incidences of abuse and the sectors' own perception, risking confirmation bias.

107. On the positive side, where the NRA process has addressed or identified higher threats and vulnerabilities a consistent national understanding has emerged. The risk of Singapore money mules being exploited in transnational laundering of cheating is well understood by Singapore agencies and financial institutions. Similarly the nexus between this threat and vulnerabilities that allow shell companies to be abused is generally well understood and accepted.

108. Singapore's understanding of threat from higher risk jurisdictions is derived from the same assessment process as the foreign threat assessment, using the same determining factors although the validation factors were modified to take into account factors such as whether the jurisdiction is a neighbouring country. This approach risks confirmation bias towards higher capacity and close partners by focusing too much on visible LEA relationships. At the time of the NRA report's publication in 2014, Singapore only considered the US; UK; Hong Kong, China and countries on the FATF blacklist (Iran and DPRK) to be high risk. This seems surprising in light of Singapore's regional position as a financial centre and wealth management hub.

109. In 2015, CAD updated its transnational threat assessment resulting in the threat assessment for some major regional proceeds generating jurisdictions to be elevated. In addition, the understanding derived from international reports led to the assessment of several facilitation jurisdictions being elevated. Singapore has yet to articulate how the threat from transnational threats relating to illicit flows to/from high risk jurisdictions are likely to materialise. As such it is not clear how an understanding of methods likely to be used by all transnational threats is to be associated with identified high threat jurisdictions. Where Singapore has experience of networks that facilitate transnational threats involving smaller values in individual cases, it has used that experience to develop understanding. CPIB has used its experience of criminal networks moving proceeds of corruption in cash form through foreign exchange and money remittance, although this understanding was not communicated in the NRA report. However, there seems to be a growing understanding of grand corruption risks as was shown in two cases of corruption – including grand corruption - provided by Singapore. Singapore is to be commended for these actions, and encouraged to continue to pro-actively target foreign grand corruption cases in Singapore, where appropriate. Similarly, although Singapore has sought to understand overseas experience of transnational threats, Singapore should seek to strengthen its understanding of global ML/TF networks associated with grand corruption and other large scale illicit flows that threaten Singapore and the methods that they are likely to use in Singapore.

110. Singapore in its NRA identifies domestic source TF as a low to medium threat and foreign source TF as a medium threat. While Singapore has a Strategic understanding of TF risk to a certain extent, in particular foreign sources of funding, they should further focus on factors such as geographical factors, level and extent of terrorism activity in the region and inherent risks such as Singapore being a financial, transport and people hub. The private sector's tactical level understanding of 'risk' is too focused on screening databases and adverse news rather than TF risk factors.

111. Some reporting entities indicated that they consider the TF risk profile higher than identified in the NRA report, and that the rise of ISIL affected the medium rating. Several other assessments have considered aspects of ML and TF risk not covered by the NRA report, although these appear more as policy documents or descriptions of sectors that discussed mitigation measures than risk assessments.

112. Since the NRA report was published, authorities have continued to seek greater understanding of risk. In particular, Singapore has sought to understand and mitigate risk areas identified by the international community. This has led to CAD engagement with international partners to seek evidence of trade-based money laundering. Although this has led to one investigation, low detection of this activity by other jurisdictions has impacted Singapore's opportunity to improve its overall level of understanding through this channel.

National AML/CFT policies and activities to address identified risks

113. Singapore has established an AML/CFT Steering Committee as the main national whole-of-government AML/CFT policy coordination mechanism. This Steering Committee presently involves over 20 government agencies, and is chaired by government officials of the highest level. Major policy changes that require political endorsement, and/or legislative changes, are tabled at the Cabinet meetings when necessary. The Steering Committee has made a high level policy statement that Singapore will devote resources to mitigating its identified ML/TF risks.

114. A supporting IAC structure that comprises the same government agencies coordinates the implementation of AML/CFT efforts at a working level, as well as providing a platform for agencies to share information such as emerging ML/TF financing of proliferation threats and trends, FATF typologies, best practices, and other related developments. The meetings also facilitate AML/CFT policy coordination and implementation across agencies as guided by the AML/CFT Steering Committee.

i. National policies to mitigate identified vulnerabilities

115. Pursuant to this policy objective, Singapore has taken action to mitigate vulnerabilities in sectors identified in the NRA. At a national level, legislative measures have been introduced to mitigate identified vulnerabilities in the pawnbroker and stored value facilities (SVF) sectors to introduce new AML/CFT controls including CDD and transaction reporting requirements. Singapore also conducted outreach to foreign partners in response to its identified tax crimes and TBML vulnerabilities. Legislative changes were also introduced to mitigate the identified vulnerability of company service providers to exploitation to create shell companies. Other vulnerabilities have been mitigated at the agency level, for example vulnerabilities in the banking sector and money changers and remittance agents (MCRAs).

ii. National policy to mitigate identified threats

116. A matrix has been introduced to inform the level of mitigation based on the level of threat, with a higher level of policy responses to greater threats and greater investigative resources dedicated to greater threats. Pursuant to this approach additional staff have been dedicated to CAD and CPIB to counter the transnational threats relating to corruption, money mules and cheating identified in the NRA. STRO resources have also been dedicated to identifying STRs relevant to identified threats, such as UML and money mules (see IOs 6&7).

iii. Use of assessment of risk in exemptions

117. Singapore has applied AML/CFT exemptions in areas identified to be low risk. Singapore drew a distinction between physical SVFs, which were assessed as lower risk, and internet-based SVFs which were assessed as higher risk. As a result, an exemption was granted so that issuers of physical SVF with load limits of less than SGD 1 000 (EUR 659 / USD 702) are exempted from certain AML/CFT measures, such as CDD. Exemptions have also been granted from the requirement to make inquiries into beneficial ownership in identified low risk situations such as dealing with entities listed on the Singapore exchange.

iv. National measures to treat risk

118. Singapore has made a high level policy statement which guides its AML/CFT regulation, surveillance, supervision and enforcement efforts. Pursuant to this statement, relevant government agencies have strengthened the legislative and supervisory framework in relation to remittance agents, money-changers, internet-based stored value facility holders (SVF), company service providers (CSPs) and pawnbrokers as the NRA identified these as sectors where AML/CFT controls were relatively less robust as compared to banks.

119. Singapore has not attempted to set out a formal national strategy following the national risk assessment, in order to coordinate prioritization of key risk through prevention, avoidance, mitigation measures. Measures have been implemented to further strengthen what the NRA rated as already strong control measures to mitigate identified medium risk in casinos. By contrast, while activity to raise awareness in the industry has been undertaken, measures were not implemented to strengthen weaker controls in real estate and property developers which the NRA analysis identified as medium and medium high risks respectively.

Consistency of objectives and activities of authorities and SRBs with the evolving national AML/CFT policies and ML/TF risks identified

120. Operational activities of authorities are targeted towards identified risk. MAS dedicates supervisory resources by risk. This is done both at a sector level and by maintaining an assessment for each reporting entity, which is updated yearly. IPTO targets its supervisory activity on the basis of risk relating to the volumes/monetary values of loans.

121. Officials reported that a threat-based policy approach is used to determine resources to counter ML/TF threats. This ranges from considering agency coordination using existing resources to counter low threats to Inter-Agency Committee intervention in to counter high threats, which may include recommending legislative change and additional resource allocation to the Steering Committee.

122. Pursuant to this approach and the Policy Statement, the MAS Act was amended to facilitate MAS international cooperation in recognition of the high transnational threats identified in the NRA. MAS also issued guidance on tax offences to private banks and on trade finance pursuant to assessment of vulnerabilities and these threats being identified as being of interest identified in the NRA.

123. Officials reported a similar threat based approach to LEA operational activity. At the low threat end this approach involves using existing resources and responding to foreign request to target ML/TF. In relation to higher threats this approach includes proactive engagement of overseas partners to identify incidences and links to Singapore and increasing outreach and guidance to industry. Pursuant to this approach CAD has engaged overseas partners to identify TBML linked to Singapore and used this engagement to generate red flag indicators, which according to the advice Singapore provided on its approach goes somewhat beyond the NRA report finding that TBML was medium risk.

Cooperation and coordination on the development and implementation of policies and activities to combat ML/TF

124. Singapore has highly effective coordination structures in place at all levels and processes to coordinate between government and SRBs. Authorities, SRBs and financial institutions are able to coordinate on operational matters using, the Interagency Group mechanism, well established SOPs and well developed networks of liaison officers. At a strategic level, agencies have used the Steering Group and Interagency Group mechanisms to facilitate projects such as the NRA and to make a joint government policy statement that was published on the three main agencies' websites. STRO has also started producing strategic reports to inform partners' operations (see IO6).

125. The IAC also coordinates proliferation financing issues, such as the dissemination of guidance, and will make recommendations to the AML/CFT Steering Committee on de-listing requests should they arise. The Chinpo case, for which the trial commenced in August 2015, involving shipment of arms from Cuba to DPRK demonstrated the effectiveness of Singapore's coordination structures to combat proliferation financing should it be detected. A cross-government investigation was conducted by CAD, AGC, MFA and MAS leading to an AGC prosecution. Concurrent activity was undertaken to inform financial institutions leading to STRs, closed accounts and regulatory action by MAS.

Awareness of the financial sector, DNFBPs and others to the results of AML/CFT assessments

126. Prior to the NRA, the authorities conducted outreach to the private sector for fact-finding and to obtain early views on risk and what NRA outputs would be useful for industry stakeholders. During the NRA, authorities conducted surveys to collect further information from the private sector, and to sensitize them to the ongoing exercise. Private sector focus group sessions were organised to validate NRA findings. Post-NRA, there were continued supervisory engagements with the private sector to ensure that they understand their existing risks and are apprised of emerging ones.

127. Private sector entities commented that the NRA report has been useful. However, the information on certain transnational threats (i.e. tax crimes and TBML) was not sufficiently extensive in the NRA report. Advice on jurisdictions identified as high risk to Singapore is not provided to financial institutions/DNFBPs though supervisors ensure that FIs and DNFBPs evaluate country risk as part of their enterprise-wide risk assessments. Real estate agents, for example, are directed to the FATF's list of non-compliant countries which differs significantly from Singapore's high risk jurisdictions. Private sector entities report that they do not need the government to tell them where risk lies and DNFBPs report high levels of knowledge. However, the understanding of transnational TF risk appears to differ between government and the private sector, specifically on the relative importance of funding of JI and ISIL and relevant jurisdictions. Knowledge of AML/CFT risks in the private sector appears uneven, and especially low in many DNFBPs.

128. In addition to the NRA, Singapore has provided financial institutions guidance including red flag indicators. This includes guidance on TBML and transnational tax based on international experience. However, this guidance could be more tailored to how these threats are likely to materialise in Singapore based on an understanding of the nexus between these threats and specific vulnerabilities. As such, assessors did not find a high level of understanding in the financial sector of how these risks will arise in their specific contexts.

129. Private sector entities seem to commonly apply an approach that some (but not all) foreigners are high risk, Singapore residents are low risk. This maps somewhat to the transnational risk, but is a crude approach that does not take into account the role of third parties, conduits or legal persons.

130. ***Singapore has achieved a substantial level of effectiveness for IO.1***

CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

Key Findings and Recommended Actions

Key Findings

Use of financial intelligence (Immediate Outcome 6)

1. Singapore routinely makes significant use of STRs at early stages of ML and predicate investigations with the majority of asset seizures and ML investigations, relating to both domestic and foreign predicate offences, being supported by STRs. Cash Transaction Reports (CTRs) and Cash Movement Reports (CMRs) are also used but to a lesser degree. STRO does not receive information pertaining to international wire transfers into or out of Singapore, and can only access trade data through coercive means and tax information in relation to ML of tax crimes; although these types of information would be useful datasets to STRO given Singapore's role as a major trade and financial hub.
2. STRO uses well-functioning systems and coordination mechanisms to integrate FIU information into LEA processes. CAD, CPIB and ISD are the primary agencies that make significant use of STRO intelligence. Although financial intelligence information is provided to other agencies, they have yet to make significant use of STRO's financial intelligence to support their investigations.
3. STRs relating to TF are routinely disclosed to ISD and have supported investigations of TF by ISD, in some cases supported by CAD.

ML investigation and prosecution (Immediate Outcome 7)

4. Singapore has a strong legal and institutional framework for domestic ML investigation and prosecution. Singapore's LEAs have the powers and capacity to become very effective ML investigators. This capability is apparent in the significant increase in the number of ML investigations, prosecutions and convictions Singapore has recorded since its last MER. In particular, Singapore has targeted key domestic ML threats, such as UML, through the effective use of its ML offences
5. Singapore recognises the bulk of its ML risks arise from foreign predicate offending and Singapore has successfully pursued certain types of foreign predicate ML (e.g. foreign wire transfer frauds through money mules/shell companies). Singapore did not however demonstrate that it was sufficiently identifying and subsequently pursuing the more significant and complex ML cases expected of a sophisticated financial centre and trade/transportation hub such as Singapore.
6. Singapore has made efforts in recent years to pursue such cases (e.g. ML relating to foreign corruption, tax crimes and TBML); however these have only resulted in few ML convictions. All of Singapore's foreign predicate ML convictions since 2011 are for shell companies and money mules involved in foreign wire transfer fraud. The moderate gaps in Singapore's understanding of its nexus with foreign ML risks and limitations in access to tax and trade information and intercepted telecommunications may have hindered Singapore's ability to pursue offenders involved in larger-scale and more complex forms of ML.

7. Singapore demonstrated that it pursues a variety of ML cases, including self-laundering and third party ML. Despite difficulties in pursuing foreign predicate ML prosecutions, primarily due to difficulties in securing foreign evidence, AGC has had success in prosecuting ML. As most of Singapore's ML cases relate to less serious forms of offending, the level of sanctions imposed for ML are generally low. The level of sanctions is however effective, proportionate and dissuasive for the types of offences that Singapore has prosecuted so far.
8. Singapore has not prosecuted a legal person for ML. Singapore prefers to combat ML by legal persons by pursuing the natural person involved in ML. The unwillingness to pursue legal persons undermines the effectiveness of Singapore's efforts to combat ML and is not in line with the FATF standards.

Confiscation (Immediate Outcome 8)

9. Singapore has a comprehensive legal framework for seizing and confiscating criminal proceeds, instrumentalities and property of equivalent value; although it could consider new amendments to more proactively target foreign proceeds. Singapore uses the Criminal Procedure Code (CPC) for seizure and confiscation in both domestic and foreign cases as it allows for much swifter action than the CDSA. Singapore's efforts have however been undermined by a lack of strategic direction and emphasis on the pursuit of confiscation of proceeds of crime as a goal in its own right.
10. Singapore has taken steps to pursue proceeds relating to certain key ML threats (foreign corruption, fraud), but could take a more proactive approach to identifying and confiscating proceeds of foreign offending. Overall, the amounts confiscated remain low in light of Singapore's risk and context.
11. In line with its risk profile, Singapore has mainly seized and confiscated cash, with lesser amounts of non-cash assets. Singapore's efforts to pursue instrumentalities have mainly focused on vehicles used in the commission of offences. Singapore has made limited use of provisions to pursue property of equivalent value. Singapore has made few efforts to pursue proceeds moved offshore through formal channels; however Singapore has taken recent steps to do so.
12. Singapore has detected a low number of breaches of its cross-border cash and BNI reporting regime, although the number of detections has increased over the years. Singapore pursues criminal prosecutions for more serious cases of offending, which ordinarily result in a fine, but does not pursue confiscation as a sanction for breaches of its cross-border reporting regime.

Recommended Actions

Immediate Outcome 6

13. Given Singapore's status as a global trade, finance and transportation hub, STRO should seek to obtain additional strategic information sources, such as international electronic fund transfer reports, and tax and trade data to complement existing reports that provide insight into international ML/TF threats.
14. Regarding the dissemination of information Singapore should:

a. Consider granting access to STRO data to promote the use of financial intelligence by IRAS, CPIB and other agencies in other areas of Singapore's AML/CFT regime.

b. Build on recent work to increase financial intelligence disseminations to IRAS, CPIB, CNB and ICA to further support financial investigations by these agencies.

15. Singapore should elicit more TF-related STR reporting that identifies high risk and suspicious activity in addition to suspected name matches to support TF investigations. STRO reporting on TF intelligence should be more broadly disseminated to include areas with TF risks and responsibilities such as LEAs and COC.

16. STRO should conduct regular analysis of compliance with STR reporting requirements to provide strategic support for supervision. This should include working with DNFPB regulators to conduct compliance analysis on those DNFBPs to determine reasons for low reporting.

17. STRO should ensure that the volume of STRs is commensurate to the risk profile of reporting entities, particularly DNFPBs.

Immediate Outcome 7

18. Singapore should take steps to improve the capability of its LEAs to proactively identify and investigate ML, particularly complex and foreign predicate ML, including by:

a. Developing a more sophisticated understanding of the nexus between threats, inherent risks, and vulnerabilities that Singapore is exposed to from foreign predicate offending, particularly key regional ML predicate threats and high ML risk countries

b. Considering creating a legislative framework for the use of special investigative powers, particularly intercepted telecommunications

c. Considering giving CAD, CPIB and SPF direct access to tax and trade information for all types of ML investigations.

d. Continuing to undertake joint investigations with domestic and foreign partners

e. Continuing to engage directly with partners to better understand relevant typologies and ML investigation techniques, and

f. Enhancing efforts to secure admissible evidence from foreign partners and to organise foreign witnesses to give evidence in Singapore trials (e.g. through video-link).

19. Singapore should pursue complex ML cases in line with its risk profile, including targeting intermediaries and professional money launderers, in addition to money mules involved in foreign wire transfer frauds. Singapore should also:

a. Pursue more foreign PEPs involved in laundering corrupt proceeds and their professional enablers located in Singapore;

b. Better integrate IRAS and Customs into Singapore's AML/CFT regime to ensure that ML relating to tax crimes and TBML respectively is appropriately pursued.

20. Singapore should enhance its efforts to pursue legal persons involved in ML, including by:

a. Increasing the maximum penalty available for legal persons convicted of ML;

b. Pursuing ML prosecutions of legal persons and corporate service providers in

appropriate cases;

c. Developing policies and procedures and making appropriate training available for investigators and prosecutors.

Immediate Outcome 8

21. LEAs should more proactively pursue the confiscation of:
    a. Proceeds of crime, particularly linked to foreign predicate offending
    b. Property of equivalent value
    c. Property moved offshore,
    d. Instrumentalities of crime that are not vehicles.

    This should include greater use of the CDSA's seizure and confiscation powers to pursue proceeds of crime that are not directly linked to offences being prosecuted.
22. To better target proceeds of foreign predicate offences, Singapore should
    a. Consider implementing legal mechanisms which lower the burden of proof for demonstrating assets are proceeds of crime (e.g. non-criminal based confiscation, unexplained wealth, illicit enrichment, use of rebuttable presumptions). This should include robust use of the future Organised Crime Act confiscation regime and consider expanding that regime to apply to serious criminal offending outside of organised criminal activity (e.g. corruption), and:
    b. Take steps to proactively identify foreign proceeds that may be subject to confiscation.
23. CAD and IRAS should continue to work together to better pursue tax-crime related proceeds and how best to confiscate tax-related proceeds of crime, particularly proceeds of foreign tax crime.
24. ICA and CAD should pursue confiscation of physical currency and BNIs for breaches of the cross-border reporting regime as a policy objective and ensure that the regime is being implemented effectively.
25. Singapore should develop a penalty regime which allows for a wider variety of sanctions to be imposed for breaches of its cross-border reporting regime to foster a more effective use of this regime.

131. The relevant Immediate Outcomes considered and assessed in this chapter are IO6-8. The recommendations relevant for the assessment of effectiveness under this section are R.3, R4 & R29-32.

Immediate Outcome 6 (Financial intelligence ML/TF)

Use of financial intelligence and other information

132. The main source of financial intelligence is stored in STRO's database which includes STRs, Cash Movement Reports, and threshold Cash Transaction Reports (CTRs) from Casinos and PMSDs.

As STRO is a CAD unit, it has direct access to SPF and other law enforcement information and relevant Police units have direct access to STRO information. STRO can also request further information from financial institutions to support its enquiries.

133. Other LEAs routinely screen STRO information (that is, ask the STRO whether it has any information of relevance to a case/person/entity) on a request basis at an early stage of investigations. Although they have direct access to STRO information, other branches of CAD will generally conduct screening of the STRO database on a request basis to benefit from STRO's FIU experience. Urgent LEA screening requests are generally responded to in matter of a few hours ensuring that LEAs have timely access to financial intelligence information held in the database (for general screening requests, STRO can typically provide the information within five working days).

Table 5. **Overview of STR information disseminated – spontaneously and upon request**

Year request submitted	**2011**	**2012**	**2013**	**2014**	**Total**
Number of requests submitted by all LEAs	438	518	612	919	2 487
Number of entities in the requests	3 899	3 718	3 032	5 129	15 778
Year of dissemination	**2011**	**2012**	**2013**	**2014**	**Total**
No. of STRs disseminated spontaneously	2 728	3 275	3 590	3 569	13 162
No. of STRs disseminated upon request	148	451	2 710	1 918	5 227
Total number of STRs disseminated to domestic agencies	2 876	3 726	6 300	5 487	18 389

134. However, IRAS and CPIB, which have their own analytical capacity, do not have direct access to STRO information. They only are able to access financial intelligence from STRO by screening entities with STRO, which fulfils agency needs in relation to specific, enquires, but may limit application in use for intelligence processes for targeting. In particular, direct access would allow these agencies to conduct data analysis and match the STRO database against their own systems.

135. The number of screening requests to STRO has steadily increased from 438 requests relating to 3 899 entities in 2011 to 919 requests relating to 5 129 entities in 2014. This increase has in part been driven by the increased number of ML and predicate investigations relating to unlicensed money lending. However, the trend continued in 2014 despite the number of investigations into UML activity reducing. This indicates a growing appreciation of the value of STRO information.

136. There has been a general upward trend for the number of investigations supported by STRs both in the absolute number and as a percentage of the number of ML investigations. This trend points to an increase in access and use of STR information.

Table 6. **Number of investigations supported by STRs**

Year case opened	2011	2012	2013	2014	Total
Total number of domestic ML investigations	79	238	337	217	871
Number of domestic ML investigations supported by STRs[1]	28 (35%)	151 (63%)	247 (73%)	146 (67 %)	572 (66%)

Table note:
1. Each investigation can be linked to more than one STR.

137. A very high percentage of ML seizures by value were supported by STRs between 2011 and 2014 averaging 91% of seizures in relation to domestic predicates and 96% in relation to foreign predicates.

138. STRs relating to TF are routinely referred to ISD. Around 2% of all STRs disseminated were security related and supported TF investigations by ISD. In 34 cases STR information has supported ISD investigations that were referred back to CAD to make use of CAD's financial investigation expertise.

139. Data on use of CTRs and CMRs in investigations is not available. CPIB reported anecdotally that CTRs from casinos have been useful in investigating domestic and foreign corruption cases. IRAS has also been successful in using CTR information to investigate tax offending.

Case Example 1. **An STR disseminated to CPIB supported ML investigation into foreign corruption involving a foreign PEP**

On 28 August 2013, CPIB received information that a Singaporean, Person X, was involved in retaining bribe proceeds of USD 700 000 linked to a foreign PEP in Country Z. Based on information from open sources, Person X and his company in Singapore, Company A, were implicated in bribing the foreign PEP.

The financial intelligence furnished by STRO revealed the existence of a Company B and substantial cash transactions were made from this company to suspicious entities. It was also revealed that Person X controlled another company, "Company B", that was owned by his mother, and suspicious cash withdrawals of significant amount were made by his family members on various occasions out of the bank account of Company B.

Given the financial leads, CPIB mounted an operation, seized more than USD 700 000 and recovered the accounting records of Company B. The accounting records of Company B showed that various suspicious cash disbursements were made to various companies in Country Z, some of which were linked to the foreign PEP. Without this financial intelligence, operations might have mounted focusing only on the recovery of evidence from Company A, and would not have uncovered evidence of the suspicious transactions made to suspicious entities by Company B, which were subsequently found to be linked to other foreign PEPs. Related investigations are still on-going.

Case Example 2. **Use of STR supported predicate offence investigation by CAD which led to seizures of USD 1.1 million cash, jewellery, branded bags, accessories and watches, and caveat lodged against five properties**

In 2014, FIG/CAD commenced investigation into Person Y and his associates for possible forgery offences. FIG/CAD received a complaint from Person T, one of the directors of Company R and S, alleging that from 2006 to 2011, Person Y and her associates had directed payments of at least SGD 4.2 million (approx. EUR 2.77 / USD 2.95) from the bank accounts of companies, including Company R and S, without proper authorisation. The payments were made to Person Y and her associates and parties linked to them. According to Person T, Person Y would forge the signatures of Person T on the cheques of Company R and S before encashing or depositing them into various bank accounts, including bank accounts of the accused.

To further their investigation, FIG/CAD conducted screening with STRO database and received STRs filed on the accused by entities in the banking, insurance and remittance service sectors. The STRs supported FIG/CAD's suspicion that various unauthorised payments were linked to insurance policies held by Person Y and her family members. It provided information on the funds flow which supported CAD's investigation and led to the successful seizure of SGD 1.1 million (approx. EUR 659 600 / USD 772 310) cash, 125 pieces of jewellery, 93 branded bags and accessories, 12 watches and caveat lodged against five properties valued at a total of about SGD 4.9 million (approx. EUR 3.23 million / USD 3.4 million). Investigation is currently on-going.

STRs received and requested by competent authorities

140. STRO uses a network of liaison officers to validate the relevance of information provided to LEAs and competent authorities. Information from liaison officers is used to provide guidance material and outreach to reporting entities on what to report and what information to include in STRs (red flags and financial information such as statements, account opening information). This process has led to STR reporting that is relevant to LEAs and generally of high quality. A joint intelligence exercise between STRO and IRAS was undertaken to guide reporting entities in filing STRs that will be relevant to tax offences. Singapore has taken steps to increase STRs used by IRAS. Between July 2013 to September 2013, STRO and IRAS reviewed all the STRs received suspected to be related to tax crimes, during the first three months of implementing tax crimes as a money laundering predicate. The review results were used to develop referral criteria and red flag indicators.

141. The number of STRs disseminated to authorities relating to high risk predicate offences such as tax offences and corruption are still relatively low (a total of 1 374 and 1 084 respectively between 2011 and 2014 compared to 1 710 relating to robbery and theft which are considered lower risk). Only 4 STRs were disseminated since 2011 relating to environmental crime which is a major regional threat. By contrast, Singapore's cross-government coordination and outreach to the private sector on identified high risk unlicensed money lending, and transnational fraud facilitated by Singapore based mules, led to high STR reporting (especially in 2013). This ensured that STRO and LEAs had access to relevant reports to initiate and support activities, which have successfully disrupted unlicensed money lending and successful investigation of money mules (see IO.7).

i. Receipt of other relevant financial intelligence information

142. STRO accesses further information from financial institutions to add value to STRs and a summary of this information, STROs findings, and where possible or appropriate networks analysis is provided to other authorities in spontaneous disseminations. STRO also uses CTRs to identify outlier transactions to inform proactive identification of suspicious transactions. Although statistics on the relevance of these reports to authorities' activities is not recorded, CTRs have been shown to be useful in several cases.

143. Use of international electronic fund transfer reporting to proactively identify targets has not been considered. Given Singapore's vulnerability to transnational ML/TF threats and in consideration of Singapore's status as one of the world's largest financial centres, information about international electronic fund transfers would be a great asset to Singapore's financial intelligence holdings.

144. Trade data is not accessible by STRO for intelligence purposes, except for specific records via an administrative order or court ordered production order, which in practice STRO does not use. This leads to protracted or incomplete analysis in reports relating to possible TBML or trade fraud; and does not facilitate data analysis techniques to detect TBML This is a shortcoming for financial intelligence in a major trade hub, and information held in Customs' Singapore's National Single Window for trade declaration, TradeNet, would add significant value if matched to financial intelligence. Similarly, tax information cannot be accessed by law enforcement (including STRO), except in relation to ML cases of tax crimes, or court order, further limiting operational efficiency and/or the breadth of information to base financial intelligence on. LEAs reported that in some instances, in particular transnational cases, STRO screening may not identify associates of targets without LEA explanation of individuals associated with the targets. This indicates that more benefit of financial intelligence could be realised to identify associates if STRO had direct access to wider sources of financial information (particularly tax and trade information) to supplement STRs and LEA information.

ii. Financial intelligence received by MAS relevant to compliance

145. STRO has recently conducted strategic analysis of STR reporting by several sectors to support MAS supervision. This analysis of reporting compliance has considered the number of STRs submitted, types of STRs, timeliness of reporting, adequacy of supporting information and usefulness. Major reporting sectors, the banking sector, capital market intermediaries and investment intermediaries, money changers and remitters, insurance sector, and casinos have been reported on. Although SVFs have reported 1 000-2 000 STRs per year, a report has not been produced on this sector's compliance. Strategic analysis has not been completed on sectors that are reporting low numbers of STRs, such as DNFBPs, have not been analysed, nor has there been analysis on reporting relating to vulnerabilities such as legal persons or trade.

Operational needs supported by FIU analysis and dissemination

i. FIU analysis and dissemination

146. Most STRO information used by investigative agencies is obtained on a request basis. In these instances simple dissemination of STRO holdings are provided to support operations by law

enforcement agencies. In addition to STRO enquiries, law enforcement agencies conduct elements of financial intelligence collection independently. Law enforcement agencies also use their own powers to gather relevant information, such as transaction histories and other information, directly from financial institutions.

147. LEAs and competent authorities may also be supported by spontaneous dissemination of STRO information. An automated rules-based process identifies STRs for further STRO enquiries to determine if the STR is of interest to LEAs. Further information may be integrated, such as statements from reporting entities, and some analytical tools such as network charting may be used. Tactical reports focus on collated screening checks on the STRO database, a commercial database, law enforcement information and a summary of relevant bank transactions.

148. Further STRO developed analytical products could deepen understanding, particularly in relation to high risk forms of transnational ML (particulars relating to tax and corruption) and TF. In possible TBML cases STRO's lack of access to trade information (other than through coercive investigative mechanisms) prevents sufficient intelligence analysis.

149. Most STRs, CTRs and CMRs are disseminated to SPF (including CAD) and CPIB, although an increasing number are disseminated to IRAS. This indicates an emerging focus support of tax administration by STRO information.

ii. Use of STR information by LEAs in investigations

150. ML investigations, mostly CAD led, regularly supported by STR information. In 66% of domestic ML cases and 82% of ML investigations of foreign predicates STR information was used, most commonly by providing information to investigations triggered by other means. ML investigations by CPIB have also been supported by STR information, although the only year in which a significant number of STRs supported/initiated a CPIB investigation was 2013 (in other years, there were 6 STRs or fewer which supported CPIB investigations). CPIB predicate investigations have been supported by a number of STRs comparable to ML investigations.

151. ML investigations are also being initiated as a result of proactive financial intelligence by STRO, although on a less regular basis than investigations supported by STRs. A total of 199 ML investigations have been initiated by 500 STRs.

152. CNB, IRAS, ICA and regulatory agencies have also made limited use of STRs in predicate offence investigations. IRAS's use of a single STR to support predicate investigations is not consistent with the number of STRs disseminated to IRAS (1 303 from 2011-2014), indicating that STR information has not yet been successful to support investigations of predicate tax offence or related ML. However, the bulk of these STRs disseminated to IRAS were referred as part of an exercise for STRO and IRAS to jointly develop red flag indicators and STR referral criteria for tax crimes.

Table 7. **Number of STRs that supported predicate offence investigations**

Year case opened	2011	2012	2013	2014
Total	341	420	858	760
With breakdown by recipients				
SPF (including CAD)	323	414	754	732
CPIB	9	3	101	19
CNB	0	2	0	0
IRAS	0	0	0	1
ICA	9	0	0	2
Regulatory Authorities	0	1	3	0
Others	0	0	0	6

Cooperation and exchange of information/financial intelligence

153. STRO's status as a unit within CAD and this leads to financial intelligence processes being well coordinated with LEA processes. This ensures secure communication using SPF protocols and access to LEA information that can be integrated with FIU information. As a unit within CAD, STRO has well defined protocols to protect information and its exchange of information with partners is governed by SOPs which protect confidentiality of STRO information.

154. Outside of CAD, STRO coordination with agencies is well governed by established SOPs. Operationally the liaison officer system ensures cooperation and coordination at tactical levels (in relation to specific enquiries) and more strategically in relation to improving red flag indicators or other guidance.

155. Foreign coordination is achieved through the Egmont information sharing channel. LEAs are able to access foreign financial intelligence by making requests through STRO. STRO also facilitates foreign requests to LEAs where relevant.

156. ***Singapore has achieved a substantial level of effectiveness for IO.6***

Immediate Outcome 7 (ML investigation and prosecution)

ML identification and investigation

157. Singapore has one general criminal investigative agency (the Singapore Police Force – SPF) and several other specialist investigative agencies. Three LEAs in Singapore conduct ML investigations – SPF, the Commercial Affairs Department (CAD) and the Corrupt Practices Investigation Bureau (CPIB). Between 2008 and 2014, CAD conducted 78% (788) of Singapore's ML investigations. SPF and CPIB conducted the other 22% of Singapore's ML investigations (183 and 37 ML investigations respectively). All other LEAs and competent authorities will refer ML cases to CAD to investigate.

158. Located within SPF, CAD is Singapore's lead LEA for ML investigations and other commercial crimes (including cheating, CBT and embezzlement). CAD has a specific division for financial and ML investigations – the Financial Investigations Group (FIG). In 2013, CAD restructured

and substantially increased the manpower of FIG. At the time of the on-site, FIG had 68 officers, of whom 59 were investigators, compared to 22 officers in 2007. FIG officers have at least 80 hours of training every year, out of which 48 hours are AML/CFT-related training.

159. CPIB has responsibility for corruption (i.e. bribery) investigations and also conducts related ML investigations. CPIB's Financial Investigation Branch was set up in June 2011 as a specialised unit to lead ML investigations related to bribery and currently has 10 officers. SPF conducts certain ML investigations relating to less complex cases (e.g. UML). SPF will refer more significant and complex cases of ML to CAD as outlined in a standard operating procedure (SOP). ML and financial intelligence training is available to SPF officers.

160. The increase in resources in CAD and CPIB is a positive development and should improve Singapore's capacity to investigate ML as new officers develop their investigative skills.

161. The main ML LEAs identify the majority of ML cases by reviewing predicate offence investigations, responding to complaints from victims, referrals from other agencies, referrals of STRs and foreign requests for assistance. Singapore has made a number of operational and policy changes to better investigate ML when it is identified through these channels. This has resulted in substantial increases in the number of ML cases investigated.

162. Singapore's small geographic size enables very close cooperation and coordination between agencies, which is a significant inherent strength of Singapore's law enforcement regime. CAD and each relevant agency have agreed to SOPs to promote detection and guide the referral of ML cases to CAD. The main LEAs and competent authorities responsible for investigating predicate offences all use a standard pro forma which requires investigators to consider whether there is a possible ML offence in their predicate investigation. The SOPs generally set out reasonable processes and CAD's proactive approach in developing these SOPs is commended. As demonstrated by the increasing number of ML referrals from SPF to CAD (42 in 2014 compared to 2 in 2011), the pro forma is a useful way of encouraging agencies to identify ML. Despite the close coordination enabled by Singapore's geographic context, the number of referrals from other LEAs remains very small (5 in 2014). The other LEAs did not demonstrate that they adequately identify ML arising from their respective predicate offences. CAD should continue its efforts to proactively engage partner agencies through mechanisms such as joint investigations/task forces.

163. Assisted by STRO's position within CAD, LEAs make good use of the financial intelligence produced by STRO to both commence and investigate ML cases. For instance, 500 STRs have led to the commencement of 199 ML investigations between 2011 and 2014 (see IO.6 for further information).

164. While Singapore has a very strong ML investigative framework under the CPC and CDSA, Singapore did not demonstrate it is using this framework sufficiently to combat ML. In particular, Singapore is not adequately identifying or investigating ML relating to foreign predicates. While 66% (665 out of 1 008) of Singapore's investigations relate to foreign predicates, they almost all relate to Singaporean money mules and shell companies that allow their bank accounts to be used to receive the proceeds of foreign wire transfer frauds. Singapore did not demonstrate that it was sufficiently identifying the more complex and sophisticated forms of ML it is likely exposed to by virtue of its large financial sector and position as a trade / transport hub. Singapore has identified few cases of ML by proactive investigation (e.g. through intelligence, non-STR data analysis, identifying individuals with unexplained wealth) and CAD did not consider these to be potential sources of ML investigations.

165. The following issues have reduced Singapore's ability to effectively identify and investigate ML:

- The moderate shortcomings in Singapore's understanding of its foreign ML risks, more specifically on the nexus between threats, inherent risks and vulnerabilities, has some implications on its ability to identify foreign predicate ML relating to certain threats (e.g. drugs, environmental crime) (see core issue 7.2 below).
- IRAS can only provide taxation information to LEAs when there is a tax-related ML case.[31] LEAs do not have direct access to tax information in other ML investigations is very limited and consequently the LEAs have made little use of tax information in ML investigations. LEAs also have similarly limited access to trade information held by Customs. The lack of direct access to this information is hindering Singapore from fully investigating ML, particularly more complex typologies, and expanding direct access should be considered.
- As there is no comprehensive legislative or policy framework for the use of several special investigative techniques (see Recommendation 31), the assessors are of the opinion that LEAs make limited use of such techniques. Nevertheless, Singapore has demonstrated SOPs and case studies during the on-site on the use of SITs. In particular, Singaporean authorities are not empowered under legislation to intercept telecommunications data and do not use such information as evidence in prosecutions or share this information with foreign partners (see Recommendation 37). This impedes Singapore's ability to pursue the more complex ML cases, such as ML conspiracies or syndicates. Singapore should consider establishing a comprehensive legislative scheme empowering LEAs to use these techniques.

166. The LEAs' familiarity with more complex and newer types of ML (e.g. trade-based ML and ML relating to tax crime) is developing, particularly as tax crime was only added as a ML predicate in 2013 (see core issue 7.2 below).

167. Singapore has taken steps to address these issues; including approaching foreign counterparts with information on foreign predicate offences; sending Spontaneous Exchanges of Information by STRO to other FIUs with the aim of identifying possible ML; undertaking joint ML investigations with foreign partners (see IO.2). CAD also analyses all foreign requests for assistance it receives through formal and informal channels to ascertain if there is sufficient evidence to initiate a domestic ML investigation, resulting in 70 joint ML investigations with foreign partners between 2011 and 2014.

168. Outside of the issues identified above, the LEAs have access to a wide range of information for the purposes of their investigations, including financial intelligence, information from public databases and police records such as criminal history and police intelligence.

169. LEAs (including SPF, CAD and CPIB) have far-reaching investigative powers under the CPC. LEAs are able to request information from individuals and organisations, including banking information, and enter and search premises, often without needing a court order or warrant. This

[31] Taxation information can also be provided pursuant to a court order in investigations into UML, corruption and organised crime (once the Organised Crime Act is implemented). On-site.

has meant that the powers in the CDSA, which require court orders, are rarely used. Singapore demonstrated that LEAs are able to access banking information and documents in a timely manner using its powers under the CPC and bank secrecy laws do not hinder their investigations. This framework enables the LEAs to take very swift action to investigate offences and prevent dissipation of assets. The private sector noted frequent engagement with LEAs and advised they were usually able to respond to requests for information in a timely manner. SPF/CAD and CPIB utilise case management systems and SOPs to effectively manage and prioritise their ML and predicate investigations. CAD aims to finish investigations within 6 months, but achieves 9 months on average. This timeline seems reasonable for the types of cases Singapore typically investigates.

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

i. ML strategy

170. As outlined in its AML policy statement, Singapore has a whole-of-government approach to combating ML which aims to detect, deter and prevent ML and associated predicate offences.[32] This statement is too high-level to provide a strategic direction for Singapore's LEAs. CAD released a specific ML strategy[33] during the on-site. This should help provide such direction, however it is too new to have any impact on effectiveness.

171. Singapore's has increased the number of ML investigations, prosecutions and convictions since its last mutual evaluation and is a positive development. Singapore attributes this rise to legislative and policy changes which made it easier to pursue ML and share information, as well as the NRA exercise which provided focus for the LEAs. The main LEAs considered that the pro forma had helped trigger a cultural shift to consider the ML aspect in predicate investigations. This shift has not fully filtered out to the other LEAs, but continued engagement from CAD should assist.

[32]MOF (nd), Singapore's AML/CFT Policy Statement www.mof.gov.sg/Policies/Anti-Money-Laundering-Countering-the-Financing-of-Terrorism-AML-CFT/Singapores-AML-CFT-Policy-Statement.

[33] Singapore Police Force (nd), AML Policy Statement and Strategies, www.police.gov.sg/about-us/organisational-structure/specialist-staff-departments/commercial-affairs-department/aml-cft/aml-policy-statement-and-strategies

Table 8. **Number of ML investigations, prosecutions and convictions from 2008 to 2014**[1]

Status	2008	2009	2010	2011	2012	2013	2014	Total
ML cases investigated[2]	**49**	**28**	**60**	**79**	**238**	**337**	**217**	**1008**
Foreign Predicate Offences	16	16	30	32	145	268	158	**665**
Domestic Predicate Offences	33	12	30	47	91	66	57	**336**
Both foreign and domestic	0	0	0	0	2	3	2	**7**
Number of individuals prosecuted for ML[3]	**23**	**26**	**14**	**44**	**57**	**79**	**111**	**354**
Foreign Predicate Offences	16	14	3	2	10	31	48	**124**
Domestic Predicate Offences	7	12	11	42	47	48	63	**230**
Number of individuals convicted for ML[4]	**24**	**26**	**18**	**33**	**71**	**82**	**89**	**343**
Foreign Predicate Offences	15	13	7	0	1	18	38	**92**
Domestic Predicate Offences	9	13	11	33	70	64	51	**251**

Table Notes:

1. Includes prosecutions and convictions under sections 46 and 47 of the CDSA and section 14(3A)(b) of the Moneylenders Act.
2. http://www.police.gov.sg/about-us/organisational-structure/specialist-staff-departments/commercial-affairs-department/aml-cft/aml-policy-statement-and-strategies
3. Statistics collated bases on the year that the investigation was commenced.
4. Statistics collated based on the year that the suspect was prosecuted. The figures may include persons who were investigated prior to 2008.
5. Statistics collated based on the year that the suspect was convicted. The figures may include persons who were investigated prior to 2008.

ii. Foreign threats

172. The bulk of Singapore's ML risks arise from foreign predicate offending, with ML,[34] cheating and foreign corruption the key threats identified in the NRA. The LEAs generally agreed with the NRA's findings of the higher risk predicates and stated that focus has shifted to ML activity relating to overseas threats. Foreign predicate ML investigations constitute 70% of the ML investigations conducted by LEAs between 2011 and 2014. This drops to 21% once the conviction stage is reached however. 94% of the foreign predicate ML investigations are foreign cheating cases, primarily through money mules and shell companies, and CAD has demonstrated a proactive response to targeting this type of offending. CAD's robust enforcement of these offences, in conjunction with a public awareness campaign, led to the number of money mule investigations dropping to 123 cases in 2014 from a peak of 212 in 2013. CAD also provided examples of where it has engaged foreign partners even where they were not aware of the foreign predicate offence. Singapore's efforts to tackle the foreign wire transfer fraud cases are commendable.

[34]Singapore clarified that this refers to cases arising from foreign requests for assistance where the offence cited in the foreign request is ML. These typically turn out to relate to the laundering of proceeds of foreign frauds through shell companies.

Case Example 3. **Pursuing domestic ML money mule investigation arising from foreign wire transfer fraud**

A money mule (Person N) was recruited by another (Person D) to receive and transfer funds derived from wire transfer fraud perpetrated against victims from the US, Canada and Cook Islands. In total, Person N received around SGD 1.25 million (approx. EUR 824 500 / USD 877 625) worth of criminal proceeds.

The active collaboration between CAD and its foreign counterpart led to Person N being convicted and sentenced to a total of 54 months' imprisonment for dishonestly receiving stolen property and ML offences. Person D was also sentenced to a total of 36 months' imprisonment for dishonestly receiving stolen property and ML offences.

173. Outside of money mules and shell companies, Singapore did not demonstrate that it sufficiently pursued foreign predicate ML. Since 2011, Singapore has not convicted a person for any type of foreign predicate ML except for wire transfer fraud. The moderate shortcomings in Singapore's understanding of its transnational risk profile (see IO.1) have further implications for this.

174. Singapore did not consider some significant regional predicates to be high risk (e.g. drug trafficking, environmental crime), and the NRA could have provided more information on regional neighbours with significant ML risks. Instead Singapore's foreign ML cases have mainly been those that are readily identifiable and relate to less complex or smaller-scale offending (i.e. money mules cases where the victim is located in a country with a well-developed international cooperation framework). This undermines the effectiveness of Singapore's AML regime as it leaves Singapore exposed to more complex transnational ML.

175. The authorities recognised foreign corruption to be a major ML threat and emphasised their commitment to preventing corrupt proceeds of crime being held in Singapore. This includes reviewing informal and MLA foreign corruption requests to ascertain whether corruption-related proceeds have passed through Singapore. When alerted to potential cases of foreign corruption, CPIB demonstrated that it has taken proactive steps to seize funds and cooperate with foreign partners. This includes conducting joint investigations and sharing information about the potential corrupt proceeds with the originating jurisdiction. CPIB and CAD have conducted 13 investigations relating to foreign corruption between 2011 and 2014 and one prosecution was underway at the time of the on-site. Singapore has not convicted an individual for ML relating to foreign corruption (although it has convicted one individual for dishonestly receiving stolen property relating to foreign corruption). Corruption relates to 20% of the total number of MLA requests Singapore has received, and STRO disseminated 138 spontaneous exchanges of information relating to foreign corruption to foreign counterparts, indicating that corrupt proceeds may be passing through Singapore. Overall, Singapore's results on tackling ML related to foreign corruption are not commensurate with its risk profile. CPIB should expand its focus to more proactively pursue ML related to foreign corruption, including more vigorously pursuing foreign PEPs and their professional enablers in Singapore. At the time of the onsite, Singapore was pursuing a very complex case involving transnational

fraud/corruption in close collaboration with foreign counterparts. This involves many jurisdictions, numerous corporate entities, a large number of bank accounts and transactions.[35]

176. Given Singapore's inherent exposure as a wealth management hub, Singapore considered the ML risk in relation to tax crime to be medium in light of other factors including the number of cases, the number of foreign requests, and feedback from foreign counterparts. Singapore added tax crime as a predicate for ML in 2013. Since then, five ML investigations have been identified, resulting in four convictions for domestic tax crime-related ML. As information flows between CAD and IRAS improve and CAD and IRAS's understanding of tax-related ML develops, this number should increase. Of particular concern was that no law enforcement action seemed to arise out of the tax review process conducted in 2013 (see IO.3 for more information on the tax review process). Despite the closure of 22 000 accounts and several thousand being STRs filed, CAD/IRAS had not identified any ML activity. Singapore should keep a watching brief on tax crime and take a more proactive approach to it as it has potential to be an emerging high risk.

177. In light of its position as a global trade hub, Singapore has taken steps to better understand TBML and identify possible TBML cases for joint investigations with foreign counterparts. Singapore has conducted 15 investigations into TBML since 2011 and is engaging key partners to develop its understanding. The assessors commend these efforts, although these have not yet translated into any prosecutions of convictions for TBML. CAD should engage Customs in particular to better target TBML and better integrate Customs into Singapore's AML/CFT regime. Trade data should also be integrated into the financial intelligence process to support and initiate TBML investigations (see IO.6).

Table 9. **ML convictions by underlying predicate[1]**

Year	2008	2009	2010	2011	2012	2013	2014	Total[2]
Domestic								
UML – Unlicensed money lending	0	0	0	15	47	51	31	144
Cheating	5	7	5	11	17	5	8	58
CBT – Criminal breach of trust	3	1	0	4	5	5	6	24
Theft	1	3	2	7	5	2	2	22
Forgery	4	5	2	2	5	3	2	23
Dishonest misappropriation of property	0	0	0	0	0	1	2	3
Counterfeiting and piracy of products	0	0	0	0	0	1	0	1
Tax evasion[3]	N/A	N/A	N/A	N/A	N/A	0	4	4
Participation in an organised criminal group and	0	0	2	0	0	0	0	2
Unlawful presence or entry in Singapore	0	0	0	0	0	0	1	1
Corruption	0	0	0	0	0	0	1	1
Smuggling of goods	0	0	0	0	1	0	0	1
Total	13	16	11	39	80	68	57	284

[35] After the on-site, two individuals were charged in court, one with ML and the other with corruption. Investigations are on-going and additional charges may be brought in the future.

Year	2008	2009	2010	2011	2012	2013	2014	Total[2]
Foreign								
Cheating	15	5	3	0	1	18	38	80
Participation in organised criminal group and	0	8	4	0	0	0	0	12
Corruption	0	0	0	0	0	0	0	0
Tax evasion[4]	N/A	N/A	N/A	N/A	N/A	0	0	0
Total	**15**	**13**	**7**	**0**	**1**	**18**	**38**	**92**

Table Notes

1. All convictions are under the CDSA, except for UML which includes convictions under the CDSA and Moneylenders Act.

2. Some ML convictions relate to more than one category of predicate, so the totals are higher than the total number of convictions.

3. Tax evasion became a predicate for ML in 2013.

4. Tax evasion became a predicate for ML in 2013.

iii. Domestic threats

178. Singapore's generally low domestic crime rate has minimised the ML threats posed by domestic predicate offending. The NRA considered that UML, cheating and CBT to be Singapore's three major ML threats and the assessors generally agree with Singapore's understanding of its domestic risks. Together these three predicates comprise the majority of Singapore's domestic ML convictions between 2008 and 2014.

179. A sizeable number of Singapore's recent domestic ML cases have related to domestic UML activities (42% of ML convictions between 2011 and 2014). Singapore's strategy to combat UML is a highly effective example of how Singapore can use its ML offences and deploy resources to target a key ML threat. The pursuit of UML through ML investigations, as part of a broader suite of measures, has led to a notable reduction in the number of complaints about UML (see case example Case Example 4 below).

Case Example 4. **Unlicensed Moneylending Strike Force**

UML is one of the crime types from domestic sources assessed to be of major ML threat to Singapore in the NRA. The UML problem in Singapore reached its peak in 2009 when there were more than 18 000 UML-related police reports. SPF recognised this as a major ML threat to Singapore and promptly employed wide-ranging measures to deal with the problem.

Singapore created the UML Strike Force (UMSF) within the SPF to provide a framework to combat UML activities. The UMSF placed a priority on pursuing ML connected to UML activities and ensured all officers considered ML elements in their investigations. Between 2011 and 2014, the UMSF conducted 136 ML investigations relating to UML activities (15% of all ML investigations).

Singapore also introduced new measures to give the SPF broader powers to freeze the assets of unlicensed moneylenders who have been placed under detention orders and created a new strict liability ML-type offence (section 14(3A)(b) of the Moneylenders Act) to target individuals who help unlawful moneylenders launder the proceeds of their crime. SPF also formalised internal SOPs and guidelines on the early detection, tracking and referral of possible ML

offences.

Combined with other enhanced measures, the number of UML related police reports fell annually from nearly 18 000 at its peak in 2009 to about 6 500 (or -64%) in 2014. This indicates that Singapore is using its ML offences to effectively to detect and dissuade criminals from carrying out UML.

iv. ML channels

180. The NRA considers that the main conduits for ML in Singapore are banks, remitters, shell companies and individual money mules. The majority of Singapore's ML cases involve these channels and Singapore has taken action to combat ML through these channels.

181. While recognising the risk posed by remitters as a sector, Singapore considered that the risk for each individual remitter was largely mitigated by its AML/CFT regulatory regime (see IO.3) and active enforcement against illegal/unlicensed remitters. Singapore's large migrant population from countries that the assessors would consider to have high AML/CFT risks (in the absence of any public geographic risk assessment by the authorities) leaves it exposed to inherent ML/TF risks, which may not be mitigated by its AML/CFT regulatory regime in all circumstances. Accordingly Singapore may be underestimating the risks remitters pose.

182. As casinos are still relatively new to Singapore, CAD is developing its understanding of ML relating to this sector. Singapore has eight cases of individuals potentially laundering funds through the casino and considered that the tight regulatory controls mitigate this risk. Other information however indicates potential ML activity that the LEAs are not identifying. The casinos lodge over 1 000 STRs a year and at least one casino has banned a substantial number of individuals due to suspected ML activity.

Types of ML cases pursued

Prosecution of ML cases

183. Overall, Singapore has significantly increased the number of ML prosecutions and convictions in recent years. Singapore conducted 354 ML prosecutions and secured 343 ML convictions between 2008 and 2014 (see Table 8, p. 58).

184. Once a LEA completes a criminal investigation, all investigation briefs are referred to the Attorney-General's Chambers (AGC) for independent review.[36] AGC indicated it agrees with the recommended course of action in the vast majority of ML cases. AGC also has Deputy Public Prosecutors co-located with LEAs, including CAD and CPIB, to provide prompt legal assessment of ML cases. These mechanisms ensure that the brief referral process operates smoothly and fairly quickly.

185. AGC conducts all ML prosecutions in Singapore and has a specialist Financial and Technology Crime Division which conducts most ML prosecutions. Other AGC divisions may conduct more minor ML prosecutions (e.g. UML) where appropriate. All prosecutors undergo specific ML training as part of their induction. CAD has also conducted outreach to the courts on ML.

[36]If a case is below a certain threshold and where the LEA proposes no further action, these can be considered by AGC officers outposted in LEAs, rather than being submitted to AGC.

186. AGC demonstrated that it is prosecuting all types of ML offences, including self-laundering, third-party laundering, standalone ML, foreign predicate and domestic predicate. Most convictions relate to third-party laundering due to Singapore's focus on money mules and UML, meaning that Singapore purses comparatively less self-laundering cases. Most convictions occur under section 47 of the CDSA (acquiring, possessing, using, concealing or transferring benefits of criminal conduct) and section 14(3A)(b) of the Moneylenders Act for ML relating to UML specifically. AGC is effective in prosecuting ML cases as indicated by its high conviction rate for ML (90%). AGC indicated that the high proportion of offenders who do not contest contributed to the high conviction rate (approximately 60% of ML cases).

Table 10. **Breakdown of ML convictions by self-laundering and third-party laundering[1]**

Year	2008	2009	2010	2011	2012	2013	2014	Total
Self-Laundering	5	12	8	21	17	14	18	95
Third party laundering	19	16	11	15	55	69	72	257
Total	24	28	19	36	72	83	90	352

Table note
1. Seven individuals were convicted of both self and third party laundering.

187. AGC did not consider that it had any major difficulties in prosecuting the ML offence. Court precedent has made clear that a prosecutor does not have to prove a predicate offence[37] and Singapore has consequently codified this in its ML offence.[38] The authorities did note the inherent difficulties foreign-predicate ML pose for prosecutions, with 26 ML prosecutions discontinued between 2008 and 2014 due to uncooperative foreign victims and/or witnesses. AGC did indicate that alternate methods of proving foreign ML offences were being pursued, such as tendering of written evidence (e.g. initial complaints, affidavits and SWIFT messages). Singapore should continue to explore ways to overcome the difficulties that obtaining foreign evidence pose. This could include using MLA to arrange foreign witnesses to give testimony, including via video link.

188. While the increasing trend for ML convictions is positive, most prosecutions are for offenders involved in small scale or less complex ML relating to wire transfer fraud money mules and UML. These are substantially less complex and sophisticated ML prosecutions and convictions than would be expected of a financial and trade centre with a ML risk profile such as Singapore. Singapore has not convicted a person for foreign predicate ML unrelated to wire transfer fraud since 2011. While Singapore provided 12 case examples of more complex and sophisticated investigations (e.g. tax ML, TBML, and foreign corruption ML) involving multiple jurisdictions, these have led to only four ML prosecutions, three ML convictions and two prosecutions/convictions for dishonestly receiving stolen property in Singapore, and have rarely led to ML convictions in foreign countries either. Singapore explained that these cases are still pending the completion of investigations as such complex cases would typically take a longer time to complete. This indicates Singapore has only begun pursuing such cases in recent years, but should lead to tangible results in the future.

[37] Jeanette Ang v PP [2011] SGHC 100.
[38] Section 47A of the CDSA.

Case Example 5. **Singapore example of a complex ML case involving multilayer shell company operation**

Singapore commenced ML investigations into Person X for setting up a shell company, Company Y, and using the bank account of the shell company to receive criminal proceeds. Investigations revealed that the bank account of Company Y had received USD 75 210.73 from wire transfer fraud committed overseas.

Further investigation revealed that Person X had also instigated a third party on a separate occasion to procure a corporate bank account to receive criminal proceeds. With the help of the third party, Person X managed to convince Person W to allow his company's bank account to be used to receive criminal proceeds derived from another wire transfer fraud. Their attempt to defraud the victim was unsuccessful however, as the funds were recalled by the remitting bank.

Person X was convicted and sentenced to 33 months imprisonment for ML and dishonestly receiving stolen property. Person W was convicted and sentenced to ten months imprisonment for engaging in a conspiracy to dishonestly receive stolen property.

189. Singapore has identified numerous companies involved in ML. In particular, Singapore has investigated a significant number of cases relating to laundering proceeds of transnational cheating through shell companies. Singapore has not prosecuted or convicted a company for ML.

190. With regard to shell companies, Singapore has implemented measures to address the underlying issue that enables their misuse, by enhancing the regulatory regime for CSPs. As these amendments were made in May 2015, they are too new to mitigate the risk in this area. The ease with which a company can be set up in Singapore has encouraged the use of shell companies as a vehicle to launder proceeds of crime, particularly in relation to foreign predicate offending. These are typically set up by non-residents based overseas using a Singaporean-based CSP. CAD has commenced 173 ML investigations into suspected shell companies. Singapore's preference has been to deal with this issue by seizing the company's assets (if any) and deregistering the company. The authorities considered this to be more effective than prosecuting the asset-less companies themselves. At the time of the on-site, AGC had a test ML prosecution underway of a CSP for their role in setting up these shell companies.[39] This is a step in the right direction.

191. For non-shell companies involved in ML, Singapore's preference is to pursue the individuals responsible for the laundering. The authorities considered that if a company were to be convicted, the company would just factor the fine into its normal course of business or wind itself up, preventing the imposition of dissuasive sanctions. AGC's policy is that it would prosecute a company where the ML was part of a corporate culture of malfeasance and no suitable case had yet been identified. This policy appears higher than the legal standard required for corporate criminal responsibility.[40]

[39] After the end of the on-site, the director of the CSP was convicted of one count of contravening section 157(1) of the Companies Act (Cap 50) by failing to exercise reasonable diligence in discharging his duties as a director and six counts of ML under Section 59(1)(b) of the CDSA. The director was sentenced to 26 months and 4 weeks imprisonment.

[40] Singapore advised the general test for corporate criminal responsibility is to determine whether the persons who are the directing mind and will of the company had committed such acts with the requisite mental state.

192. The unwillingness to purse legal persons undermines the effectiveness of Singapore's efforts to combat ML and is not consistent with the FATF standards. Singapore should pursue legal persons for ML offences, as well as continuing its efforts to pursue CSPs. To facilitate this process, policies and procedures should be developed and investigators and prosecutors should have appropriate training made available.

Effectiveness, proportionality and dissuasiveness of sanctions

193. All offenders convicted of ML have had a prison sentence imposed. Around half of those convicted also have had a fine imposed (averaging SGD 80 000 – approx. EUR 52 758 / USD 56 165). Cases of less serious offending are dealt with by way of a letter of warning from SPF (in consultation with AGC).

Table 11. **Sentences imposed for ML offences**

Year	2008	2009	2010	2011	2012	2013	2014	Total	% of total
Prison sentences									
≥ 48 months	3	1	1	1	1	0	1	**8**	**2%**
36 to < 48 months	1	8	1	3	2	0	1	**16**	**5%**
24 to < 36 months	1	8	3	1	2	2	4	**21**	**6%**
12 to < 24 months	8	4	3	9	8	8	18	**58**	**17%**
< 12 months	11	5	10	19	58	72	65	**240**	**70%**
Total	**24**	**26**	**18**	**33**	**71**	**82**	**89**	**343**	**100%**
Fines									
Persons fined	0	2	0	16	47	56	26	**147**	**43%**
Total amount fined (SGD)	0	6 300	0	2 802 000	4 540 000	3 162 000	1 952 000	**12 462 300**	
Average fine (SGD)	0%	3 150	0	175 125	96 596	56 464	75 077	**84 778**	

194. In general, the sanctions imposed for ML convictions are low. 70% of the convictions between 2008 and 2014 involved a prison sentence of less than 12 months and only 8 prison sentences were greater than four years (one such example is described below). The total sentence increases once the predicate offence is also taken into account (18% of the global sentences are above 4 years).

195. The sentences imposed are low because they reflect the kinds of cases AGC is prosecuting (e.g. ML relating to money mules and UML). However the sentences imposed so far are proportionate, dissuasive and effective to the types of offences prosecuted. For example, Singapore has only detected two cases of re-offending.

Case Example 6. **Six year sentence imposed for ML**

Over a three year period, Person K and L deceived Company S into paying about SGD 12 million (approx. EUR 7.9 million / USD 8.4 million) for goods and services it did not receive. Person K had also committed fraud against other companies he was previously working for. Person K was charged with more than 300 counts of cheating and ML offences. He was sentenced to 22 years' imprisonment, with 6 years' imprisonment for ML specifically. Person L was charged with 282

3

counts of cheating and sentenced to 15 years in jail. Investigators also confiscated a SGD 6.2 million (approx. EUR 4.1 / USD 4.35) worth of properties and cash, luxury watches and jewellery from Person K, SGD 1.3 million (approx. EUR 857 480 / USD 912 730) from Person K's wife and SGD 1.2 million (approx. EUR 791 520 / USD 842 520) worth of assets and valuables, including luxury watches and $2 million from Person L's close relatives.

196. As no legal person has been convicted of ML, it is not possible to assess the effectiveness, proportionality and dissuasiveness of sanctions on legal persons specifically.

197. Singapore should continue its efforts to pursue CSPs, as well as pursue legal persons in appropriate cases. To facilitate this process, policies and procedures should be developed and investigators and prosecutors should have appropriate training made available.

Alternate criminal justice measures

198. Where Singapore is unable to secure an ML conviction, they will consider prosecuting offenders for other offences (e.g. dishonestly receiving stolen property). Between 2011 and 2014, eight offenders have been convicted of dishonestly receiving stolen property. If the facts of the case do not suggest that an alternative criminal charge is appropriate, SPF will, in consultation with AGC, issue a Letter of Warning. Where a suspect has absconded, Singapore may also pursue confiscation of their proceeds of crime and provided a case example demonstrating this.

199. For cases of foreign predicate offending, Singapore also demonstrated it brought such cases to its foreign partners' attention to enable them to pursue criminal investigations in their jurisdictions.

200. ***Singapore has achieved a moderate level of effectiveness for IO.7***

Immediate Outcome 8 (Confiscation)

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

201. Singapore did not demonstrate that confiscation is a key priority in Singapore's criminal justice regime or pursued as a policy objective, although Singapore has made operational and policy changes to promote asset seizure and confiscation (see below). The assessors felt that the LEAs do not focus on seizing and confiscating proceeds of crime as a goal in itself and there are few policies to promote confiscation as an integral mechanism to deprive criminals of their illicit wealth. This is apparent in the low level of confiscations, although asset seizures are considerably higher, as well as the lack of use of the asset seizure and confiscation powers in the CDSA.

202. A contributing factor may be the lack of overarching strategic direction. Singapore's whole-of-government AML/CFT policy statement[41] does not explicitly include confiscation as a policy

[41] MOF (nd), Singapore's AML/CFT Policy Statement www.mof.gov.sg/Policies/Anti-Money-Laundering-Countering-the-Financing-of-Terrorism-AML-CFT/Singapores-AML-CFT-Policy-Statement.

objective. During the on-site, CAD released a formal AML policy statement and strategy[42] that include asset confiscation as a desired outcome. This is a positive development, but is too new to have an impact in this evaluation. It should help provide CAD with a strategic direction in the future.

203. Since 2013, Singapore has made operational and policy changes to promote asset seizure and confiscation. All agencies' ML referral SOPs with CAD note the importance of seizing property to prevent the dissipation of assets. CAD has also established a specific Asset Confiscations Branch to conduct concealed income analysis for other LEAs and competent authorities. This has promoted asset seizure as an objective in ML investigations; accordingly the majority of Singapore's seizures and confiscations relate to ML. The new Organised Crime Act will also allow for the confiscation of assets relating to organised crime on a non-conviction basis on the civil standard of proof (i.e. on a balance of probabilities). The effective implementation and use of this regime should help Singapore's pursuit of the proceeds of crime.

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

i. Proceeds of crime

204. The CDSA sets out a seizure and confiscation framework for Singapore. The LEAs rarely use the CDSA seizure and confiscation provisions in practice. The specific forfeiture powers under the CDSA have only been used to confiscate proceeds of crime in two ML and 10 predicate offence cases since 2011. Instead, LEAs primarily use the CPC to seize and confiscate proceeds of crime due to its minimal procedural requirements. The CDSA powers require a court order, while the CPC allows authorised officers to seize assets without resorting to the courts. The LEAs also make some use of other acts (Customs Act, Immigration Act, Misuse of Drugs Act (MDA) and Prevention of Corruption Act (PCA)) in specific predicate investigations.

205. The CPC offers obvious advantages to LEAs, as it enables Singapore to very rapidly seize assets and prevent their dissipation. Singapore provided examples where they have frozen bank accounts in just a few hours after receiving a foreign request for assistance. However the CPC's powers are primarily focused on securing evidence of offending rather than taking the profit out of crime. The CPC also only allows confiscation of proceeds directly linked to the offence for which a person is convicted for. The CDSA allows for the confiscation of proceeds of crime not directly linked to an offence, but the LEAs have made little use of its powers. The LEAs should make greater use of the CDSA to ensure a wider range of proceeds of crime is confiscated.

[42] Singapore Police Force (nd), AML Policy Statement and Strategies, http://www.police.gov.sg/about-us/organisational-structure/specialist-staff-departments/commercial-affairs-department/aml-cft/aml-policy-statement-and-strategies

Table 12. **Seizures by Act (in SGD)**

Act	2011	2012	2013	2014	Total
CPC	70 800 000	42 200 000	122 500 000	68 000 000	303 500 000
Customs Act	2 200 000	2 070 000	2 010 000	2 500 000	8 780000
Immigration Act	0	100 000	100 000	100 000	300 000
MDA	450 000	730 000	680 000	490 000	2 350 000
PCA	500 000	800 000	240 000	0	1 540 000
CDSA	23 000 000	2 300 000	0	0	25 300 000
Total	**96 950 000**	**48 200 000**	**125 530 000**	**71 090 000**	**341 770 000**

Table 13. **Confiscation by Act (in SGD)**

Act	2011	2012	2013	2014	Total
CPC - restituted	1 400 000	13 500 000	6 900 000	10 200 000	32 000 000
CPC - forfeited	700 000	200 000	900 000	1 200 000	3 000 000
CDSA	500 000	0	100 000	0	600 000
MDA	0	100 000	0	300 000	400 000
PCA	363 000	1 319 000	2 002 000	1 423 000	5 107 000
Customs Act	1 600 000	1 600 000	1 800 000	1 500 000	6 500 000
Immigration Act	0	100 000	100 000	0	200 000
Total	**4 563 000**	**16 819 000**	**11 802 000**	**14 623 000**	**47 807 000**

206. Between 2011 and 2014, Singapore has seized (frozen) a total amount of SGD 342 million (approx. EUR 31.1 million or USD 35.3 million) and confiscated SGD 48 million (approx. EUR 208.4 or USD 221.8) of assets. Singapore has focused mainly on seizing currency relating to domestic cheating and CBT cases and ML cases relating to foreign corruption and cheating (90% of seizures made between 2011 and 2014). These seizures comprise 2,002 individual cases between 2011 and 2014 (an average of 500 cases a year). The majority of confiscations relate to cash to be returned to foreign and domestic victims of frauds (66% of confiscations between 2011 and 2014). These confiscations comprise 1 004 cases (an average of 250 cases a year).

207. The amount seized and confiscated since Singapore's last MER and the number of cases in which seizure and confiscation has occurred has slowly increased with each year. Confiscations peaked in 2012, which Singapore attributed to more aggressive action by LEAs, however figures have tapered off since then. Nevertheless, the total seems low in light of Singapore's risks and context. Of particular concern is the very low number of confiscations. Only 14% of assets seized between 2011 and 2014 have been confiscated. Singapore advised that majority of the seizures are still pending the completion of investigations and that funds were sometimes released due to the lack of support from foreign counterparts. However the low level of confiscations and high proportion of seized funds that Singapore has released back to the subjects indicates Singapore could do more to proactively confiscate proceeds of crime.

Table 14. **Seizures and confiscations in relation to ML cases only by year of seizure, in SGD millions[1]**

	2008	2009	2010	2011	2012	2013	2014	*Total*
Amount seized	29.1	8.1	68.5	63.1	21.5	116.9	40.6	*347.7*
Amount confiscated[2]	23.9	1.5	13.2	4.3	6.3	8.8	2.1	*59.9*
Amount released to subjects	0.3	5.5	54.6	0.9	0.0	0.8	1.0	*63.6*
Amount still under seizure	4.9	1.1	0.7	57.9	15.2	107.3	37.5	*224.1*

Table notes:

1. These figures are for seizures relating to ML cases only, which is why they are less than the figures reported above. They also extend to 2008, whereas Singapore only commenced collecting broader statistics relating to asset seizure and confiscation in 2011.

2. This is the amount of proceeds seized from that year that was subsequently confiscated.

208. The authorities stated that responding to foreign requests for confiscation of foreign proceeds was a high priority. Singapore's policy is to seize the funds immediately if there is sufficient evidence to suggest that the funds are criminal proceeds, regardless of whether the predicate offence has been committed in Singapore or overseas. Singapore provided a number of case examples where it responded quickly and efficiently to formal and informal international cooperation requests. Singapore has shared SGD 7.5 million (approx. EUR 4.94 million / USD 5.26 million) of confiscated proceeds with foreign partners since 2011, all of which relates to ML cases. Case example 7 is a good example of what Singapore can do when another country seeks assistance. Singapore's LEAs however could also take a more proactive approach themselves to ensure it does not become a safe haven for foreign proceeds.

209. Singapore noted however the inherent difficulties involved in transnational investigations and advised that SGD 56 million (approx. EUR 36.94 million / USD 39.32 million) of funds seized domestically between 2008 and 2014 had to be released back to the subjects due to reasons beyond the control of the domestic LEAs. Lack of information from the foreign LEA providing evidence of the predicate offending meant funds had to be released in four cases. Singapore should consider measures to enable the LEAs to better confiscate proceeds of crime in such circumstances. This could include using the civil confiscation regime established by the future Organised Crime Act or implementing unexplained wealth laws which reverse the burden of proof on the individual to demonstrate that the funds in question are not proceeds of crime. Singapore should also consider expanding the confiscation regime established by the Organised Crime Act beyond organised crime situations to enable the LEAs to target proceeds not linked to organised crime (e.g. corruption). This would enable Singapore to better pursue proceeds of crime where sufficient evidence of offending is difficult to obtain. The LEAs should also work to improve their cooperation with key foreign partners to address these issues (see IO.2).

Case Example 7. **Seizure of assets relating to foreign predicate**

The US and Hong Kong, China were conducting an investigation on Person Q for ML offences. Person Q, the director of a state organization in China, was alleged to have embezzled funds amounting to CN¥ 237 million (approx. SGD 38.7 million / EUR 25.52 million /USD 27,17 million). The criminal proceeds were alleged to have been transferred to overseas bank accounts including Hong Kong, China; Singapore and the United States.

The US authorities then informed CAD that both the US and Hong Kong, China authorities were investigating Person Q. In June 2014, Hong Kong, China wrote to CAD and sought its assistance to consider seizing the bank accounts of Person Q in Singapore. In order to prevent the dissipation of funds by Person Q when any one jurisdiction takes unilateral action first, it was proposed that Hong Kong, China, Singapore and other relevant jurisdictions conduct a joint operation to seize Person Q's assets simultaneously.

In August 2014, CAD commenced a domestic ML investigation and, acting in tandem with US and Hong Kong, China authorities, seized about SGD 14.8 million (approx. EUR 9.76 million or 10.39 million) of suspected criminal proceeds. The investigation was ongoing at the time of the on-site.

210. Singapore's effort to pursue restitution to victims of frauds is a positive aspect of its confiscation regime. Nearly 90% of Singapore's confiscation cases under the CPC between 2011 and 2014 (59 out of 66) involved restitution to a victim.

211. Singapore included tax crime as a predicate for ML in 2013 Singapore has used its taxation regime on a few occasions to target proceeds of crime and IRAS is reviewing how the taxation framework could be used to do so for more cases. Continued engagement between CAD and IRAS should help improve this understanding. CAD and IRAS should focus in particular on how best to target the proceeds of foreign tax crime and whether this is best pursued through the confiscation or tax framework. Outside of the confiscation framework, Singapore has fined offenders substantial sums under the Income Tax Act and Goods and Services Tax Act (SGD 49 million or EUR 32.32 million or USD 39.32 million) in the two years since including tax crime as a predicate).

ii. Non-cash assets, property of equivalent value and instrumentalities

212. As Singapore's major risks relate to foreign predicate offending, it is more likely that the proceeds located in Singapore will be funds in bank accounts. This is reflected in Singapore's results, where the vast majority of seizures relate to funds. Singapore provided a number of case examples where such assets (e.g. luxury watches and bags) were seized, and in some cases, confiscated. Between 2011 and 2014, 6.4% percent of Singapore's seizures were for non-cash assets, which included 27 vessels, 200 kilograms of gold and silver and 12 properties. In the same period, Singapore also confiscated non-cash assets, which included 18 vessels and 3 properties. .Singapore also provided a number of case examples where contraband cigarettes and illicit narcotics were also seized. Singapore has not considered seizing a business before, but should consider such action in appropriate cases.

213. Singapore has seized SGD 8.6 million (approx. EUR 5.67 million / USD 6 million) and confiscated SGD 5.3 million (approx. EUR 3.5 million / 3.72 million USD) worth of property of equivalent value between 2011 and 2014 (which includes cash and non-cash assets such as real

estate and luxury watches). CAD's Asset Confiscation Branch has used concealed income analysis in 10 cases to proactively identify income criminals have accumulated which they could not satisfactorily account. However, the very sparse use of the CDSA provisions indicates that the seizing of property of equivalent value is not routinely pursued.

214. All of Singapore's efforts to pursue the instrumentalities of crime relate to the seizure and confiscation of vehicles used in the commission of offences in Singapore. Between 2011 and 2014, Singapore seized 1 360 vehicles valued at SGD 8.72 million (approx. EUR 5.75 million or 3.72 million USD) and confiscated 648 vehicles valued at SGD 7.4 million (approx. EUR 4.88 million or 5.19 million USD). Authorities noted challenges in successfully confiscating vehicles if they were hired vehicles, as it would be harsh to punish the rental company if it was not complicit in the crime. Singapore should pursue a wider variety of instrumentalities.

Case Example 8. **Seizure of instrumentalities of crime**

In 2012, Singapore Customs mounted an operation to intercept targeted prime-movers used to smuggle contraband cigarettes out of one of Singapore's major ports.

Two Singaporeans were arrested in the operation. A total of 1 000 cartons of duty unpaid cigarettes worth more than SGD 11 000 (approx. EUR 7 256 / USD 7 723) were seized. The total amount of duty and Goods and Services Tax evaded exceeded SGD 95 000 (approx. EUR 62 662 / USD 66 700).

Two prime-movers, being instrumentalities of the crime and cash were seized by Customs. Investigations established that one of the prime movers and some of the cash which were seized were instrumentalities and proceeds of crime, respectively. The cash, cigarettes and one of the prime movers that were seized were successfully forfeited.

iii. Property moved offshore

215. Singapore does not generally pursue funds that move offshore through formal channels Singapore has successfully confiscated funds that have moved offshore only on one occasion, where SGD 16 000 (approx. EUR 10 554 / USD 11 234) was confiscated as a result of a Singaporean request. Singapore advised that it has reached out to its foreign counterparts through informal channels to pursue funds that move offshore on occasion, but has had little success in recovering money. While Singapore's low domestic crime rate may reduce the amounts of domestic proceeds moving out of Singapore, the LEAs could do more to 'follow the money' when it moves out of Singapore, including by making greater use of the formal MLA framework and improving its cooperation with key foreign counterparts.

iv. Asset management

216. Singapore's main LEAs have SOPs and procedures in place that set out strict guidelines on the procedures for seizure, tracking, storage, withdrawal and disposal of case properties. To ensure that these processes remain sound and efficient, SPF, the Ministry of Home Affairs and the Accountant General's Office conduct regular audits on accounts and records. In addition, a register of all seized assets is maintained and reported to the Magistrate when the seized assets are no longer relevant for the purposes of investigations, inquiries, trials or other proceedings, or one year from

the date of seizure, whichever is earlier. The authorities did not note any significant problems with asset management.

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

217. Singapore's cross-border cash movement reporting regime (CBCRR) requires that all cross-border movements of physical currency and BNIs over a SGD 20 000 (approx. EUR 13 192 or USD 14 042) threshold be reported to the Immigration and Checkpoints Authority (ICA) and STRO. Breaches of the CBCRR are referred to CAD for investigation and the reports (Cash Movement Reports – CMRs) are forwarded to STRO. A SOP is in place to guide this process.

218. Singapore's current CBCRR has been in place since 1 Nov 2007 STRO receives approximately 65 000 CMRs a year. Approximately 60% of those are submitted by travellers, with remaining 40% submitted by senders, carriers and recipients of physical currency and BNIs. Singapore has enhanced the CBCRR including by reducing the reporting threshold from SGD 30 000 (approx. EUR 19 788 / USD 21 063) to SGD 20 000 (approx. EUR 13 192 / USD 14 042) to bring it in line with Recommendation 32. The requirement to make a CMR is included on arrival cards. Assessors noted signage at the airport advising of the reduction in the threshold and requirement to report. Substantial signage was also observed at the casinos advising patrons of their requirement to make CMRs if they are carrying cash of greater than SGD 20 000 (approx. EUR 13 192 / USD 14 042) out of Singapore.

Table 15. **Number of CMRs made (all sources)**

Year	2008	2009	2010	2011	2012[1]	2013	2014	Total
Total number of CMRs made	97 040	92 529	92 529	100 427	85 012	66 301	64 173	**598 011**
Total value of CMRs (SGD)	Not available	Not available	Not available	Not available	Not available	136 billion	106 billion	**242 billion**
Average value of CMR (SGD)	*Not available*	*Not available*	*Not available*	*Not available*	*Not available*	*205 125*	*165 178*	***185 151***

Table notes:

1. Prior to 2012, CMRs received is counted based on the number of physical forms received. As a single transaction may have more than one form, this led to the higher numbers prior to 2012.

Table 16. **Number of CMRs made by travellers**

Year	2008	2009	2010	2011	2012	2013	2014	Total
Total number of CMRs made by travellers	38 274	40 350	40 350	51 368	43 669	45 135	38 852	**297 998**
Total value of CMRs (SGD)	Not available	Not available	Not available	26 billion	27 billion	25 billion	22 billion	**100 billion**
Average value of CMR (SGD)	*Not available*	*Not available*	*Not available*	*500 000*	*627 000*	*554 000*	*576 000*	***564 250***

Table Notes:

1. Prior to 2012, CMRs received is counted based on the number of physical forms received. As a single transaction may have more than one form, this led to the higher numbers prior to 2012.

219. ICA stated that all luggage was x-rayed at land and sea checkpoints for currency and BNIs. Security risk profiling is also conducted on all land and sea travellers, with selected passengers undergoing thorough physical checks. For airport checkpoints, ICA conducts random checks on the baggage of air travellers and screens passengers disembarking from selected flights originating from red-flagged airports. Security risk profiling is conducted on air travellers, with selected passengers undergoing thorough physical checks and x-rays. Intelligence received from domestic and international partners feeds in to ICA's targeted screening of high risk travellers. ICA also has certain red flag indicators to profile high ML/TF/CMR risk travellers. ICA officers also receive training on identifying high risk travellers. Cases of false or non-declaration are referred to CAD for investigation, which has a specialist team to investigate these cases.

Table 17. **Detection of breaches of CBCRR requirements**

Detection	2008	2009	2010	2011	2012	2013	2014	Total
Number of non-declarations	43	41	69	62	70	55	85	425
Number of false declarations	2	3	1	2	0	0	2	10
Total	**45**	**44**	**70**	**64**	**70**	**55**	**87**	**435**
Total amount seized (SGD)	7 549 717	7 462 005	16 324 294	8 402 059	8 916 360	7 811 225	8 768 304	65 233 964
Cash	7 535,841	6 701 486	15 938 694	8 165 781	8 916 360	7 666 465	8 768 304	63 692 931
BNIs	13 876	760 519	385 600	236 278	0	144 760	0	1 541 033
Average per detection (SGD)	**167 771**	**182 000**	**240 063**	**131 282**	**146 170**	**153 161**	**100 785**	***160 176***

220. Despite these measures, the assessors did not consider that the CBCRR was being effectively implemented to dissuade the laundering of physical currency and BNIs. Singapore does not pursue cash detection, or detection of related ML/TF, as a priority. While failures to declare and false declarations have been detected, Singapore has not detected any ML arising from currency that is declared at the border. The LEAs do not proactively investigate declarations of substantial sums of currency for suspicions of ML.

221. Singapore has detected 435 breaches of the CBCRR between 2008 and 2014 and has seized SGD 65 million (approx. EUR 42.9 million / USD 45.6 million) in associated cash and BNIs. From all the detections at checkpoints, Singapore has not identified any suspect ML/TF activity. This seems very anomalous in light of Singapore's risk and context. Singapore received over 15 million international visitors in 2014 and is one of the world's major trade and transport hubs. Its proximity to countries with substantial ML/TF risks makes it vulnerable to cash couriers seeking to move illicit funds into Singapore. Overall, Singapore considered the physical cross-border movement of illicit funds to have a medium ML/TF risk.

222. Singapore has detected and investigated 18 cases of non-declaration, where the breach was detected in a domestic ML investigation after the breach had occurred. This indicates ICA is not sufficiently detecting breaches of the CBCRR. Further, ICA had not followed-up to understand how the breaches had occurred. CAD and ICA should improve cooperation and information sharing to better investigate breaches of this kind

223. Where breaches of the CBCRR are detected at the border, the authorities' policy is to not pursue confiscation. Instead, breaches are pursued by criminal prosecution. Singapore does not generally pursue confiscation in addition to criminal prosecution, as the authorities considered this would be disproportionate to the nature of the crime. As Singapore has not detected any ML relating to declared currency, it is not clear whether Singapore would pursue confiscation in such circumstances. Singapore has confiscated SGD 2 million (approx. EUR 1.32 million or USD 1.40 million) of the SGD 65 million (approx. EUR 42.9 million or USD 45.6 million) seized, however this relates entirely to ML investigations where a breach of the CBCRR is later identified and the cash was linked to criminal activity.

Table 18. **Prosecutions and convictions for breaches of the CBCRR**

Action	2008	2009	2010	2011	2012	2013	2014	Total
Number of persons prosecuted for breaches of the CBCRR								
N° prosecutions into false declaration	0	2	0	0	0	0	0	**2**
N° prosecutions into non declaration	2	14	7	7	7	10	21	**68**
Total	2	16	7	7	7	10	21	**70**
Number of persons convicted for breaches of the CBCRR								
N° convictions for false declaration	0	2	0	0	0	0	0	**2**
N° convictions for non-declaration	2	14	7	6	7	10	18	**64**
Total	2	16	7	6	7	10	18	**66**
Fines levied on convicted persons								
Total (SGD)	37 000	112 000	398 000	40 000	79 000	101 000	50 000	**817 000**
Average (SGD)	18 500	7 000	56 857	6 667	11 286	10 100	2 778	**16 169**

224. More serious breaches of the CBCRR are prosecuted and convicted offenders may be imprisoned and/or fined. Singapore has convicted 66 people for breaches of the CBCRR. Singapore considers the criminal sanctions imposed to be effective, as Singapore has not observed any case of reoffending. However offenders have had an average fine of SGD 12 379 (approx. EUR 8 165 or USD 8 691) imposed for breaches. This is a very low number and is unlikely to be sufficiently dissuasive or proportionate. The 369 individuals not prosecuted had no sanction placed on them, as there is no civil penalty available such as an administrative fine (they instead receive a letter of warning from SPF). These cases typically relate to smaller sums of money and where investigations revealed offenders were not aware of the reporting obligation and the funds were not linked to criminal activities. In such cases, a written warning may be issued in lieu of prosecution. Nevertheless the lack of a range of sanctions (e.g. a civil or administrative penalty) prevents the imposition of proportionate sanctions on offenders.

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

225. Singapore considers its high risk domestic ML predicates to be UML, cheating and CBT and high risk foreign ML predicates to be cheating and corruption. Approximately 56% of the assets seized and confiscated by Singapore relate to these key threats, indicating consistency with Singapore's assessment of its risks. In particular, approximately a quarter of Singapore's confiscations relate to domestic cheating and foreign cheating (through shell companies, money mules and wire transfers). UML seizures and confiscation remain low due to the low level of sums typically involved.

226. Singapore has made relatively substantial seizures in relation to foreign corruption (SGD 123 million / EUR 81.13 million/ USD 86.91 million) between 2011 and 2014). Only SGD 4 million (approx. EUR 2.64 million / USD 2.80 million) has been successfully confiscated and repatriated to its source country. Singapore explained that this is because the vast majority is still seized pending investigation (SGD 119 million EUR 78.49 million/ USD 83.55 million). Nevertheless, the amount confiscated remains low and Singapore could take more proactive action to confiscate the proceeds of foreign corruption by improving its engagement with key foreign counterparts.

227. Moderate limitations in Singapore's understanding of its nexus with foreign predicate ML risks may also have a limited impact on its ability to seize and confiscate the associated proceeds of crime (see IO.1 for further information).

228. The lack of confiscation in relation to breaches of the CBCRR does not seem commensurate with the risks Singapore faces as a major transport hub.

229. ***Singapore has achieved a moderate level of effectiveness for IO.8***

CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

Key Findings and Recommended Actions

Key Findings

TF offence (Immediate Outcome 9)

1. Singapore has demonstrated that it has a general understanding of its TF risks. . Nevertheless, there remain gaps. In particular, the methodology used in the NRA to assess and allocate TF risk ratings to sectors and activities is unclear. Moreover, Singapore's reliance on domestic indicators of risk has hindered its ability to appreciate the inherent TF risks associated to its geographical location and its status as one of the world's largest financial centres. Singapore refers all TF matters to ISD for intelligence-related investigations. ISD investigations are not financial investigations.
2. TF-related offences are not investigated criminally; CAD's involvement when requested by ISD is only to assist ISD in its intelligence-related investigations into TF (which are not criminal in nature).
3. CAD has been involved in 413 TF and terrorism investigations assisting ISD since 2008 but none have resulted in any prosecutions (and consequently no convictions) for TF. No financial information has been provided by Singapore in relation to the nature of the 413 cases.
4. Singapore lacks a comprehensive TF strategy that integrates the roles of the ISD and CAD in relation to terrorist financing. There is also little evidence that Singapore routinely pursues parallel financial investigations with CT investigations.

Targeted financial sanctions related to TF (Immediate Outcome 10)

1. Singapore has demonstrated that targeted financial sanctions pursuant to UNSCR 1267 and its successor resolutions are properly implemented. Listing in Singapore is automatic after UN designation and without delay.
2. Singapore has also been implementing UNSCR 1373 but the team could not assess the effectiveness regarding foreign designated terrorists because Singapore has not yet received any formal request for designation pursuant to UNSCR 1373 from foreign jurisdictions. However, Singapore has received requests through informal channels and assessed the request in the same manner as it would do with a formal request.
3. Financial institutions and all types of DNFBPs, except PSMDs, are well aware of TF freezing obligations and appear to effectively implement their obligations on TF sanctions.
4. Given the significant trading volume by PSMDs, the fact that a large portion of PSMDs are not subject to the full range of AML/CFT obligations has a negative impact on the implementation of existing TF sanctions obligations.
5. MAS has created an e-mail alert system for FIs and the broader public, including DNFBPs, to receive updates to various UN sanctions list. This system appears to be effective for FIs and also to a lesser extent for all types of DNFBPs, except PSMDs.

4

Non-profit organisations (Immediate Outcome 10)

1. Singapore demonstrated a strong capacity to obtain information on its NPO sector which has allowed it to reasonably assess which organisations are at risk of terrorist financing abuse, based on their activities and characteristics. However, the inherently high vulnerability of NPOs to TF abuse is lost in Singapore's NRA report, which only addresses residual risk. Singapore's low risk rating is hindered by a reliance on domestic cases as an indicator of risk and a lack of a comprehensive domestic risk assessment.
2. Singapore's competent authorities have appropriate regulations and enforcement powers in place to safeguard NPOs from TF abuse however Singapore has not implemented a targeted approach in doing so. Oversight of NPOs is restricted to good governance reviews. While Singapore has recently added an AML/CFT component to these reviews there are no targeted reviews based on any assessment of TF abuse risks.

Proliferation financing (Immediate Outcome 11)

1. Singapore has demonstrated that targeted financial sanctions (TFS) pursuant to UNSCR 1718, 1737 and their successor resolutions are properly implemented. Listing in Singapore is automatic after UN designation and without delay. The e-mail alert for sanctions list from MAS seems to be effective, both for FIs and to a lesser extent for all types of DNFBPs, except PSMDs.
2. Financial institutions and all types of DNFBPs, except PSMDs, understand well and effectively implement obligations of proliferation financing.
3. Singapore demonstrated a robust information sharing mechanism among relevant authorities in charge of export control, financial supervision, intelligence and law enforcement. The Iran Prohibition Notice further assisted to create awareness, although this may have worked as a driver of de-risking. In practice, Singapore approved four cases where financial institutions used a clause in the Notice to seek approval to exempt certain transactions from the prohibition. The Prohibition Notice was cancelled with effect from 28 January 2016, following the arrival of Implementation Day (16 January 2016) pursuant to the Joint Comprehensive Plan of Action (JCPOA).

Recommended Actions

TF offence (Immediate Outcome 9)

1. Conduct specific TF risk assessments taking into account risks in the region and with neighbouring countries as well as domestic factors.
2. Have a clearly defined set of definitions of "low risk", "medium risk" and "low to medium risk" as well as "high risk" in relation to TF and a clear set of criteria for assigning risk ratings in the appropriate circumstances.
3. When STRs disclose possible TF offences, even if terrorism offence allegations are involved, the CAD should investigate the TF allegations in the first instance.
4. Parallel financial investigations should occur with all CT investigations whether or not these lead to TF charges.
5. Establish a clear strategy for managing TF matters - between CAD, ISD and others – when it is

appropriate to use criminal justice measures and when appropriate to use alternate measures.

Targeted financial sanctions on TF (IO.10) and financing of proliferation (IO.11)

1. Singapore should continue its current robust implementation of the targeted terrorist and proliferation financing measures pursuant to UNSCRs.
2. Singapore should ensure that remaining PSMDs (in addition to those with pawnbroker's license) become subject to AML/CFT preventive measures and regulation and ensure that these PSMDs effectively implement the targeted financial sanctions for both TF and PF.
3. Singapore should further improve the communication related to TFS across all DNFBP sectors, in particular the PSMDs.

NPOs (IO.10)

1. Singapore should conduct a comprehensive sector review to better understand the types of organisations within the NPO sector that are inherently vulnerable to TF abuse and continue outreach to NPOs to raise awareness of specific TF abuse risks.
2. Singapore's competent authorities responsible for NPOs should work more closely with the Internal Security Department in order to better assess the risks of and detect TF abuse of NPOs and should commence examinations targeted at protecting NPOs from the threat of TF abuse.

230. The relevant Immediate Outcomes considered and assessed in this chapter are IO9-11. 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 consisten with the country's risk-profile

231. While Singapore has a general understanding of its TF risks, Singapore's assessment of regional TF vulnerabilities should be further improved.

232. The methodology used to assess TF risk in Singapore examines both domestic and foreign TF risk against whether actual cases have arisen in Singapore. For domestic TF risk, Singapore notes that with the disruption of the JI network in 2001 there have been no cases of domestic TF detected. For foreign TF risk the assessment process noted that while there is a possibility of self-radicalisation of individuals who may donate money for overseas conflicts, and that Singapore might be used as a transit point for terrorist financing, there is no evidence that this is actually occurring. Moreover, Singapore acknowledges that there is a large foreign community in Singapore which could encourage foreign terrorist groups to use Singapore as a base for terrorism fund raising amongst their own nationals. Authorities are also aware that Singapore continues to be a potential target for terrorism.

233. TF is considered by government agencies as ´low/medium risk´ as follows:

- Domestic-source TF risk is "low to medium;"
- Foreign-source TF risk is "medium."

234. It is not clear in the NRA (no definition is provided), nor was it made clear in discussions with officials during the on-site visit:

1) what the meaning of "low risk," "medium risk" and "low to medium risk" is in relation to TF; and
2) how the attribution of those ratings was made in relation to domestic and foreign TF.

235. Singapore acknowledges that it is in close proximity to a number of countries with a high risk of TF and that the recent phenomenon of ISIL and its aggressive global fund raising activities is a regional concern at the least. But Singapore indicates that while it has examined both of these issues, neither has the effect of increasing the overall TF risk profile in Singapore, notwithstanding that there are recent cases involving self-radicalization of Singaporeans in relation to ISIL propaganda and cases have been detected (figures below).

236. On the other hand, some private sector agencies felt that TF risk in Singapore has, in reality, changed as a result of recent developments (in particular the threats posed by ISIL and the real risk of its development in the region close to Singapore) and that the risk in Singapore of both domestic and foreign TF is now higher than it was assessed in 2014.

TF identification and investigation

237. In Singapore TF is linked to terrorism through a national security policy framework. Singapore's enforcement strategy is to use the Internal Security Act and ISD to pursue TF activities. STRs that disclose TF activities are referred to the ISD; preventive and other ISD powers are used to address TF.

238. Singapore authorities made it clear that ISD is the front line agency for TF and that if TF cases are detected by law enforcement (CAD) those cases are referred to ISD for intelligence investigation under their Internal Security Act in the first instance. A *Guideline on Delineation of Responsibilities Between Internal Security Department and Commercial Affairs Department* for managing issues under the TOSOFA, dated 26 April 2013, articulates the responsibilities of both departments in relation to TF and other terrorism offences and provides that "ISD is the lead agency for all investigations into terrorism and /or terrorism related offences" (para 3). Furthermore, "*as TF is invariably linked to terrorism, CAD will conduct investigations into TF but only at the written request of ISD…*" (para 4). TF investigations by ISD do not include financial investigations. Under the Guideline noted above, financial investigations are not conducted by ISD, but by CAD in coordination with ISD as the lead agency.

239. The assessment team understands from Singapore authorities that if, on investigation, ISD determines that a TF case involves a "pure TF offence" (i.e. an allegation of TF unrelated to a terrorist act) then ISD will refer the case to CAD with no further involvement of ISD (although this is not consistent with the *Guideline* cited above). On the other hand, if ISD determines that allegations of terrorist acts are disclosed in any TF-related intelligence investigation, then ISD retains investigatory responsibility for the matter. Whatever the informal arrangements are between ISD and CAD outside the scope of the cited Guideline, it is clear from the statistics below and from discussions with

authorities that there have not been any separate and independent TF criminal investigations by CAD for TF in Singapore. CAD investigations are always to be in support of ISD. Nor have there been any "pure TF cases" referred by ISD to CAD.

240. The following table provided by Singapore shows the total number of investigations undertaken by ISD since 2008 into TF and terrorism cases:

Table 19. **Total number of TF and terrorism investigations by ISD since 2008**

	2008	2009	2010	2011	2012	2013	2014	Total
No. of CT/TF investigations	220	152	149	72	52	59	76	**780**
No. of TF investigations	38	15	8	6	7	6	7	**87**
No. of investigations into suspected TF activities that resulted in designation action	0	2	0	2	0	1	0	**5**
No. of TF investigations resulted in alternative enforcement action - travel control restriction	36	5	5	3	4	4	5	**62**
No. of TF investigations where no further action was taken pending further developments	2	8	3	1	3	1	2	**20**

241. A total of 780 cases involved both TF and terrorism offence allegations over the seven year period from 2008 to 2014, inclusive. of this figure:

- Five cases led to terrorist designations under UNSCR 1373; and
- 87 were TF-related investigations.

242. The following statistics are relevant:

Table 20. **Number of TF STRs disseminated since 2008**

	2008	2009	2010	2011	2012	2013	2014	Total
STRs disseminated leading to ISD TF investigations	**30**	**42**	**64**	**61**	**99**	**128**	**114**	**402**
No. of STRs on suspected TF activities disseminated that are linked to cases where enhanced monitoring actions were taken against the subjects of concern	1	3	3	5	6	3	5	26
STRs on suspected TF activities - no further action taken due to insufficient evidence of TF	18	25	46	35	74	114	91	403

243. According to these figures, 538 TF-related STRs were referred to ISD from 2008 to 2014 (inclusive) leading to intelligence-related investigations.

244. ISD has a specialised team of investigators for TF, but the assessment team was advised that most of the STRs are "false positive" name investigations only and do not involve evidence collection for the purpose of a criminal justice response with a view to a possible criminal prosecution.

245. To guide ISD intelligence investigators in determining if there is any TF activity involved, ISD investigators complete a document known as the "Proforma for Detection of Possible Terrorism Financing". This document guides investigators to look out for information that indicates possible TF activities. In addition, ISD's TF investigators engage other specialist units within ISD that possess specialised investigative and intelligence gathering capabilities to conduct holistic investigations. To facilitate TF investigations, the team also has access to resources that allow it to gather financial intelligence and conduct checks with FIs and other relevant entities.

246. Of the 780 case leads, other than clearing false positive name matches, it does not appear that financial investigations were ever done in relation to any of the TF cases. Also, there is no indication that the investigation of the ten Singaporeans radicalised by ISIL propaganda since 2014 involved financial investigations.

247. ISD's intelligence gathering capabilities under the Internal Security Act include police powers (name screening, recording of statements, searches, and seizures etc.) and STR analysis to track leads from TF-related information. In some cases ISD has sought the assistance of CAD to investigate TF and terrorism cases however in those cases CAD acts in a subordinate role in support of ISD pursuant to the *Guideline on Delineation of Responsibilities Between Internal Security Department and Commercial Affairs Department* of 2013. Over the same seven year period, ISD has requested CAD in 413 (of the 780) cases to assist ISD with investigations involving either TF, terrorism or both.

248. The following table breaks down these statistics by year:

Table 21. **No. of CT/TF investigations where CAD's assistance was sought**

		2008	2009	2010	2011	2012	2013	2014	Total
	Total No. of CT/TF investigations where CAD's assistance was sought	85	40	79	62	36	43	68	413
Case Outcomes	Designation	0	0	1	1	1	2	2	7
	Alternative enforcement actions	65	25	55	36	10	11	21	223
	No further action pending new developments	20	15	23	25	25	30	45	183

249. Of the 413 TF and terrorism cases Singapore advised that:

- 109 involved foreign entities; and
- 301 involved domestic entities.

250. Under the *Guideline* referred to above (outlining the responsibilities of both departments), ISD and CAD cooperate on a case-by-case basis, but the "outcomes of CAD's financial investigations would be forwarded to ISD as possible leads for ISD's further investigation." CAD's involvement appears to stop at that point with no criminal TF investigation by CAD. On the information provided, no criminal investigations independent of ISD's involvement have yet been undertaken – CAD's involvement is to assist ISD, not to act independently in its own criminal investigations. As a consequence, no criminal prosecutions for TF have yet been undertaken in Singapore.

251. It is not clear what the nature of the 413 investigations were. No information has been provided by Singapore as to the nature or size of the funds involved (other than that the funds were "small"); whether the funds under investigation involved collection, use or movement; whether there were other criminal offences, including money laundering, involved, etc. Singapore has indicated (as stated above) that many TF investigations involve false positive name matches and the assessment team was of the view that the 413 cases were primarily about those issues (false positives).

252. In relation to cases involving ISIL, in particular, Singapore has indicated figures as follows:

Table 22. **Cases involving ISIL**

		2014	2015	Total
	No. of cases linked to ISIS	8	7	15
Case Outcomes	Dealt with under ISA	0	5	5
	Other actions taken	2	0	2
	Investigations are ongoing	6	2	8

253. In 2014 and 2015, 10 cases involved Singaporeans radicalised by ISIL propaganda and wanted to join, and fight, with ISIL. Of these, five were dealt with by administrative measures (detention) under the Internal Security Act and two involved "other action taken" (the action was not stipulated). Others are under continuing investigation. However, there is no information that financial investigations were undertaken in relation to the 10 self-radicalised individuals.

TF investigation integrated with -and supportive of- national strategies

254. As noted above, Singapore advises that 413 intelligence investigations conducted by ISD between 2008 and 2014 involved CAD but Singapore has yet to detect any confirmed case involving funds raised domestically or abroad for terrorism-related activities and little evidence of foreign funds flowing into or through Singapore for terrorist activities, persons or groups. Accordingly there have been no TF prosecutions.

255. Financial investigations related to terrorism (including stand-alone TF) only start from STRs and such investigations (whether or not they lead to TF charges) do not seem to be commenced as a matter of course either by ISD or CAD when there are CT inquiries/investigations. No financial investigations are undertaken in parallel with either CT investigations or ISD.

256. Singapore has taken preventative actions (detention and restriction orders) against a number of individuals and organisations in relation to terrorism. But Singapore does not consider TF criminal investigations connected with terrorist acts to be an appropriate response within its national security framework. Singapore's policy is to investigate TF (through ISD with the assistance of CAD) under TSOFA as an administrative matter, not a criminal one.

257. Singapore has indicated, however, that detention and restriction orders issued under the Internal Security Act amount to "criminal convictions" because such orders are treated as such for the purposes of the Registration of Criminals Act. However, although registration under the Registration of Criminals Act may occur in relation to administrative orders issued under the

Internal Security Act, those registrations do not amount to criminal convictions for the purpose of the FATF standards.

258. When offenders are also involved in terrorism-related (terrorist acts) activities, and the ISA is used to deal with any imminent or related security threats, the TF elements will form part of the grounds of detention (but not prosecution). As a consequence the terrorists' assets will simultaneously be dealt i.e., frozen.

4

Effectiveness, proportionality and dissuasiveness of sanctions

259. At the time of the on-site visit, there had been no prosecutions or convictions for TF offence, so no sanctions have been applied for the TF offence.[43]

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

260. As noted above, Singapore does not pursue TF cases through criminal investigations but through ISD (intelligence investigations) as part of its CT strategy. Singapore utilises measures in the ISA and the ISD to investigate and apply preventative (administrative) measures for TF offences only within its broader terrorism strategy. These penalties include preventative detention and restrictive orders. Of the 413 cases involving TF and terrorism, 223 involved "alternative enforcement actions" (administrative measures).

261. The strategy to use alternate measures, however, does not consider the practicability of securing TF convictions before the application of administrative measures occur. Singapore uses these alternate measures as its priority response.

262. ***Singapore has achieved a low level of effectiveness for IO.9***

Immediate Outcome 10 (TF preventive measures and financial sanctions)

Implementation of targeted financial sanctions for TF without delay

i. Implementation of UNSCR 1267 without delay

263. With regard to UNSCR 1267 and its successor resolutions, an individual or an entity designated by the UN Sanctions Committee is automatically referred to under Section 1 of the First Schedule of the TSOFA, and freezing-measures go into effect immediately upon designation by the UN Sanctions Committees. The members of the Inter-Ministerial Committee on Terrorism Designation (IMC-TD), which comprises relevant ministries and agencies and the MAS, provide a link to the UN Sanctions Committees on their websites. Financial institutions and most types of DNFBPs are encouraged to subscribe to the e-mail alerts on MAS' website to receive relevant UNSCRs updates, either for new designations or changes to previous designations. In practice, most of the DNFBPs have subscribed to the websites of the IMC-TD or MAS, but most types of DNFBPs indicated that they rely on commercial databases. Except for non-pawnbroker PSMDs, the competent

[43] Since the onsite, Singapore has reported the prosecution of 6 individuals for TF offences in May 2016. The assessment team was not able to discuss these issues with the authorities and is therefore unable to assess if these convictions are indeed relevant for IO.9.

authorities and SRBs for DNFBPs have close communication channels with financial institutions and DNFBPs to ensure that they are aware of updated lists and conduct proper screening of the designated persons. Between 2008 and 2014, Singapore has frozen USD 1 895 pursuant to UNSCR 1267 and its successor resolutions, and FIs have also reported false positives to the Government.

ii. Implementation of UNSCR1373 without delay

264. Singapore implements financial sanctions pursuant to UNSCR 1373 in two ways. One is a general prohibition based on the TSOFA. The TSOFA prohibits any dealing in property related to a terrorist or terrorist entity as defined in the TSOFA (s.2). This measure is not based on a list of designated persons. The other way is by updating a list of terrorists at the First Schedule (s.1A) of the TSOFA. Currently, 16 Singaporean individuals [as of 3 December 2015] are on the list. Singapore indicated that it designates terrorists regardless of nationality.

265. In addition, Singapore also implements financial sanctions through a non-public "alert list" of persons, which is made available to FIs and DNFBPs on a confidential basis. Assessors have reviewed this, but can share no further information due to the confidential nature of the list.

iii. Communication

266. The MAS obliges financial institutions to subscribe to the website of the MAS and to receive the updated lists of the designated persons. The competent authorities or self-regulatory bodies of DNFBPs also encourage individual DNFBP to subscribe to the MAS website. The subscription to MAS website by both FIs and some DNFBPs is verified through their regular on-site inspections by competent supervisors.

267. The MAS, the STRO and other competent authorities receive inquiries from financial institutions and DNFBPs on how to deal with screening against the list, especially when there is any doubt about possible false positives. With regard to the non-public list, the authorities also advise financial institutions and DNFBPs to contact them when a customer/transaction matches with the list. The competent authorities indicated that their advice covers how to proceed or not with the transactions with these customers based on an holistic analysis of the information available and to file an STR.

268. In Singapore, there are no competent authorities supervising PSMDs, except for those with a pawnbroker's license. Given this lacuna, it is not known to what extent the PSMD sector complies with the obligations pursuant to UNSCR 1267 and its successor resolutions and UNSCR 1373. Authorities have committed to enhance the supervision of this sector moving forward.

iv. Request from/to foreign authorities

269. For both UNSCRs 1267 and 1373, requests from foreign authorities are to be received by the MFA as a formal channel, and then the information is considered by the IMC-TD for designation. Singapore indicated it has not yet received any formal request for designation pursuant to UNSCR 1373 from foreign jurisdictions, but they have received requests through informal channels, and assessed the request in the same manner as they would be a formal request.

v. Review of 1373 list

270. The IMC-TD and other competent authorities constantly review and update the designations pursuant to UNSCR 1373.

vi. Response to claims by designated person

271. The IMC-TD is to review the designation if any appeal is made by a designated person. The IMC-TD has legal authority and publishes publicly known procedures for delisting individuals and entities. In case of UNSCR 1267 and its successor resolutions, the IMC-TD is to submit de-listing requests to the relevant UN Sanction Committees. A website of the IMC-TD and the MAS provide an explanation of the procedures.

vii. Implementation, Notification

272. In case financial institutions and DNFBPs have a match with the lists, they are obliged to inform the Commissioner of Police immediately (s.8 of the TSOFA), in addition to informing the relevant supervisors (e.g. MAS). Representatives of financial institutions and DNFBPs the team met stated that they would also file an STR when there is a potential name match (see also relevant discussion in IO.4 below). The competent authorities also conduct regular on-site inspections thereby verifying that the reporting entity keeps the updated list of designation and conducts proper screening.

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

273. Singapore has a large and generous NPO sector, the oversight of which is the responsibility of a number of competent authorities. Singapore has demonstrated a strong capacity to obtain information on its sector which has allowed it to assess to some extent which organisations, based on their activities and characteristics, are at risk of TF abuse.

274. Singapore's competent authorities have appropriate regulations and enforcement powers in place to safeguard NPOs from TF abuse. However Singapore has not implemented a targeted approach in doing so for what appears to be two main reasons: (1) a lack of a comprehensive understanding of the TF abuse risks faced by NPOs in Singapore; and (2) a lack of expertise within the competent authorities to identify and address potential cases of terrorist financing abuse.

275. Singapore's understanding of the TF abuse risks faced by NPOs is limited to international work done in this area. A lack of a comprehensive risk assessment as part of their domestic sector review has resulted in Singapore relying on domestic cases as an indicator to inform their risk assessment. In addition, the National Risk Assessment only identifies an assessment of residual risk (taking into consideration control measures in place to address inherent vulnerabilities), which is assessed to be low. Therefore the inherently high vulnerability of NPOs to TF abuse is lost in such an assessment.

276. All competent authorities responsible for the oversight of NPOs in Singapore have conducted outreach to organisations that fall under their respective responsibilities. In each case, however the guidance is general in nature addressing, at a high level, information regarding

combatting money laundering and terrorist financing absent of a comprehensive discussion specific to NPOs' vulnerability to terrorist financing abuse risks.

277. Singapore has a number of regulatory measures in place which provide it with appropriate touch points to address TF abuse of its NPOs. There is however an over reliance on screening techniques against publicly available watch-lists, lists of officially designated entities and government indices checks. In addition oversight of NPOs is restricted to good governance reviews and while Singapore has recently added an AML/CFT component to the reviews conducted by the charity regulator, there remains a lack of targeted reviews based on any assessment of TF abuse risks.

278. Singapore's lack of appreciation for the TF abuse risks faced by its NPOs has hindered its ability to detect such abuse. In addition Singapore's competent authorities responsible for NPOs, while a part of the Government's AML/CFT regime, are isolated operationally from the traditional enforcement agencies particularly the Internal Security Department. Singapore's competent authorities responsible for NPOs have not received any TF-related STRs from STRO.

279. The Office of the COC monitors fundraising appeals for foreign charitable causes and uses the Fund-Raising for Foreign Charitable Purposes (FRFCP) regime as a measure to control and determine the end use of overseas funds. Information that the Office of the COC requires includes details of end beneficiaries, which must be registered organisations; proof that the beneficiaries are bona fide organisations in its country; and a write-up about what the funds are intended to be used for. End beneficiaries are screened against World-Check to scan for links to terrorist organisations/risk of TF. In addition, for locations which are considered high risk, additional checks are conducted with relevant agencies such as ISD/MHA and MFA. Permit holders are also required to submit their audited statement of accounts and acknowledgement of receipt by the endorsed beneficiaries within 60 days from the close of the fundraising appeals. There is a real risk that this regulatory burden, absent of analysis based on an understanding of risk as opposed to screening checks, may have an adverse on charitable giving.

Deprivation of TF assets and instrumentalities

280. Between 2008 and 2014, Singapore has frozen assets (including property) worth SGD 2 858 000 (approx. EUR 1 885 137 / USD 2 006 602). No funds have been confiscated. This is largely consistent with Singapore's assessment of its TF risks.

Consistency of measures with overall TF risk profile

281. The NRA report states that Singapore, as a financial and transportation hub, is vulnerable to terrorist elements seeking its hub status to raise funds domestically, and to terrorism-related developments at the global and regional levels by directing funds from abroad to support terrorism activities in Singapore or use Singapore as a conduit for foreign terrorism financing. In light of such potential high TF risks inherent to Singapore, flexible implementation of TF asset-freezing measures in tandem with foreign countries will be crucial for effective risk-based implementation. The NRA Report emphasises a potential terrorist financing risk by foreign terrorist organizations such as Hamas or Hezbollah. However, the sanction list open to the public only designate Singaporeans, and the authorities indicated that there is no need to list Hamas or Hezbollah as they are considered to

be well known as terrorist organisations, and the TSOFA more generally prohibits any dealing with such terrorist or terrorist organisations. To implement such catch-all system, FIs and DNFBPs have been reminded of the general prohibition and wide definition of "terrorist" under the TSOFA through circulars, outreach and engagement. FIs and DNFBPs will undertake their due diligence, including the conduct of screening, and take into account the TSOFA definition of terrorist. When there is hit or potential hit, FIs and DNFBPs will file an STR and seek further instructions from the authorities. FIs and DNFBPs will also place a temporary freeze or hold on the accounts or transactions pending additional feedback from the authorities.

282. The lack of supervision over PSMDs, which are known to have a significant trading volume in Singapore, has a negative impact on the existing TF preventive measures.

283. ***Singapore has achieved a moderate level of effectiveness for IO.10***

Immediate Outcome 11 (PF financial sanctions)

Implementation of targeted financial sanctions related to proliferation financing without delay

i. Without delay

284. The mechanism implementing proliferation financial sanctions is similar to that for terrorist financing sanctions. An individual or an entity designated by the relevant UN Sanctions Committees is referred to the UN (DPRK/Iran) Regulation and MAS (DPRK/Iran) Regulations, and prohibitions including freezing-measures go into effect immediately upon the designation by the UN. The website of the MAS has a link to the UN Sanctions Committees, and financial institutions and DNFBPs subscribe to the website, as set out in detail in IO.10 above.

ii. Communication

285. The MAS and the competent authorities respond to inquiries from financial institutions or DNFBPs on how to deal with possible false positives (name matches) to the designated information. Singapore emphasised that most of the DNFBPs (approximately 80%) are also subscribing to the website of the IMC-TD or MAS, but given that PSMDs without pawnbroker's license are not regulated and supervised, it is however not known to what extent PSMDs are aware of the existing PF sanctions regime.

286. Except for non-pawnbroker PSMDs, the competent authorities and SRBs for DNFBPs have close communication channels with financial institutions and DNFBPs to ensure that they are aware of updated lists and conduct proper screening of the designated persons. Once there is a hit with a designated person, the reporting entity is obliged to immediately inform the Commissioner of Police and file an STR, in addition to sharing the information with the competent supervisory authorities.

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

287. Regarding Iran, in addition to sanctions pursuant to UNSCRs, MAS issued a notice in June 2012 to all financial institutions in Singapore to prohibit any transactions with the government of Iran and financial institutions in Iran (Prohibition Notice). The Prohibition Notice is aimed at protecting the financial system of Singapore from illicit financial flows from Iran in recognition of:

(i) FATF's assessment that Iran presents on-going and substantial money laundering and terrorist financing (ML/FT) risks, and (ii) concerns those transactions with the Iranian government or financial institutions in Iran could be routed through Singapore. The Prohibition Notice has a clause which exempts the prohibition of certain transactions based on MAS's approval. The authorities indicated that four cases regarding payment of basic expenses and humanitarian transactions have been granted. The prohibition notice further assists to create awareness, although the assessment team is concerned this may have worked as a driver of de-risking. The Prohibition Notice was cancelled with effect from 28 January 2016, following the arrival of Implementation Day (16 January 2016) pursuant to the Joint Comprehensive Plan of Action (JCPOA).

288. Regarding DPRK, Singapore has been promptly responding to information provided by the UN and foreign jurisdictions regarding entities related to designated entities under relevant UNSCRs. In November 2014, the Singapore authorities issued an advisory note to a Singaporean shipping company to comply with UN Resolutions in response to a request by the Panel of Expert of UN Security Council for information about alleged links with another entity designated by the UN under UNSCR 1718. The MAS had sent alerts to financial institutions in Singapore on entities that may be involved in DPRK's proliferation of WMD's activities and requested them to report if and when they have any transactions with the specified entities. Where appropriate, financial institutions are expected to conduct the relevant enhanced customer due diligence, and freeze assets as required.

289. The Singaporean authorities indicated that no funds, assets or economic resources have been frozen pursuant to the MAS Iran/DPRK Regulations and the UN Iran/DPRK Regulations.

FIs and DNFPBs' understanding of and compliance with obligations

290. Financial institutions and DNFBPs the team met with were well aware of the financial sanctions against Iran and the DPRK. However, financial institutions and DNFBPs indicated that they rather prefer to reject transactions when they identify any possible links to these countries through commercial search engines, regardless of their relevance for proliferation. While this is somewhat beyond the scope of the IO 11, during the on-site visit, the assessors also understood that such *de-risking* may also be taking place for transactions with countries on the FATF's public documents identifying jurisdictions with significant deficiencies in their AML/CFT measures, countries in conflict zones (e.g. countries in the Middle East region) and other countries subject to sanction programs by third countries. This phenomenon is not peculiar to Singapore, but there are concerns that the reliance on a risk-assessment based on the results of the consultation of commercial databases could act as a driver for de-risking.

Competent authorities ensuring and monitoring compliance

291. Singapore demonstrated a robust information sharing mechanism among relevant authorities in charge of export control through the IMC-EC, financial supervision, intelligence and law enforcement. The IMC-EC provides a whole-of-government policy oversight of all export control matters and serves as Singapore's policy and operational coordination mechanism for implementation of UNSCRs pertaining to WMD-proliferation issues. There are no competent authorities supervising PSMDs other than those with pawnbroker's license.

292. Singapore has achieved a substantial level of effectiveness for IO.11

CHAPTER 5. PREVENTIVE MEASURES

Key Findings and Recommended Actions

Key Findings

1. FIs and DNFBPs generally demonstrated a reasonably good understanding of ML risks impacting Singapore domestic clients, but a less developed understanding of the risk of illicit flows into and out of Singapore.
2. FIs had a less mature understanding of TF risks, and often only considered the risks of actual terrorism. Several DNFBPs demonstrated a poor understanding of TF risks.
3. The requirements for CDD, record-keeping and PEP clients were well understood by FIs spoken to, although some sectors (insurance, remittance agents/money changers and money lenders) had a less sophisticated understanding of ongoing monitoring. There were potential gaps between FIs in their understanding of the overall source risk for the proceeds of foreign corruption entering Singapore. Overall, DNFBPs' implementation of CDD and PEP requirements is clearly at a lower level in comparison with FIs and this seems to be due to the fact that AML/CFT preventive measures were only recently introduced for most of them. While the EP-200 for accountants does not qualify as low or other enforceable means, accountants appear to interpret its provisions as being mandatory.
4. The STR requirements were generally well understood, but with potential defensive filing in the insurance sector. Although general guidance is given by both STRO and MAS, little targeted feedback is given on the quality and usefulness of STRs filed. In the DNFBP sector, the low numbers of STRs filed in the last few years show that much needs to be done in tandem with the competent authorities and SRBs to achieve effective implementation.
5. FIs and DNFBPs are required to submit an STR "as soon as is reasonably practicable" after it comes to their attention. The Guidelines state this as being within 15 business days of referral internally. In reality, complex cases could take longer than this. STR filing in the money lending sector is very low.
6. FIs were found to have a good understanding of the need to have internal systems and controls to ensure compliance with the MAS/IPTO requirements. This included the need for group policies to be adjusted for global operations (foreign-based FIs) and for Singapore-based FIs operating overseas. Financial secrecy provisions are, in practice, not found to be hindering the sharing of information within groups. While DNFBPs have internal policies and controls in place, those of trust service providers and casinos are better developed.

Recommended Actions

1. The authorities are encouraged to revise the NRA to deal more specifically with the ML threats to the financial sector in the context of Singapore's position as a financial centre. The NRA's treatment of TF should be similarly revised and updated to reflect more recent threats.
2. In conjunction with the above, the authorities are encouraged to continue dialogue with the FIs to promote a better understanding of ML and TF risks. Singapore should increase the level of communication and information sharing by competent authorities and SRBs with DNFBPs to ensure a better understanding of the ML/TF risks and to fine-tune existing

measures.

3. MAS and IPTO are encouraged to continue to work with the insurance, remittance/money changing and money lending sectors to improve understanding of ongoing monitoring requirements.
4. The authorities are encouraged to continue to work with FIs to improve the understanding of the source risk for proceeds of foreign corruption entering Singapore.
5. Competent authorities and SRBs should increase awareness of AML/CFT preventive measures for the various categories of DNFBPs to ensure that CDD and PEP measures are better understood by all DNFBPs.
6. Singapore should clarify the expectations of filing STRs with a view to shortening the time taken to submit STRs.
7. The authorities should continue to work with the financial sector to increase the quality of STRs with a view to improving the level and quality of disseminations, and provide greater feedback on the quality of STRs submitted.
8. Singapore should also improve the feedback from the authorities and SRBs to DNFBPs in regard to STRs, –including by encouraging DNFBPs to consider filing STRs rather than simply rejecting certain customers and transactions. This should be facilitated by a better understanding of ML/TF risks by DNFBPs.
9. Singapore should continue to work with sectors where low numbers of STRs are being filed (e.g. money-lenders) and where there is the possibility of defensive filing (insurers) to ensure that the STR requirements are fully understood.

293. The relevant Immediate Outcome considered and assessed in this chapter is I0.4. The recommendations relevant for the assessment of effectiveness under this section are R9-23.

Immediate Outcome 4 (Preventive Measures)

Understanding of ML/TF risks and AML/CTF obligations and application of mitigating measures

i. Financial institutions

294. All FIs in Singapore are required to identify, assess and understand their money laundering and terrorism financing risks. This requirement is set out in the relevant Notices, and the financial sector supervisors (MAS and IPTO) have issued comprehensive guidelines to assist FIs in understanding their AML/CFT obligations.

295. Singapore's NRA report sets out a number of vulnerabilities for each sector. These were developed in consultation with the private sector, who generally found the NRA to be useful.

296. FIs with a domestic focus demonstrated a less sophisticated understanding of ML and, in particular TF risks facing them. Foreign FIs (banks in particular) were found to have a better understanding of ML risks, although even here there appeared to be a concentration on crime impacting Singapore account holders (e.g. money mules and internet scams) as opposed to a developed understanding of possible flows of illicit funds into and out of Singapore. Each FI spoken to had their own views of the source countries that posed ML risks, especially in relation to the

potential for proceeds of foreign corruption. The authorities consider this to be consistent with the emphasis MAS places on FIs to conduct "enterprise-wide" risk assessments that incorporate risks from these countries.

297. Although this view was in part coloured by the geographical reach of each FI, it in part reflected the lack of an overall national level pronouncement on geographical risk. Given Singapore's geographical position, and in particular the level of activity in the large private banking and trade finance sectors, this is an area where both the private and public sector are encouraged to develop a more detailed common understanding.

298. The understanding of TF risk was less current, but in line with the limited findings of the published NRA report. In particular, some FIs tended to conflate the risk of terrorism with the risk of terrorist financing, with efforts being focused on screening for sanctions. One FI considered that the NRA document should be updated to reflect current TF risks.

299. Money lenders and remittance agents/money changers were generally focussed on the risk of volumes of transactions, and demonstrated an overall lower understanding of ML/TF risk facing them, except those that concentrated on a particular country/region.

300. Overall there has been a notable increase in the number of AML/CFT compliance staff hired across all sectors, which the authorities see as a sign of the increasing seriousness with which FIs regard AML/CFT issues.

ii. DNFBPs

301. Representatives of DNFBPs demonstrated that they are all aware of the NRA report, and find the risk assessment fair. They also demonstrated that they recognise ML/TF risks inherent to their own sector.

- *Casinos* – The Casino operators are responsible for establishing internal controls for prevention of money laundering and terrorist financing (PMLTF) and for implementing the necessary preventive AML/CFT measures. Each casino's PMLTF internal controls framework sets out precise measures on, amongst others, CDD, EDD, higher risk transactions including through thresholds of gaming, and indicators for STRs. Red flags are used to identify suspicious and high-risk transactions or behaviours, and customers (e.g. large buy-in but no gaming, chip-passing, adverse media news, and customers not providing sufficient customer information). The casino operators share information with one another in Singapore and as part of their risk assessment, they will also review any ML/TF cases and trends that occurred in other jurisdictions to further strengthen their framework.
- *Real Estate Agents* – CEA conducted a series of outreaches on AML/CFT. CEA distributed a self-assessment check list for sales persons in May 2015 to promote better understanding of ML/TF risks and AML/CFT measures they should implement. The self-assessment check list covers procedures for CDD and indicators of ML/TF activities. CEA also provided Frequently

Asked Questions on STRs. Foreigners especially from conflict regions are considered to be high - risk customers, while buying property in physical cash is identified as being a typical high risk transaction.

- *Lawyers* - The Law Society is mainly responsible for AML/CFT measures for lawyers, and it conducts annual inspections of lawyers. Although the Law Society indicated that the inspection includes AML/CFT aspects, it is not clear to what extent these aspects are looked at. Lawyers recognise that foreign clients, PEPs and those on the sanction lists are high risk customers, and consider the value and patterns of certain real estate transactions also constitute high risk. However, while lawyers are aware of the obligations, until recently many law practices did not have specific policies or procedures on how to deal with situations where they have to file an STR and the consequential consideration in relation to a client whom they have filed an STR against.
- *Company Service Providers (CSPs)* - ACRA conducts outreach sessions to raise awareness of AML/CFT. Since CSPs may be professional accountants or lawyers as well, the outreach conducted by the relevant SRB or competent authorities also covers CSPs. ACRA conducted inspections on CSPs in the 3rd quarter of 2015. CSPs consider shell companies and companies owned by foreigners as high risk. CSPs identify specific cases of shell companies through their client's profile and activities.
- *Accountants* - ISCA issued EP-200 to members and conducted a survey to get a view on the sector's measures in place. ACRA conducted its initial AML/CFT inspection in April 2015. Accountants the team met with recognised that high risk customers and transactions consist of moneylenders, money remittance agents, casinos, pawnbrokers and transactions involving Iran.
- *Trust Service Providers (TSPs)* - TSPs recognise that a complex trust with an unidentifiable beneficial owner is a high risk, as stressed in the NRA report, even though such arrangements are not so common. Further, TSPs emphasised that trusts involving PEPs are high risk. TSPs the team met with have a specific internal unit looking into PEPs and conducting internal audit reviews to assess the entire AML/CFT system in place.

302. As such, all DNFBPs demonstrated awareness of risks. However, the risk mitigating measures they are taking present a mixed picture, with TSPs and casinos being stronger compared to other DNFBPs in terms of scope and degree of implementation.

303. The casino sector has been taking comprehensive systematic measures, such as: (i) screening of every employee; (ii) restriction of taking chips over SGD 10 000 (approx. EUR 6 596 / USD 7 021) out of the integrated resort; (iii) quarterly review of clients' (patrons') accounts and termination of dormant accounts; and (iv) internal and external audit. Against this, measures taken by other DNFBPs are rather focused on simply preventing customers

identified as high risk from being accepted and high-risk transactions being executed than exercising enhanced due diligence and managing the risk. Such an approach appears conservative, but it casts a doubt on whether it is based on DNFBPs' understanding of ML/TF risks and on the results of a fair risk assessment. While the type of customers and transactions are different by sector, the team has the impression that there is a significant difference in the level of understanding of the ML/TF risks between the financial sector and DNFBP sector and even among the DNFBP sector (i.e. casinos, TSP vs. others).

Application of enhanced or specific CDD and record keeping requirements

i. Financial institutions

304. Financial institutions generally demonstrated a good understanding of the CDD and record-keeping measures set out in the various Notices, which, along with the Guidelines, are comprehensive. In particular, they were able to describe clear procedures for obtaining beneficial ownership information and banks/capital markets intermediaries had a good understanding of the requirements for ongoing monitoring, in particular the need to adjust criteria for automated systems in accordance with the type of business and customers dealt with.

305. The insurance sector was slightly less sophisticated, with some being in the process of updating their systems for ongoing monitoring. Money lenders and remittance agents/money changers tended to set their parameters on the basis of volumes/value of transactions only.

306. All FIs spoken to were aware of the need to refuse or terminate business if unable to obtain complete CDD information and many gave instances of where this had been done.

307. The results of supervisory work suggest that the overall levels of compliance for CDD are fairly robust, and have improved in areas such as trade finance (which is an area of concern identified in the NRA), although some breaches have resulted in remedial action being required.

ii. DNFBPs

308. The team confirmed that representatives of DNFBPs the team met have basic awareness of CDD and record keeping obligations. While the FATF expects that business is to be refused in case CDD is incomplete, in many cases business is simply refused at the time of a first screening rather than based on the results of formal CDD processes with verification of aspects such as ID and purpose of the transactions, consistent with the FATF standards. Representatives of DNFBPs also stated that professional common sense is their last resort to identify risks rather than being based on formal risk identification processes.

309. Casinos conduct CDD several times throughout a gaming process at various circumstances: e.g. (i) at a membership counter for registration of a membership account with the casino operator; (ii) purchasing of chips above SGD 5 000 (approx. EUR 3 298 / USD 3 510); and (iii) when winnings above SGD 5 000 are paid out in cash, cheque or telegraphic transfers. The casino operator conducts screening of the customer at the various CDD trigger points (i.e., circumstances as specified in s.139 (1) of the CCA). Screening is made against UN sanction lists, PEPs and the jurisdictions the FATF has called for counter-measures. All these results are recorded and kept for five years.

Application of enhanced or specific CDD requirements

i. Financial institutions

(a) PEPs

310. Given its position as a financial centre, FIs in Singapore have a varying degree of exposure to PEPs (both foreign and domestic) with the private banking sector having the most number of PEPs as clients. Whilst the supervisors report that isolated breaches of the requirements have been discovered during on-site visits, the FIs spoken to demonstrated a good understanding of the requirements for dealing with PEP clients, with most using a variety of techniques to identify and monitor the activities of PEP clients, and many having committees to consider the risks of dealing with them. Several were able to give examples of where PEP business was refused. The risk of the proceeds of corruption was often cited as a key concern, and the geographical spread of foreign PEPs varied by institution, depending on their business focus. Most FIs had their own list of countries of concern, which varied. Given the lack of focus on geographical risk in the NRA document, there is a risk of gaps developing between the various FIs in their respective understanding of corruption risks.

(b) Correspondent banking

311. Correspondent banking is a key feature of banking operations in Singapore, both for general operations and those connected with trade finance. Given the additional risks associated with trade finance, banks were able to demonstrate a good understanding of the controls required to mitigate the risks of ML in this activity. The findings of supervisory work by MAS suggests that compliance in relation to correspondent banking, especially in a trade finance context, has improved since publication of the NRA. Despite the large number of correspondent accounts held by banks, the overall trend for correspondent relationships was downward, as banks reported a reluctance to open new relationships. This appeared to be especially acute in foreign-owned banks, and resulted from global policies as opposed to perceptions of local requirements. Banks spoken to found the MAS Guidance on Anti-Money Laundering and Countering the Financing of Terrorism Controls in Trade Finance and Correspondent Banking (published in October 2015), helpful. Wire transfer rules were similarly found to be well understood, with banks in particular able to describe the importance of robust systems and controls in this area.

(c) New technologies

312. The various MAS Notices set out requirements to identify and assess the ML/TF risks of new products, business practices and technologies. At present, the development of new technologies in the financial sector was largely found to be limited to the use of mobile banking facilities, and the view was that the supervisor keeps a close eye on developments. Although one FI felt that MAS was at times slow to react to new developments, the assessment team did not feel that this had a negative impact on effectiveness in this area. Virtual currencies were widely regarded as an area of future growth, and this has been identified in the NRA report as a risk that requires further study.

(d) Targeted financial sanctions relating to TF

313. All financial institutions and DNFBPs that the assessment team met indicated that they subscribe to the MAS' website. In practice, however, most types of DNFBP that do not necessarily require immediate update for their operation rely on commercial databases. Given that the quality and contents of the database vary by the vendor, it is not clear to what extent they have access to accurate and updated information in a timely manner.

314. Where financial institutions and DNFBPs have a match with designated individuals (or terrorists), they are obliged to inform the Commissioner of Police immediately (s.8 of the TSOFA).For financial institutions and money lenders, a parallel report will be made to MAS and IPTO respectively. Representatives of financial institutions and DNFBPs stated that they are also advised to file an STR when there is a partial name match. The competent authorities also conduct regular on-site inspections, thereby verifying that the reporting entity keeps the updated list of designation and conducts proper screening.

(e) Higher-risk countries identified by the FATF

315. Financial institutions were generally aware of the FATF lists of higher-risk countries and had factored these into their systems and controls. The MAS publishes the list of countries of concern after each FATF plenary, and FIs spoken to demonstrated adequate knowledge of the counter-measures listing process, but less about other countries on the list. FIs are required to conduct their own risk assessment, which includes country risk. MAS then subjects this risk assessment to robustness checks and issues inspection findings where risks are inadequately considered. The comments made above about more general geographical risk and the lack of any national pronouncement on the regional risks facing Singapore mean that FIs have an uneven appreciation of geographical risks in the area. Some geographical risk mitigation is motivated by group policy (e.g. not doing business with European clients).

ii. DNFBPs

(a) PEPs

316. Representatives of the DNFBPs are also aware of PEPs and their inherent risks. The team was informed, however, that to identify PEPs several categories of DNFBPs (e.g. real estate agencies and accountants) are using commercial search engines publicly available. Many of them, especially small-sized practitioners, explained this approach by referring to the high costs related to relying on reliable external databases. The team has serious concerns that the more general and publicly available search engines do not necessarily allow the identification of PEPs and that related information is not kept properly updated and fully reliable when accessed. It is evident that there is a clear and urgent need for competent authorities as well as SRBs to provide further advice and guidance to the DNFBPs under their regulation and supervision on how to identify PEPs.

(b) Targeted financial sanctions relating to TF

317. See subsection on financial institutions above.

(c) Higher-risk countries identified by the FATF

318. Some of the DNFBP representatives stated that they are also aware of dealing with certain high risk countries, especially those identified in the FATF's public documents and those subject to UN sanctions. In addition, through media reports and daily transactions, individual practitioners identified specific countries as high risk. However, it is not clear to the team as to whether these countries are identified as high risk in terms of ML/TF or in terms of other risks such as stability in the political situation and legal system. These specific risk assessments rely on the professional judgement of individual practitioner's or the group policy for larger companies and are not necessarily consistent with broader domestic risk assessments. Indeed, the NRA report does not include any references to these specific country risks.

Reporting obligations and tipping off

i. Financial institutions

319. STR reporting has generally increased across all sectors (see table 23) since 2009. STRs are filed with STRO and a copy is also received by MAS/IPTO. The various pieces of MAS guidance contain red-flags appropriate to the relevant sectors, and the assessors found a generally good understanding of the requirements in the Notices for submitting STRs, which went beyond the need to merely match red-flags. The banking sector has submitted the most number of STRs, which relate to a variety of issues including trade finance, PEPs and unlicensed money-lending. However, it was notable that most FIs spoken to have not filed STRs related to TF. The insurance sector has filed a notably large and increasing number of STRs. The NRA report concludes that "some DL insurers adopt a conservative approach in reporting suspicious transactions". The assessors discussed this issue with the industry, who appeared to be defensively filing STRs, by filing STRs without much consideration of whether there are grounds for suspicion. The authorities, however, consider that the increase in STRs filed reflected the increased awareness of the sector, and have been useful to STRO's analysis and data mining. Other sectors felt that MAS was concerned with raising the number of STRs, and it was apparent across the financial sector that little targeted feedback had been given on the quality of the STRs filed by either STRO or MAS (although both were reported to ask for additional information if an STR is incomplete). This was particularly apparent in relation to the exercise that Singapore undertook in 2013 and 2014 when MAS required all FIs under its supervision to conduct a review of the tax legitimacy of assets in client accounts. This resulted in over 22 000 accounts being closed, with a total of 2 988 STRs being filed. FIs spoken to reported little feedback on STRs filed unless this had been pro-actively requested.

Table 23. **STR filing by financial institutions**

FI Entity	2009	2010	2011	2012	2013	2014
Banks (Total)	3 414	3 909	4 075	6 959	8 193	10 212
- Full banks			3 752	6 516	7 175	8 985
- Wholesale banks			190	269	684	842
- Offshore banks			45	56	93	107
Merchant banks			88	118	241	278
Finance Companies	55	45	49	79	52	79
Money-Changers & Remittance Agents	707	849	2 004	2 738	3 536	5 922
Direct Life Insurers	4 401	3 679	2 583	3 453	4 923	5 714
SVFs	1 000	1 647	2 107	1 742	1 101	1 335
Capital Market Entities	1 354	1 183	1 206	946	1 122	1 217
Moneylenders	0	0	0	0	0	4
Total	**10 931**	**11 3120**	**12 024**	**15 917**	**18 297**	**24 483**

320. The number of STRs filed by money-lenders is low, and steps should be taken to improve understanding of the requirements and risks in the industry.

321. The assessors were concerned to note that, despite the CDSA stating that an STR should be filed "as soon as is reasonably practicable" after it comes to the filer's attention, the Guidelines direct that this period "should not exceed 15 business days of the case being referred by the relevant bank employee or officer". STRO has conducted some analysis of the time taken for filing STRs (albeit looking at the times taken to file from the date of the first transaction): a 2014 study recorded that, in the sample taken, it took on average 28 calendar days in the banking sector, 16.1 days for remittance agents/moneychangers and 29.3 days in the insurance sector. The authorities consider that the majority of STRs are filed promptly and that longer time is taken in complex cases.

322. Singapore itself acknowledges that the banks are more familiar with the STR filing requirements than other sectors, and the percentage of disseminations from STRs submitted would tend to support a conclusion that the quality of STRs is better from the banking sector. From 2011 to 2014 the average dissemination rate was:

- Banks – 36.8%
- Capital markets – 12.9%
- Remittance agents and money changers – 19.4%
- Insurance – 6.3%.

ii. DNFBPs

323. AML/CFT preventive measures have been put in place recently for most of the DNFBPs, however, the suspicious transaction reporting requirements were imposed on DNFBPs at the same time as on financial institutions, and, therefore, the low numbers of STR filing by DNFBPs cannot be justified. Representatives of the various categories of DNFBPs, except casinos and TSPs, stated that they are confronted with a number of suspicious transactions in practice, but that potential

customers are rejected in the context of the screening process and subsequently not filed as an STR. Some of the representatives also stated that a practitioner's character as a professional advisor discourages them to file an STR unless there is a strong reason to believe that the transaction or the client has clear links with criminal activities. The team is of the view that cases filed as STRs are therefore only the tip of the iceberg, and that it does not show a fair and entire picture of potential suspicious transactions taking place. Some DNFBP representatives did not seem to understand that the purpose of the STR is to provide the authorities with information that more generally could lead to the detection of criminal conduct.

324. Among the DNFBP sector, a disparity is observed in terms of the practitioners' sensitivity to STR. While respective supervisory authorities and SRBs provide guidance on STRs, some of them only provide a mere conceptual explanation with a few examples, whereas casinos use a list of nearly 30 specific patterns by types of gaming, customer and transaction. DNFBPs would benefit from targeted outreach from the competent authorities and SRBs, including sharing of concrete examples of suspicious transactions. This would allow them to have a better understanding of suspicious transactions and prompt them to file quality STRs when they suspect or have reasonable grounds to suspect that funds are the proceeds of a criminal activity.

Table 24. **STRs filed by DNFBPs**

	2009	2010	2011	2012	2013	2014
Casinos	-	530	1 429	1 942	3 331	4 359
PSMDs (including Pawnbrokers)	0	0	0	0	0	0
Company Service Providers	1	2	1	1	33	13
Trust Service Providers	41	28	20	16	62	44
Real Estate Agents	5	0	0	0	1	2
Lawyers	6	4	7	9	13	15
Professional Accountants (including Public Accountants)	2	5	1	0	0	2

325. Singapore requires certain sectors to file a cash transaction report (CTR) to STRO when conducting a transaction exceeding a certain threshold. Casinos are subject to filing of CTRs when a casino operator conducts a cash transaction with a patron (client) which exceeds SGD 10 000 (approx. EUR 6 596 / USD 7 021) in a single transaction. Dealers in precious metals and stones, including pawnbrokers, are also subject to filing a CTR when they are confronted with a cash transaction exceeding SGD 20 000 (approx. EUR 13 192 / USD 14 042) in a single or multiple linked transaction.[44] The sector representatives explained that they consider that there is no (potential) relationship between CTRs and STRs, and STRs are generally not filed concurrently with CTRs. However, the situation is different for the casino sector where operators conduct quarterly reviews of both CTRs and STRs, and also have a regular meeting with the STRO to discuss the quality of STRs submitted.

[44] S. 48I (1b) of the CDSA.

Internal controls and legal/regulatory requirements impending implementation

i. Financial institutions

326. The requirements for FIs to understand and mitigate their ML/TF risks described above are complemented by requirements to develop and implement adequate internal policies, procedures and controls, taking into consideration the ML/TF risks facing the FI. These are specifically required to cover all aspects of the MAS/IPTO rules. All FIs spoken to had internal controls at Singapore level, with overseas groups adapting their global systems to local requirements, where appropriate. Examples given were the additional audit measures that MAS requires, which sometimes went beyond global requirements for groups headquartered overseas. Singapore-based groups ensure that Singapore requirements are used group-wide, again with local variations, if appropriate.

327. Financial institutions used either specific client approval to share information or the regulatory exception in the Banking Act to release client data within a financial group and with other FIs, and thus secrecy does not appear to impede the sharing of information.

ii. DNFBPs

328. Regardless of the size, each DNFBP indicated they have their own internal controls and policies; however they differ in detail and scope depending on the nature of their business. Not all elements of the internal policies are aimed at AML/CFT, but more general policies such as thresholds applicable to client accounts held by a law firm, and red flag indicators based on the gaming amount and customers' behaviour by casinos also serve as AML/CFT preventive measures. The team had the impression that internal policies significantly rely on individual DNFBPs' experiences and knowledge on top of sector-wide accepted standards.

329. ***Singapore has achieved a moderate level of effectiveness for IO. 4***

CHAPTER 6. SUPERVISION

Key Findings and Recommended Actions

Key Findings

Financial institutions

1. Licensing controls are generally robust in the financial sector, with MAS and IPTO conducting a variety of checks at application and on an ongoing basis.
2. The Singapore Government has imposed a moratorium on new licences for money lenders. Given the NRA's finding that unlicensed money lending is a key concern, it is unclear how this policy assists.
3. Singapore's sophisticated financial system is vulnerable to both money laundering and terrorist financing, which the authorities recognise. Whilst the NRA goes some way to identifying the vulnerabilities in the system, moderate improvements in Singapore's understanding of its ML/TF risks will maximise the potential value of the NRA to financial sector supervision.
4. The MAS categorises sectorial risk for both ML and TF on the basis of the NRA, and then rates each FI for ML/TF. Although this is a useful tool, some inconsistencies have arisen: despite the NRA's finding that insurance is low risk, MAS categorises 13 out of 20 direct life and composite insurers in the higher risk categories.
5. For most FIs, AML/CFT supervision appears robust, with a variety of off-site factors examined and comprehensive on-site examinations/follow-up being conducted. Money lenders are subject to a less intensive supervisory regime.
6. There have been very limited AML/CFT inspections of SVF holders (despite the risks identified in the NRA for internet-based SVFs) and non-bank card issuers.
7. Singapore has a range of remedial measures that it can impose on financial institutions. The methodology for imposing financial penalties by MAS could be more flexible. No direct action has been taken against senior management.
8. Financial sector supervisors are well-respected and FIs welcome the close contact they are able to have on a regular basis. Guidelines produced by MAS are comprehensive and FIs spoken to found them useful.

DNFBPs

1. Singapore has recently developed and extended AML/CFT supervision to most types of DNFBPs, but there are significant differences in effective supervision of AML/CFT requirements between relevant supervisory bodies.
2. Sectors such as the casino and trust service providers are well supervised, but the majority of PSMDs are not subject to AML/CFT supervision and only those with a pawnbroker's license are regulated for AML/CFT purposes.
3. The financial penalty structure across the DNFBP sector is quite diverse and concerns exist about the differences in approach in terms of dissuasiveness and proportionality. Apart from the casino and TSP sectors, sanctions for non-compliance have not been tested.

6

Recommended Actions

Financial institutions

1. On the basis of a fuller NRA, more closely target supervisory activity to ML/TF risks.
2. Increase the ML/TF focus of IPTO visits to money lenders.
3. Carry out further work to look at the risk in the licensed and unlicensed money lending sectors and see if market capacity and existing measures are sufficient to deter illegal perimeter activity.
4. Review and consider revising the MAS enforcement policy, especially in relation to financial penalties for capital markets entities. Make full use of all available tools including, where appropriate, direct action against individuals/senior management.
5. Step up supervisory activity for areas not previously within scope (e.g. non-bank credit card issuers and SVFs).
6. Given the number of insurance companies in the higher risk categories, consider increasing targeted supervision of these firms based on ML/TF risk.
7. Monitor the need for specialist AML/CFT supervisory resources in the light of any revisions to the NRA.

DNFBPs

1. Singapore should ensure effective supervision for AML/CFT across all categories of DNFBPs through risk-based, targeted and prioritised outreach to and inspections of the non-financial professions.
2. Singapore should extend AML/CFT supervision to all PSMDs.
3. Singapore should improve its financial penalty structure across the DNFBP sector and enforce a sanctioning regime for non-compliance with AML/CFT measures.

330. The relevant Immediate Outcome considered and assessed in this chapter is IO3. The recommendations relevant for the assessment of effectiveness under this section are R26-28 & R.34 & 35.

Immediate Outcome 3 (Supervision)

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

i. Financial institutions

331. Licensing controls are generally robust in the financial sector, with MAS and IPTO conducting a variety of checks of directors, substantial shareholders, beneficial owners and key appointment holders at application and on an ongoing basis. Both supervisors were able to give examples of how their systems work in practice for both foreign and domestic applicants, of where applications were rejected and where ongoing monitoring checks of fitness and propriety led to prohibition orders and revocation of licences. In addition, some examples were given by MAS of how initial applications were withdrawn in the light of requests for further information.

332. The Singapore Government has imposed a moratorium on new licences for money lenders. Singapore explained that the moratorium on new licences for money lenders arose from concerns about the potentially harmful social effects of allowing a proliferation of money lenders that may make credit too accessible to those of low income. The processing of applications for new licences was therefore suspended while a review of the money lending regulatory regime was conducted. Given the NRA's finding that unlicensed money lending is a key concern, the assessors would encourage the authorities to prioritise work on capacity and ML/TF risks in the sector.

ii. DNFBPs

333. Licensing, registration and other forms of control over the various categories of DNFBPs are in place to prevent criminals or their associates from being professionally accredited. Laws regulating each DNFBP sector provide specific criteria for fit-and-proper tests, and based on these criteria, the screening of applicants is conducted in a holistic way. Singapore has extended and further developed its AML/CFT supervision of the DNFBP sector (i.e., casinos, real estate agents, accountants and CSPs) since the adoption of the 3rd round MER in 2008. Singapore also extended its AML/CFT supervision to pawnbrokers whom it assessed to play an essential role in dealing in precious metals and stones. In the meantime, other PSMDs are subject to some AML/CFT preventive measures, such as those relating to STR and CTR requirements.

334. Each of the individual legal statutes has a provision pertaining to fit-and-proper tests of the relevant professions. The competent authorities and SRBs for DNFBPs demonstrated that the screening system developed based on the legal criteria has been working to prevent DNFBPs from being engaged by criminals and their associates. There are cases where application for or renewal of the required certificate was rejected for failing to meet the application or licensing criteria (e.g. accountants (one case since 2012), casinos, and real estate agents (over 400 cases since 2010)). There is no such case for TSPs, but the MAS indicated that there are cases where they advised applicants to withdraw their application when the person was found to be unqualified. As far as lawyers are concerned, there was one case in 2009 where an applicant was rejected to be certified due to his criminal record. No cases were reported related to pawnbrokers and PSMDs.

Supervisors' understanding and identification of ML/TF risks

i. Financial institutions

335. Singapore has a well-developed financial sector and is one of the leading financial centres in the region. As such, the financial system is inherently vulnerable to both money laundering and terrorist financing, which the authorities recognise. MAS was closely involved in the development of the NRA. The NRA goes some way to identifying the vulnerabilities in the financial system, including unlicensed money lending, the use of domestic bank accounts for money mule activities and some examination of the risk from foreign corruption, tax offences and trade-based money laundering. However, moderate improvements in Singapore's understanding of its ML/TF risks will maximise the potential value of the NRA to financial sector supervision.

336. MAS categorises the ML/TF risk of each sector, looking at the threat of ML/TF to each sector before coming up with a scoring (low/medium/high) for inherent risk, based on a number of factors such as cash intensity, size and number of higher risk customers typically targeting the market. An assessment of a set of control factors (such as market entry, on-site inspections) then

results in a further rating, which is combined to produce an overall risk score for the sub-sector. MAS separately rates the ML/TF risk presented by each individual FI in four categories[45] taking into account factors such as its business activities, client profile (e.g. proportion of PEPs and other high risk accounts) transactions with high risk countries and volume of assets managed (where appropriate), and the quality of its controls. This assessment is based on several sources of information, such as STRs (to which MAS has access), on-site supervisory findings and off-site supervisory information including questionnaires and audit reports. The results of this exercise were shared with the assessors, and were generally in line with the overall sectorial risks identified. However, a notable inconsistency was direct life insurance where, despite an overall sectorial risk rating of low, over half of the insurers were rated in the top two categories of risk. Singapore considers that the sub-sectorial ratings are used to allocate supervisory resources across the financial sector, whereas the individual FI ratings are used to allocate resources between FIs in the same sub-sector. However, the assessors remain concerned about the divergence of ratings between the NRA and for individual FIs in areas such as insurance.

337. The majority (by number) of remittance agents were rated in the lower categories of risk, despite the overall categorisation of the sector as medium high. MAS considers that the largest remitters by volume are in the individual higher risk categories. However, given the concerns expressed about the lack of recognition of TF risks and the limited geographical assessment of risk affecting remitters in the NRA, it is unclear whether these assessments are accurate.

338. Singapore itself recognises the need to carry out further work on SVFs (especially internet-based SVFs) which it has identified as posing high ML/TF risk in the NRA. On-site supervision of this sector is in its infancy.

339. IPTO prioritises the supervision of its 179 money lenders, largely based on the volume of business conducted, rather than any demonstrable ML/TF risk assessment. Basing its supervisory risk-based approach largely on the volumes of loans does not appear to be a sufficiently robust methodology, and the assessors would encourage IPTO to increase the range of factors used.

ii. DNFBPs

340. All of the competent authorities for the DNFBP sector and relevant SRBs (i.e., ISCA for professional accountants, and Law Society for lawyers) demonstrated that they acknowledge and agree with the risk assessment in the NRA. Regardless of the NRA findings, each of them is also aware of what types of transactions or customers are at high risk in their sector, and they have been focusing on preventive measures in their outreach and inspection programmes. For example: (i) the CEA (regarding real estate agents) identified transactions related to private housing, especially by foreign customers as high risk; and (ii) supervisors of lawyers and accountants (including CSPs) indicated that transactions involving holding or managing client money are considered to be high risk. The real estate agencies the team met indicated that they try to reduce exposure to non-Singaporean clients to mitigate risks, and they verify complete beneficial owner's information and rationale for acquiring property in Singapore when dealing with foreign clients. Lawyers the team met indicated that they have internal controls in relation to client accounts such as filing a report when receiving cheques, and prohibition of credit to the account and transfer of funds from client account to the 3rd party. Guidance is also provided to lawyers on client accounts through their Practice Direction and the Legal Profession Rules issued by the Law Society of Singapore.

[45] The ratings were shared with the assessment team, but remain confidential.

Risk-based supervision of compliance with AML/CTF requirements

i. Financial institutions

341. Each MAS supervised FI is assigned a contact point/relationship manager. Each of MAS' 400 supervisors undergoes a basic level of AML/CFT training involving classroom and practical training, as well as annual training sessions to ensure that they are current. More specialist AML/CFT knowledge rests with 65 experts who spend between 30% and 100% of their time dealing with AML/CFT issues, and act as contact points for other supervisors who identify issues in the course of their supervision. These specialists are given additional training through courses held by other financial regulators and industry bodies. Financial institutions spoken to during the visit gave the impression that MAS is a well-respected and approachable supervisor.

342. MAS uses an overall Comprehensive Risk Assessment Framework and Techniques (CRAFT) tool to assess the impact and probability of certain risks affecting all aspects of an FI's operations and safety and soundness. Until September 2015, ML/TF was part of Legal Regulatory and Reputational Risk, before MAS made it a stand-alone category of risk. Although ML/TF feeds into the overall assessment of an FI's risks, MAS is careful to ensure that supervisory activity relating to ML/TF is separated, to ensure that it is not given a lower priority overall.

Off-site

343. IPTO relies on quarterly returns of transaction volumes and STR information to keep its assessment of money lenders current. The low level of STR reporting in the sector means that limited information is available to it. MAS uses a variety of off-site tools to target supervision, including the findings of the NRA, STRs (which it receives direct), questionnaires and auditors' reports (internal and external).

On-site

344. MAS uses a combination of the off-site tools mentioned above to inform its on-site activity. This includes a self-assessment questionnaire, whereby FIs are asked to rate the inherent risks they are exposed to and their own effectiveness in addressing ML/TF risks and compliance with regulations. MAS informed the assessors that they regard this information with caution; they also consider it to be a useful tool in assessing an FI's risk awareness, controls and compliance with the regulations. Based on the results of its individual assessment of the combined ML/TF risk of each FI, on-site supervision consists of planned visits (in the regular cycle), events-based visits and thematic visits, such as trade finance/private banking visits to banks. On-site visits take place at least every 3-4 years (for higher risk FIs, especially banks) and last several weeks. MAS has detailed operating procedures covering file sampling, and this is further tailored to meet the needs of the type of visit (e.g. thematic, routine or event-driven) and any specific risks identified. The visits and the corresponding reports seen by the assessors appear to be thorough. Follow-up is similarly thorough, with MAS either conducting follow-up visits or requiring external auditors to confirm that any remedial action has been taken.

345. A notable gap in MAS on-site supervision is for SVF holders and non-bank card issuers. Internet-based SVF holders are identified as posing potentially high ML/TF risks in the NRA. Despite

this, MAS did not have authority to inspect these FIs until June 2015. This is an area that requires further attention. At the time of the on-site visit, MAS had just completed an on-site inspection of the largest internet-based SVF and a supervisory visit to one of the two non-bank card issuers.

346. IPTO supervision of money lenders is aimed at covering most of the 179 institutions on a yearly basis. However, there appears to be little targeting of visits on the basis of ML/TF risk, with risk assessment being focussed on transaction volumes. In addition, visits appear to be very short (sometimes one hour) and include general financial soundness issues as well as ML/TF.

Table 25. **Number of AML/CFT on-site inspections**

	2011	2012	2013	2014	2015 (until Oct)
Banks/finance companies (Total)	14	26	38	40	15
- (of which) Private banks/private banking operations	8	9	13	14	6
Direct life insurers	3	4	4	5	1
Money-changers and Remittance Agents	10	9	9	11	104[1]
Capital Markets	78	5	21	330	11
SVFs	-	-	-	-	1
Money lenders (IPTO)	44	81	122	123	60

Table Note:

1. Of which 100 were performed by external auditors engaged by MAS.

347. MAS considers that the current system of using a pool of specialist AML/CFT supervisors within the wider population of supervisors is a flexible way of using its resources. Whilst the assessors share this view, Singapore is encouraged to keep the level of resource assigned to ML/TF supervision under review, especially in the light of any shift in areas of focus that might arise from the revision of the NRA.

ii. DNFBPs

348. All of the competent authorities and SRBs supervising each sector demonstrated that they take account of risks identified respectively. In order to ensure effective resource allocation in conducting inspections, they indicated that they put priorities by: (i) volume or amount; (ii) size of practitioner; and (iii) type of customers dealt with (e.g. foreign customers). The authorities and SRBs emphasise that, with the exception of TSPs and lawyers, AML/CFT supervision in the DNFBP sector has started in recent years (i.e., the initial AML/CFT inspection was in 2012 (casinos), March 2015 (real estate agents), May 2015 (accountants and CSPs), and that they are going to enhance their inspections. Since 2010, the Law Society conducted AML/CFT inspections at the rate of five law firms per year. The team acknowledged that the authorities and SRBs have their agendas and future plans for AML/CFT supervision.

349. The competent authorities and SRBs in charge of DNFBPs do not have any uniform supervisory tools, given the different agencies in charge (and the differences in business profiles and risks of the various sectors). Each of them indicated that they have a unit exclusively in charge of

AML/CFT inspection. The inspectors have been trained through in-house training courses, and the ACRA, CRA and IPTO indicated they have officers with professional experience in police units.

350. As explained above, except for casinos, the numbers of STR filed by the DNFBPs in the last few years are very low, especially when compared with the numbers of practitioners (see Chapter 5). Nevertheless, the competent authorities and SRBs emphasised that they have been encouraging the sector to file STRs through their outreach. The low numbers of STRs was mainly attributed to the nascent stage of AML/CFT implementation in these sectors. The team has the impression that advice from the competent authorities and SRBs does not necessarily satisfy the needs of individual DNFBPs when confronted with actual cases.

351. With the exception of IPTO for pawnbrokers, there are no designated competent authorities for PSMDs and they are not subject to either licensing or registration. Therefore, anyone can start a PSMD's business in Singapore, without being regulated and supervised. Based on information from past surveys and engagement sessions with the PSMD trade associations, the Singapore authorities estimate that there are between 750 and 1 000 PSMD dealers in Singapore, but no accurate number exists. In addition, there is an unregulated exchange market of precious metals called "Singapore Precious Metals Exchange (SGPMX)". SGPMX was established in August 2011. SGPMX is an online precious metals exchange that claims to be backed by a physical store of bullion, and their annual turnover for 2014 was approximately USD 9.5 million. Though the SGPMX's website states a rule of not permitting cash payments, neither the Singaporean authorities nor the team have confirmed whether these measures are in line with the FATF standards. SGPMX itself states on its website that it is not supervised by MAS. The continuity of ownership of the gold between first seller and last buyer is unknown to the authorities. The authorities emphasise that they recognise the PSMD sector as vulnerable to various ML/TF threats and that they are considering a policy response. They are currently collecting information and data. The team shares this view and ML/TF risks that this sector presents for both in terms of retail and wholesale should be addressed as soon as possible. This is especially true taking into account of the fact that Singapore is an international commodity trade hub with a free port, special no-tax measures for gold trading and local exchange market of precious metals such as the SGPMX.

Remedial actions and effective, proportionate, and dissuasive sanctions

i. Financial institutions

352. Singapore has a range of remedial measures that it can impose on financial institutions. These range from written requests for corrective action following on-site visits, to criminal prosecutions for breaches of the Notices issued under the MAS Act. In practice, breaches of the Notices are often compounded into financial settlements, without the need for MAS to refer the matter to the AGC for criminal prosecution. Whilst not having to undertake a criminal prosecution in each case is arguably an efficient way to deal with breaches of the MAS Notices, the methodology seen by the assessors for compounding financial penalties is rigid, and could be more flexible. The guidelines suggest a level of severity for each transgression, with the penalty for each transgression fixed as a percentage of the maximum fine that would be available on prosecution. For example, the percentage of the fine available for breaches by capital markets intermediaries is lower than that available for banks. MAS explained that capital markets intermediaries are generally less well-resourced than the banking sector, and thus the potential impact of a sanction is greater. However,

as some capital markets intermediaries are global financial institutions, the potential limit on financial penalties is a concern. MAS considers that the system is flexible, as sanctions are available per breach and sanctions imposed may and have exceeded the guidelines in some cases. However, examples seen of enforcement actions to date suggest that penalties are imposed for specimen breaches. The maximum financial penalty imposed at the time of the on-site was SGD 800 000 (approx. EUR 527 680 / USD 561 680), and most are considerably lower[46].

353. The assessors noted that no direct action had been taken against senior management in an FI at the time of the on-site, despite repeated mention of the importance of senior management accountability/responsibility throughout MAS's Notices and Guidelines[47]. At least one example of enforcement action shared with the assessors gave rise to concerns about senior management oversight. MAS considers that its powers are dissuasive, even if not formally used, pointing to examples of FIs removing senior management staff on their own account after MAS inspections and other supervisory actions. The assessors consider that MAS should review the effectiveness of its enforcement policy, given the current level of use of the tools at its disposal.

[46] Following the on-site, Singapore reported that MAS had imposed financial penalties amounting to SGD 13.3 million in May 2016 on a bank for AML/CFT breaches. MAS also directed the bank to cease operations in Singapore.

[47] Following the on-site visit, Singapore reported that in 2016 MAS dealt with one case in which it referred 6 members of a bank's senior management and staff to the Public Prosecutor to evaluate whether they have committed criminal offences.

Table 26. **MAS remedial actions against financial institutions**

	2011	2012	2013	2014	2015 (to October)
BANKS/FINANCE COMPANIES	**15**	**29**	**42**	**44**	**15**
Reports requiring remediation	14	26	34	38	11
Warnings and reprimands	0	2	4	5	0
Restrictive actions	0	0	4	0	0
Composition fines	1	1	0	1	4 (plus 3 pending)
Maximum/Range of fines	**SGD 200 000**	**SGD 350 000**	**-**	**SGD 450 000**	**SGD 300 000 – 800 000**
Revocation/non-renewal of licence	0	0	0	0	0
PRIVATE BANKS / PRIVATE BANKING OPERATIONS	8	9	15	14	4
Reports requiring remediation	8	9	13	14	2
Warnings and reprimands	0	0	2	0	0
Restrictive actions	0	0	0	0	0
Composition fines	0	0	0	0	2
Range of fines (in SGD)	-	-	-	-	**SGD 300 000 – 800 000**
Revocation/non-renewal of licence	0	0	0	0	0
DIRECT LIFE INSURERS	**3**	**4**	**4**	**4**	**2**
Inspection reports requiring remediation	3	4	4	4	1
Warnings and reprimands	0	0	0	0	0
Restrictive actions	0	0	0	0	0
Composition fines	0	0	0	0	1 (plus 3 pending)
Range of fines					**SGD 125 000**
Revocation/non-renewal of licence	0	0	0	0	0
MONEY-CHANGERS AND REMITTANCE AGENTS	**17**	**15**	**9**	**0**	**8**
Inspection reports requiring remediation	10	9	4	0	0
Warnings and reprimands	0	0	0	0	0
Restrictive actions	0	0	0	0	4
Composition fines	5	2	3	0	4
Range of fines	**SGD 4 800 – 27 750**	**SGD 33 500 – 40 000**	**SGD 5 000 – 27 900**	**-**	**SGD 1 000 – 36 000**
Revocation/non-renewal of licence	2	4	2	0	0

	2011	2012	2013	2014	2015 (to October)
CAPITAL MARKETS ENTITIES	**13**	**7**	**27**	**333**	**14**
Inspection reports requiring remediation	10	4	21	330	4
Warnings and reprimands	0	2	5	2	7
Restrictive actions	2	0	0	0	1
Composition fines	1	1	1	1	2
Range of fines	**SGD 50 000**	**SGD 187 500**	**SGD 25 000**	**SGD 300 000**	**SGD 40 000**
Revocation/non-renewal of licence	0	0	0	0	0

ii. DNFBPs

354. Laws and regulations that apply to the DNFBP sector include a range of sanction or remedial measures, such as a warning letter, financial penalties, and a revocation/suspension of license/registration. The maximum amounts of financial penalties appear disproportionate and possibly not dissuasive in comparison with those in financial sector and between the various categories of DFNBPs (see table below and discussion regarding R.35 in the TC Annex). The competent authorities and SRBs offered various reasons why simple comparison is however not reasonable because: (i) often the penalty is imposed on individual practitioner or salesperson in case of DNFBPs, whereas a penalty is imposed on a financial institution as an entity; and (ii) the impact of the sanction needs to be assessed in its totality taking into account other sanctions available, such as revocation and suspension of licenses.

Table 27. **Financial penalties for the various categories of DNFBPs**

Type of DNFBP	Maximum amount of financial penalty (SGD)	Statute
Financial institutions	1 000 000 (per breach)	MAS Act (Section 27B)
Accountants	100 000	Accountants Act (Section 53(2)(d))
Real Estate Agents	75 000	EAA (Section52(3))
CSPs	25 000 (per breach)	ACRA Act (Section 28F(13)(d))
Casinos	A sum not exceeding 10% of the casino operator's gross gaming revenue, or 1 000 000 (per breach)	CCA (Section 54 (1)(d))
Pawnbrokers	100 000 (per breach)	Pawnbrokers Act (74(6))

355. The team acknowledges that the argument made by Singapore is valid, but considers it premature to draw that conclusion. There are some cases involving TSPs where remedial actions and sanctions have been taken, however other than remedial actions against casinos and lawyers there have been no cases in other DNFBPs. In addition, the cases for casinos and lawyers are not concerning significant breaches of laws and regulations, but they rather relate to a delay in filing of a cash transaction report, and a case of suspension of a lawyer from practice due to non-cooperative attitude to AML/CFT inspection. In this regard, it is hard to conclude that the remedial system has been functioning in an effective and a full-fledged manner for all DNFBPs. Other than TSPs and

casinos, the low numbers of inspections of most DNFBPs and the low numbers of STRs filed also justify this conclusion.

Impact of supervisory actions on compliance

i. Financial institutions

356. MAS and IPTO appear to be well-respected, and the FIs spoken to welcome the interaction they have with them. MAS considers that its routine, thematic and events-driven work has led to improvements in overall compliance by the FIs it supervises. Most MAS enforcement action has been aimed at ensuring changes to FIs' behaviour, and includes a thorough system of follow-up for remedial action through external auditors' reports or follow-up visits. MAS gave the example of the tax review carried out in 2012 and 2013 as an area where compliance had improved. This exercise involved the exiting of 22 431 accounts in the banking sector, and a total of 2 988 STRs being filed across the banking, insurance and capital markets sectors. MAS subsequently undertook industry outreach and issued guidance on how FIs should handle tax risk. While the authorities consider that they had assessed the outward flows of information in the context of private banking, it does not, however, appear that the authorities have extracted the maximum value from this exercise, such as information on the flows of money into and out of the accounts.

ii. DNFBPs

357. The authorities and SRBs stressed that their efforts help improve awareness of ML/TF risks in each sector. However, except for the TSP and casino sector, their outreach activities are limited in number and scope (see the following sub-section), and it is hard to find them sufficient. This is also further supported by the fact that only a few numbers of STRs have been filed by the DNFBP sector except TSPs and casinos.

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

i. Financial institutions

358. MAS uses a variety of means to promote an understanding by FIs of their AML/CFT obligations. Examples include:

- Guidelines on AML/CFT Notices,
- Guidance/best practices papers on specific issues, such as Guidance on Private Banking Controls issued in 2014, and Guidance on AML/CFT Controls for Direct Life Insurers issued in 2015, Guidance on AML/CFT Controls on Trade Financing and Correspondent Banking in 2015.
- Joint guidance papers with industry, such as the Association of Banks in Singapore (ABS)'s Guidelines on Tax Crimes and the Private Banking Industry Group's Industry Sound Practices
- Industry engagement, such as conferences and joint exercises with STRO.

359. IPTO has issued a narrower set of guidelines on the outcomes of the NRA and STR filing requirements. FIs found both supervisors' outreach useful. In addition, FIs found the regular interaction with MAS and IPTO useful in deepening their understanding of AML/CFT issues.

360. AML/CFT obligations appear to be clearly understood in most sectors. The promotion of understanding of ML/TF risks is less apparent in the money lenders sector than it is for FIs. In addition, the moderate shortcomings in Singapore's understanding of ML/TF risk identified in IO 1 has some implications the effectiveness of measures taken to promote understanding of ML/TF risk.

ii. DNFBPs

361. The authorities and SRBs have demonstrated what they have addressed and the progress since the 3rd round MER was adopted. The outreach program includes: (i) regular dialogue between practitioners and supervisors (real estate agencies, pawnbrokers), (ii) seminars designed for various levels of officers (real estate agencies, lawyers, CSPs, accountants and pawnbrokers), (iii) distribution of self-assessment checklist (real estate agencies); (iv) distribution of red-flag indicators (all DNFBPs); and (v) e-learning course (accountants). Some of the SRBs and authorities produce and distribute their own guidelines and information guide (e.g. Salespersons Guide by CEA for real estate agencies, Practice Direction by the Law Society for lawyers and Information Guide on the Prevention of ML and TF for pawnbrokers), so that practitioners and salespersons have a better understanding of their tasks in relation to AML/CFT obligations.

362. The team confirmed that the authorities and SRBs have a clear perspective and agenda to further promote understanding of ML/TF risks and compliance with the AML/CFT obligations. For example: (i) the CRA is strengthening on-site inspections in casinos; (ii) the ACRA is enhance its training programmes for accountants and CSPs; and (iii) the CEA is going to enhance their inspection on small- or medium-size agencies in the real estate sector. Given that disparities are observed in the progress and contents of the AML/CFT programmes by sector, however, there is a need for enhanced awareness raising of AML/CFT to all individual practitioners, including PSMDs. At the same time, practitioners also need a detailed and well-tailored programme for individual types of customers and transactions.

363. Although financial sector supervision by MAS is generally of a satisfactory level, some areas of improvement are required, as set out above. In addition, IPTO supervision of money lenders requires improvement. The less robust and more recent supervision of parts of the DNFBP sector (except for casinos and TSPs) has a negative impact on the overall rating.

364. ***Singapore has achieved a moderate level of effectiveness for IO.3***

CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS

Key Findings and Recommended Actions

Key Findings

1. Singapore has not undertaken A ML/TF risk assessment of all forms of legal persons and legal arrangements.
2. Authorities acknowledge that legal persons and arrangements created in Singapore, and registered or operating in Singapore from foreign jurisdictions, can be used to facilitate predicate crimes and ML/TF offences. However, there is no consistent and coherent understanding within the government and the private sector of the inherent and residual risks associated with legal persons and arrangements.
3. LEAs have not pursued investigations into ML in relation to companies other than shell companies.
4. While Singapore has put CDD measures in place requiring CSPs (including lawyers and accountants) and LTCs to collect beneficial ownership information, in practice the collection of beneficial ownership information is not always possible. And, it is not uniformly clear from the private sector in what circumstances new or existing accounts with legal persons and arrangements would be refused when that information is not available.
5. There are no measures in place to mitigate the risk posed by bearer shares and bearer share warrants permitted to be issued by foreign companies under their originating jurisdictions.

Recommended Actions

Singapore should:

1. Conduct comprehensive ML and TF risk assessments for all types of legal persons (private companies, public companies, foreign companies, etc.) to identify where the risks are and develop policy to address those risks.
2. Ensure that minimal information on the creation of legal arrangements, including those that file tax returns with IRAS, is publicly available.
3. Enact and implement measures to mitigate the ML/TF risk posed by bearer shares and bearer share warrants which foreign companies may issue in Singapore.
4. Enact and implement measures to mitigate the ML/TF risk posed by nominee directors and nominee shareholders as well as nominee partners and nominee managers (for LLPs).
5. More effectively supervise FIs and DNFBPs for compliance with CDD requirements in relation to legal persons and legal arrangements and where appropriate impose proportionate and dissuasive sanctions.
6. Enact mitigating measures to address the risk posed by foreign companies permitted under the jurisdiction in which they are formed to issue bearer shares/warrants within Singapore.

365. The relevant Immediate Outcome considered and assessed in this chapter is IO5. The recommendations relevant for the assessment of effectiveness under this section are R24 & 25.

Immediate Outcome 5 (Legal Persons and Arrangements)

375. As indicated in the TC annex the process for the creation of legal persons and for obtaining and recording basic ownership information is set out in the Companies Act and the Limited Liability Partnerships Act. Mechanisms for the obtaining or recording of beneficial ownership information (as that term is defined by FATF) beyond the immediate shareholder of a company or a direct interest in a LLP are publicly available.

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

376. Authorities (including ACRA, CAD, MOF, IRAS, Minlaw, AGC and MAS) acknowledge that legal persons and arrangements created in Singapore, and registered or operating in Singapore from foreign jurisdictions, can be used to facilitate predicate crimes and ML/TF offences. However, there is no consistent and coherent understanding within the government and the private sector of the inherent and residual risks associated with legal persons and arrangements.

377. "Shell companies," defined in the NRA report as Singapore registered companies with minimal paid-up capital and no legitimate business objective, were assessed to pose a high risk of ML and TF in Singapore. The NRA was supported by a number of cases involving shell companies and the unique manner in which they have been used for ML (primarily for cheating offences). However, apart from shell companies, the ML/TF risks posed by other types of legal persons (public, foreign, etc.) was assessed for ML and TF risk in the NRA nor were any cases provided to the assessment team which indicated how they have been used to facilitate money laundering and/or terrorist financing.

378. ACRA produced an undated document referred to as *ACRA's risk assessment of legal persons* to the assessment team on 30 November 2015 during the on-site visit. That document outlines a process in 2013 during production of the NRA, where ACRA examined the risks posed by other forms of legal persons. This document is not a comprehensive assessment of all forms of legal persons in Singapore. Nor is it clear that the results of the exercise outlined in the document were shared with other government agencies or the private sector.

379. While Singapore has acknowledged the risks posed by shell companies, no statutory measures have been enacted in the Companies Act to mitigate the risk identified and posed by those companies in Singapore.

Mitigating measures to prevent the misuse of legal persons and arrangements

380. Singapore has implemented some preventive measures designed to prevent the misuse of legal persons and arrangements for ML and TF. In particular, CSPs (including lawyers and accountants) are subject to AML/CFT regulations which require them to perform the same CDD as financial institutions when engaging existing and new customers (section 28F(9) of the ACRA Act and Part II of the First Schedule to the ACRA [Filing Agents and Qualified Individuals] Regulations 2015, paragraphs 8 to 10 and 18). Beneficial ownership information held by CSPs is

required by law to be up-to-date and relevant. This information extends to the natural person behind any legal person.

381. While Singapore has put CDD measures in place requiring CSPs (including lawyers and accountants) to collect beneficial ownership information, in practice CSPs as well as lawyers and accountants indicated that the collection of beneficial ownership information is not always possible (for instance in the case of foreign companies). Yet, they did not view this barrier to collection of that information as a necessary impediment to on-boarding clients. It was indicated that they would deal with each case on its own facts. Conversely, it is not uniformly clear from the private sector in what circumstances new or existing accounts with legal persons and arrangements would be refused where there is a failure to collect that information.

382. While the CDD obligations noted above apply to CSPs (including lawyers and accountants), Singapore acknowledged that companies can be formed by local persons in Singapore who are not CSPs. Companies cannot be formed by persons not in Singapore as a *Singpass* is required. Persons with a *Singpass* who form companies and are not CSPs are not subject to AML/CFT requirements. No information was provided on the extent to which the creation of legal persons in Singapore in those circumstances, collect beneficial ownership information. Singapore indicated that most of the companies formed in the country are done through the use of a CSP. Foreigners wishing to incorporate companies in Singapore must go through a CSP who will be required to collect beneficial ownership information. Foreigners cannot incorporate without the use by a CSP of a *Singpass* (it is an offence to provide a *Singpass* number to anyone in an unauthorised manner). Where a foreigner does not act as a director and appoints a local to act as a director, that beneficial ownership information would not be collected. However the local director would be easily identified as the primary offender for the illegal acts committed by the company and would be prosecuted and punished as such.

383. ACRA has the power to require CSPs to provide information obtained by CSPs under section 31(1D) of the ACRA Act when investigating breaches of a CSP's terms and conditions of registration. These powers do not extend to trust arrangements.

384. Singapore permits the use of nominee directors and shareholders for companies as well as nominee partners and nominee managers for limited liability partnerships but, with no disclosure requirements or mandatory licencing and no other mitigating measures to address the risks posed by these nominees, Singapore cannot be said to have mitigated the ML and TF risks in those areas.

385. Moreover, while Singapore prohibits the issuance of bearer shares and bearer share warrants for companies formed in Singapore, there are no mitigating measures in the Companies Act or elsewhere to address the risk posed by the same instruments that may be issued by foreign companies registered in Singapore but permitted under their originating jurisdiction to issue those same types of bearer instruments.

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

386. With respect to legal persons:

- Basic information of all entities registered with ACRA is available from ACRA;

- Police can obtain accurate and current basic information on legal persons through ACRA without a search warrant. Police can obtain further information from FIs and DNFBPs, including CSPs, with a warrant and from the company itself;
- STRO has power to require any person, including DNFBPs and FIs, to disclose any document or information it may require for its analysis, including: (i) information on the beneficial owner of a company; and (ii) information from land and home ownership registries;
- IRAS can obtain information from DNFBPs and FIs under statutory powers. From 1 January 2012 to 31 December 2014, IRAS responded to 82 requests from foreign jurisdictions for information of legal persons.

387. All of the information obtainable from FIs and DNFBPs may not include beneficial ownership information notwithstanding that FI and DNFBPs are required to collect that information (see 5.2).

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

388. With respect to legal arrangements, authorities have the same powers where a trust uses the services of a FI or DNFBP.

389. With respect to trustees of legal arrangements, there is no general obligation on them (trustees) to collect beneficial or beneficiary information and so authorities may not be able to secure adequate, accurate and current basic and beneficial ownership information on all types of legal arrangements created in Singapore. In the case of foreign trusts where the trustee is overseas, this information, if held, would only be available through formal or informal cooperation mechanisms, which may not involve the timely exchange of that information.

390. And while a trustee (including the trustee of a foreign trust) is required to file a trust tax return in Singapore when a trust earns income, the return may disclose beneficiaries or beneficial owners but only when income from the trust is distributed to beneficiaries of the trust. Otherwise, no information is required to be filed with IRAS on the beneficial owners of trusts. Coupled with the fact that trustees are not required to collect that information and to hold it, it would not necessarily be available to provide, if requested.

Effectiveness, proportionality and dissuasivness of sanctions

391. In the last five years there have been eight (8) cases where sanctions have been applied on FIs for failure to collect proper beneficial owner information in relation to legal persons as follows:

Table 28. **Sanctions on FIs for failure to collect proper beneficial owner information for legal persons**

	2011	2012	2013	2014	2015 (June)
Warnings /reprimands	0	0	0	3	0
Restrictive actions	0	0	0	0	0
Composition fines	0	1	0	1	3
- Fine amounts[1]	0	SGD 350 000	0	SGD 450 000	SGD 350 000 SGD 800 000 SGD 300 000
Revocation/non-renewal of licences	0	0	0	0	0
Warnings /reprimands	0	0	0	3	0

Table Note:

1. Amounts indicated in this table relate to total financial penalties, including for BO breaches.

392. No sanctions have been applied against DNFBPs (CSPs, lawyers and accountants) and no sanctions against FIs and DNFBPs have been applied in relation to failure to collect the same information in relation to trusts.

393. ***Singapore has achieved a moderate level of effectiveness for IO.5***

CHAPTER 8. INTERNATIONAL COOPERATION

Key Findings and Recommended Actions

Key Findings

1. Singapore provides a range of international cooperation, including MLA, extradition, intelligence/information, and beneficial ownership information. The quality of assistance is high, often supporting complex investigations and helping to secure convictions.
2. Few outgoing requests for MLA have been made prior to 2015, especially in comparison to the number received and considering Singapore's status as a financial centre and its vulnerability as a transit point for illicit funds. Singapore has taken steps to increase outgoing MLA requests in 2015, more than doubling the entire number of MLA requests in the previous 3 years. LEAs, STRO and financial supervisors are generally well engaged in making and receiving requests. Particularly, CAD, SPF and CNB uses informal cooperation effectively, making a significantly larger number of outgoing requests compared to incoming requests.
3. Singapore faced occasional challenges with executing some MLA requests in a timely manner. Singapore indicates that since the 3rd round mutual evaluation, it has adopted a policy of positively responding to requests as far as possible; time is often taken to seek clarifications to facilitate the processing of requests which do not contain sufficient information. However, delays can also be caused by strict interpretation of the MACMA or a lack of resources to deal with an increasingly complex caseload.
4. Asset restraint can be conducted quickly using domestic LEA powers; however this channel requires that LEAs conduct a domestic ML investigation. Using the MACMA restraint provisions is an alternative, a process that takes longer because of the requirement for an order of the High Court. Singapore shares beneficial ownership information for legal persons and arrangements in response to a foreign request, although this is limited because Singapore can only share information that is required to be available in Singapore.

Recommended Actions

1. Singapore should continue to systematically use MLA to follow and restrain assets that have moved to other jurisdictions, and pursue the people involved.
2. Improve response times in responding to foreign requests, whether through changes to laws or SOPs, additional training or resources, or enhanced engagement with relevant countries.
3. Foster trust and connections with foreign counterparts, for example by continuing training events, posting of LEA liaison officers in foreign jurisdictions as appropriate, and joining practitioner networks (e.g. ARIN-AP).

4. TC issues: Singapore should revise the legal framework to ensure that instrumentalities "intended for use" in ML, predicate offences or TF are captured, and that a range of investigative techniques are available in the context of MLA requests. Continue efforts to extend extradition to a broader set of countries of greater risk, and to ensure that current treaties are up-to-date. Information sharing by STRO should be broadened to a larger number of countries, including those of greater risk. For example, STRO could consider using the Egmont Charter and "Principles for Information Exchange" as basis for information sharing and spontaneous disclosures.

394. 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

391. All incoming and outgoing requests for mutual legal assistance (MLA) and extradition are coordinated by a team of 15 legal officers in the International Affairs Department (IAD) of the Attorney-General's Chambers (AGC), the designated Central Authority. Singapore uses an electronic case management system and SOPs to manage the prioritization and processing of inbound and outbound MLA and extradition requests; the system will prompt case officers on deadlines and outstanding requests from domestic LEAs.

392. The legal framework for MLA as set out in the Mutual Assistance in Criminal Matters Act (MACMA) is generally broad. Singapore can provide MLA to another country on the basis of bilateral treaties, the ASEAN treaty on MLA and on the basis of reciprocity. Dual criminality is a mandatory ground for refusal, although recent amendments have lifted the dual criminality requirement for foreign tax evasion in cases where there are cooperation agreements and in non-coercive measures.

393. Between 2011 and 2014, Singapore received 179 requests relating to ML and predicate offences, 79 of which had a ML aspect. There was one request relating to TF. Consistent with Singapore's role as a global financial centre, the types of assistance most frequently requested from Singapore are the production of documents (usually bank records) and the restraint of assets (usually financial assets). Of note, incoming MLA requests doubled in 2013 and are expected to remain at this higher level. Authorities indicated that this trend is due to two main factors, the legislative changes and SOPs that have broadened the legal basis and lowered the restrictions for Singapore to provide assistance, and the increased capacity of some requesting countries that has introduced new partners in international cooperation. Singapore reacted to the increase with improvements to its: (i) processes; (ii) allocation of resources; and (iii) use of information technology such as its case management system.

394. Over the same period, Singapore made 14 requests relating to ML and predicate offences, five of which involved ML. There were no MLA requests relating to TF. ISD exchanges information with its international counterparts directly through their established intelligence channels. Singapore indicated that the reason for the differential between incoming and outgoing requests was that they were able to obtain the needed evidence through other means and that they rely upon

exchanges between FIUs and LEAs. Singapore's status as a global financial centre and its vulnerability as a transit point for illicit funds from foreign predicates suggest that outgoing MLA requests would still be needed, in particular MLA requests for bank account information and the restraint of assets. Singapore has taken steps to increase MLA requests: in 2015, 20 formal requests were sent out as at the time of the on-site in December 2015. The requests that are sent are of high quality.

395. Between 2011 and 2014, 16 extradition requests were received, 11 of which were executed. In the same period, Singapore made 44 extradition requests, 38 of which were executed. Cooperation on incoming requests is limited due to the legal framework, in particular the coverage of some higher risk countries (see Recommendation 39). The simplified process for "backing of warrants" between Singapore, Malaysia and Brunei Darussalam has allowed for requests to be addressed on an LEA to LEA basis, in an average time of five days. Extradition cases have been expedited where the facts of the case have demanded urgent action, such as if the fugitive may flee the jurisdiction or where the fugitive is transiting Singapore.

Table 29. **MLA and Extradition: ML and Associated Predicate Offences (as at 23 July 2015)**

Types of requests/Year request received	2011	2012	2013	2014	TOTAL
Extradition					
Requests received	**3**	**5**	**1**	**7**	**16**
Executed	1	3	1	6	11
Declined	2	2	0	1	5
Requests made	**6**	**9**	**9**	**20**	**44**
Executed	5	5	9	19	38
Declined	1	0	0	0	1
Mutual legal assistance					
Requests received	**31**	**31**	**63**	**54**	**179**
Executed	28	25	47	32	132
Declined	0	0	3	3	6
Withdrawn	15	3	3	5	26
Requests made	**0**	**4**	**5**	**5**	**14**
Executed	0	1	4	1	6
Declined	0	1	0	0	1
Withdrawn	0	1	0	1	2

396. Between 2011 and 2014, Singapore received approximately 64 MLA requests to restrain assets, and 24 MLA requests for confiscation. In over ten cases, AGC obtained the restraint order using the powers under MACMA. However, for a large number of these requests, even where the legal requirements were complied with, restraint/confiscation was not possible as there were no funds in Singapore, or funds had been moved out of Singapore prior to the request.

397. Assets can be restrained quickly using domestic LEA powers, rather than the MACMA provisions. The Central Authority and the relevant law enforcement agencies review all incoming

MLA requests. If the facts indicate that an ML offence was committed in Singapore, Singapore will initiate a domestic investigation and restrain the assets using CPC powers. Where a joint investigation team (JIT) or parallel investigation is established, they can subsequently use informal channels to exchange information. This approach has worked in countries where international cooperation relationships are well established and where there are informal channels to exchange the information. Where this is not possible, asset restraint through the MACMA is required a process that takes longer because of the requirement of a High Court order. In total, an estimate of SGD 194 222 719 (approx. EUR 127 999 700 / USD 136 247 104) has been seized and an estimate of SGD 6 251 785 (approx. EUR 4 414 502 / USD 4 698 941) has repatriated through confiscation proceedings in Singapore or through LEA's facilitation of asset repatriation.

398. Singapore has made over ten MLA requests for restraint of assets amounting to more than SGD 11 491 139 (approx. EUR 7 579 555 / USD 8 067 92)9. As indicated above, this amount is low considering the risk profile of Singapore.

Table 30. **Assets restrained and repatriated in SGD**

	Year request received				
Types of requests[1]	**2011**	**2012**	**2013**	**2014**	**TOTAL**
Assets seized	62 642 177	2 684 152	110 066 404	19 829 986	194 222 719
Assets Repatriated/Shared	0	2 041 144	3 469 966	740 675	6 251 785

Table Note:

1. The assets restrained and repatriated included amounts in SGD, USD, and Euros. Values have been converted to SGD, as at April 2016.

399. The quality of assistance provided by Singapore is high, as was confirmed from feedback received from 45 countries. Evidence provided and obtained through MLA channels has helped to secure convictions, and restrain and confiscate assets. Singapore has developed a constructive approach to facilitate MLA. Information on the legal requirements and electronic templates for filing MLA requests is available on the Internet and case officers will provide clarifications and guidance in advance. Within a few days of receiving the request, contact details (e-mail addresses and telephone numbers) of the assigned case officer of the Central Authority are sent to the requesting authority or competent domestic agency. Where MLA requests do not meet the legal requirements or the information is unclear, case officers work with the requesting country to remedy these shortcomings and have introduced LEAs and STRO to support the gathering of needed intelligence to support the request. For complex cases, as well as where the requesting country finds it useful, case officers make themselves available for consultations with their counterparts, whether face-to-face meetings or video or telephone conferencing. The authorities indicated that these factors, together with the revisions in the laws, have helped to lower the number of refusals to less than 2%. Case officers are described as professional, courteous and responsive.

400. Singapore has a framework in place to expedite requests, including broad mechanisms for submission of the request (can be submitted by e-mail, mail or fax, in addition to diplomatic channels), SOPs and flowcharts which address the prioritization of requests, an electronic case

management system that flags deadlines with case officers, and close domestic coordination that allows for the case officers of the Central Authority to work closely with LEAs and the Ministry of Law to respond quickly. Singapore provided examples of swift action – within hours or days – including in cases involving the restraint of assets.

401. Singapore faced occasional challenges in executing requests in a timely fashion. Delays were noted in the feedback from several countries, including countries with established/frequent cooperation with Singapore. A few stated this directly, including two that mentioned delays of up to two years; others referenced a number of cases that remained open after two years. Singapore authorities explained that some of the feedback could be due to misunderstandings, which it has sought to clarify with some of the countries. They also explained that a significant proportion of this time is spent in communications and seeking clarification from the requesting country, especially when the original requests does not provide sufficient information or the facts do not support the assistance sought. Where possible, the Singapore authorities will provide assistance in part, dealing with the executable components of the request, while awaiting further information. Singapore reports that the average turnaround time for incoming MLA requests calculated from the date of receipt of the request was 9 months in 2013 and 8.3 months in 2014. Once the requesting country has provided sufficient information, non-urgent requests requiring court orders may take up to four months, whereas non-coercive assistance would take a significantly shorter time.

402. Other data suggests that the delay is also on the Singapore side. The feedback from a few countries suggests that in some cases, there has been an overly strict interpretation of the legal requirements of MACMA. For example, countries indicated that they were asked to provide exact dates for transfers, and exact amounts of money involved, or the link between the account and the proceeds of crime. However, one country subsequently clarified that this was a unique case and that the challenges related to that case were not systemic. Another country noted that a response was delayed for two years due to concerns that provision of the MLA could prejudice an ongoing domestic investigation, a ground for refusal under MACMA. However, Singapore kept that country regularly updated on the status of the matter and the domestic investigation resulted in successful prosecution as well as successful repatriation of assets to that country. The requirement for statutory notice to the Ministry of Law and approval by the Minister was also cited as a possible delay by one country; however Singapore indicates that responses are usually obtained within two weeks. These delays may ultimately hinder the usefulness of the evidence and the effectiveness of Singapore's international cooperation efforts.

403. Finally, staffing resources at the IAD are low considering the number of cases and the complexity of these cases. While staff have doubled since the last mutual evaluation, the case load has doubled and the cases are increasingly complex, require the use of a range of international cooperation mechanisms, together with parallel investigations in foreign jurisdictions (see box below as two of several examples provided).

Case Example 9. **Use of a range of international cooperation mechanisms**

Senior officials of Company X located Country A embarked on a complex scheme to avoid declaring losses arising out of a drop in the value of its investments, laundering proceeds through shell companies with the aid of a Singapore-based bank consultant. Various forms of international cooperation were used to support investigations in both countries, including:

- Request under the IOSCO MMoU for accounts used to transfer funds to shell corporations.
- Seven requests for MLA by Country A between December 2011 and May 2015 under which the following assistance was provided
    - CAD provided beneficial ownership information of a related company along with company and bank records including BO information of a related company;
    - Evidence of the bank consultant was recorded before a Magistrate;
    - Bank records for a suspect's account
    - Service of a court order on two entities and a bank in Singapore
    - Request to restrain SGD 464 000 (approx. EUR 306 054 / USD 325 774) in a suspect's personal bank account

Based on CAD's own domestic investigations, accounts containing SGD 1 374 753 (approx. EUR 906 589 / 965 214) were seized. Company X and the senior officials were convicted and there are criminal proceedings against the abettor. During the recording of the bank consultant's evidence, pursuant to the MLA request, AGC successfully contested the bank consultant's attempt to block disclosure on grounds of banking secrecy.

Case Example 10. **MLA to obtain evidence to support conviction for stolen assets and subsequent repatriation of assets**

A top civil servant in Country A had embezzled SGD 18 million (approx. EUR 11.87 million or USD 12.64 million) from his government. Singapore commenced ML investigations and the accused was convicted in Singapore for offences in relation to the stolen property laundered in Singapore and upon serving his sentence, returned to Country A to face criminal charges.

Singapore sent an MLA request to Country A pursuant to which Country A provided evidence of the predicate embezzlement offences by way of bank documents, fund remission receipts, statements of witnesses, as well as its key investigator to testify at the Singapore trial.

CAD Singapore authorities provided its investigation findings to Country A, which included asset screenings (property, casino accounts, and bank accounts), brief facts of the case and statements from the accused and his wife. Pursuant to Country A's MLA request the accused and his wife's assets (bank accounts and real property) totalling approximately SGD 4.8 million (approx. EUR 3.17 million / USD 3.37 million) were frozen.

Singapore worked closely, through face to face meetings with the authorities of Country A in the preparation of evidence and responding to legal challenges.

Singapore received the final confiscation order from Country A at the end of 2015, and asset repatriation proceedings are underway.

Providing and seeking other forms of international cooperation for AML/CTF purposes

404. STRO, LEAs and supervisory authorities generally cooperate well with their foreign counterparts. Overall, STRO, LEAs and supervisory authorities make a large number of outgoing requests, and respond positively to incoming requests. The majority of feedback from countries indicates that information and intelligence is of sufficient quality and timely. Procedures are in place to protect confidentiality, and no issues were raised in the feedback. Most indirect exchanges of information take place through STRO. STRO will request information from foreign FIUs on behalf of domestic LEAs, or STRO will provide information to foreign FIUs and – in compliance with the Egmont Principles of Exchange -- will give consent to its foreign FIU counterparts to disseminate STRO information to foreign LEAs. There are not yet examples of diagonal exchange.

FIU

405. STRO is limited in exchanging financial intelligence only with 31 MOU countries and two LOU countries, a requirement that applies even to Egmont members that have agreed to the "Principles of Exchange" platform for exchange among Egmont members without an MOU (see 40.9). This limits Singapore's effectiveness in sharing more broadly, in particular spontaneous disclosures to non-MOU/LOU countries. For countries that it can share with, the feedback complimented the cooperation from STRO, in particular the timeliness and quality of the information provided. Between 2011 and 2014, STRO made 670 requests to foreign FIUs, received 591 requests from foreign FIU, and issued 960 spontaneous disclosures. The number of spontaneous disclosures doubled in 2013 and continued at a similar level in 2014. This is due to a more proactive approach, including the sending spontaneous disclosures on the basis of information received through Interpol or MLA channels.

406. STRO has requested intelligence from foreign FIUs and foreign Interpol National Central Bureau to support STR analysis and has made subsequent disclosures to domestic law enforcement. STRO facilitates indirect exchange on behalf of domestic LEAs. In fact, the majority of STRO's requests in 2013 and 2014 were made on behalf of LEAs (236 of 244 in 2014; and 158 of 162 in 2013).

Supervisory

407. While an MOU is not required for MAS to share information, MAS has 62 MOU partners and is a signatory to the International Organisation of Securities Commissions Multilateral Memorandum of Understanding (IOSCO MMOU) and the International Association of Insurance Supervisors Multilateral Memorandum of Understanding (IAIS MMOU). MAS spontaneously shares information, including inspection reports on AML/CFT controls with the host/parent supervisor. Between 2011 and 2014, MAS made 599 requests, received 381 requests, and spontaneously shared information on 80 occasions. The significant increase in sharing in 2013 and 2014 is due to the fact that requests in relation to capital market entities are included, whereas they were not included in 2011 and 2012. The majority of these requests are fit and proper requests, but also include requests for AML/CFT inspection reports, information on the financial institution for AML/CFT purposes, and for beneficial owner information for securities and derivative transactions. MAS has also conducted joint inspections with foreign counterparts or granted inspections by foreign counterparts, on FIs in

Singapore on 23 occasions. Information is also exchanged at bilateral meetings and supervisory colleges. Where relevant, the colleges would cover AML/CFT issues and have provided useful insights on AML/CFT compliance of Singapore's FIs and allowed MAS to seek/provide observations from/to its counterparts.

408. International cooperation between supervisors of DNFBPs has not occurred, with the exception of the CRA. The CRA has 7 MOUs with foreign casino regulators. Most of the sharing has been in relation to the screening of employees.

Law enforcement

409. LEAs generally cooperate effectively with their foreign counterparts, and the number of requests made by CAD, SPF and CNB in particular are significantly larger than the number of requests they receive, (see table below). LEAs make use of foreign law enforcement attaches in Singapore (Australia, Japan, Indonesia, France, China, Chinese Taipei, Korea), as well as others based in the region. Singapore has one SPF Police Attaché posted to Indonesia who covers law enforcement issues in Indonesia and the Philippines and another in China since September 2015 – a relatively low number considering the risk profile of Singapore. Singapore is not yet a member of ARIN-AP, a regional network that shares operational information and intelligence on asset recovery cases. LEAs also participate in (and host) international conferences, which serve as platforms to gain and exchange information, expertise, knowledge and good practices, and to build relationships with foreign counterparts.

410. *CAD* - Statistics suggest that CAD routinely seeks assistance from foreign counterparts, with 1,470 requests made between 2011 and 2014, compared to 328 requests received during that same period. The types of assistance that CAD seeks from its foreign counterparts include statements from witnesses or other entities involved, information as to whether police reports have been lodged or if an investigation is also taking place in the foreign country for crimes with cross border elements, company registration records and other company information and information as to whether suspects have criminal records outside Singapore. CAD has also been successful in the use of joint investigative teams (JITs) or parallel for co-operative investigations with foreign counterparts, resulting in convictions, asset restraint and confiscation. Between 2011 and 2014 a total of 126 joint investigations have taken place: 124 of these were with the United States, one was with China, and one was with Switzerland. CAD also cooperates closely with the United Kingdom and Hong Kong, China and has conducted parallel investigations with a larger group of countries on a range of offences, including investigations on ML, embezzlement, and tax fraud.

411. CAD has also actively engaged several foreign counterparts to discuss ML threats and trends (e.g. money mules), and to highlight to its foreign counterparts any suspicious fund flows into or out of Singapore. CAD has an established bilateral meeting with its Malaysian counterpart on a regular basis, and has organised International Economic Crime conferences for ASEAN countries annually since the 1990s. During such engagements, CAD also discusses appropriate action to be taken in investigations, including requesting foreign law enforcement agencies to consider commencing investigations in their country. For example, an investigation into money laundering in a foreign country could facilitate the tracing of criminal proceeds remitted from Singapore to that country. Where appropriate, this is followed up with an MLA request to the foreign country.

412. *CPIB* - CPIB cooperates well with anti-corruption agencies in the region, in particular Malaysia, Brunei, Indonesia, and Hong Kong, China, as well as other foreign law enforcement agencies in the United States, Australia and the United Kingdom. CPIB signed the South East Asia - Parties against Corruption (SEA-PAC) MOU, which provides a forum for CPIB to share operational information with its MOU partners. In addition, CPIB and the Malaysian Anti-Corruption Commission have established a bilateral working group for the purpose of intelligence-sharing and conducing joint operations. Between 2011 and 2014, CPIB made 31 requests for assistance; compared to 76 requests for assistance from foreign jurisdictions – 8 of which involved ML -- during that same period. Five joint investigations were conducted.

413. *SPF* - SPF has signed 19 MOUs with relevant foreign counterparts and is a member of INTERPOL and ASEANAPOL. The SPF is the designated INTERPOL National Central Bureau (NCB) for Singapore, the contact point for the 189 INTERPOL member countries. Using this channel, SPF made 6,086 requests for assistance between 2011 and 2014 and received 3 745 requests from foreign counterparts. They have also participated in JITs. In addition to attending and organising international meetings and conferences, SPF also has regular bilateral meetings with its strategic counterparts. These include law enforcement agencies in Australia, Brunei, China, Malaysia and Vietnam.

414. *CNB* - CNB works closely with foreign drug enforcement agencies, in particular Malaysia, Australia, and the United States, and is an active participant in the ASEAN Senior Officials Meeting on Drugs and the ASEAN Ministerial Meeting on Drugs. Between 2011 and 2014, CNB made 389 requests for assistance and received 134 requests for assistance from foreign jurisdictions. CNB has also conducted joint operations with countries in the region such as Malaysia, Indonesia, Thailand, Cambodia and Lao PDR.

Other

415. *IRAS* - IRAS uses a number of bilateral tax treaties to facilitate sharing, including 76 avoidance of double taxation agreements and one tax information exchange agreement, on the basis of reciprocity. Between 2011 and 2014, IRAS made 134 requests for assistance (out of which 13 were in respect of suspected tax evasion cases) and received 643 requests for assistance from foreign jurisdictions, suggesting that IRAS could be more proactive in seeking information from foreign counterparts. IRAS has regular contact with jurisdictions with which it has significant exchanges to discuss requests which may be complex or unclear, as well as to exchange views pertaining to Exchange of Information (EOI) matters. For requests that are unclear, IRAS seeks clarification from the respective treaty partners. IRAS has never declined a request for information.

416. An EOI committee, comprising the Deputy Commissioner of International, Investigation & Indirect Taxes group, Assistant Commissioner of Investigation and Forensics Division, IRAS' Chief Legal Officer and Director (ITAR), monitors and evaluates performance of EOI on a monthly basis. The EOI Committee also meets and discusses major EOI issues (including complex EOI cases) with the operational team on a regular basis to ensure that EOI issues/cases are resolved expeditiously.

417. *Customs* - Singapore Customs makes EOI requests to foreign jurisdictions to assist in its investigations into suspected customs offences. Between 2011 and 2014, Customs made 21 requests for assistance from foreign jurisdictions and received 643 requests, suggesting that Customs could be more proactive in seeking information from foreign counterparts. The feedback from countries

was mixed: two countries indicated that the assistance was timely and of good quality; two countries noted that Singapore Customs could improve in sharing information, with one country noting that a number of requests remain outstanding. These exchanges are done bilaterally as well as through regional and international fora such as the Regional Intelligence Liaison Office (RILO) under the World Customs Organization (WCO). For exchange of information on traders, Singapore Customs can do so in accordance with the terms of international agreements, or upon obtaining the consent of traders for the exchange of their information, a provision which Singapore indicates has not blocked the exchange of information in practice.

418. *ISD* - ISD has intelligence exchanges with other foreign services on security matters related to terrorism (including terrorism financing). Between 2011 and 2014, ISD received 19 requests for assistance in a TF case, and it has made 4 requests.

Table 28. **Other types of international cooperation – requests received and made**

Types of requests/Year request received	2011	2012	2013	2014	TOTAL
FIU cooperation					
Requests received	152	111	164	164	**591**
Acceded to (in full or in part)	143	98	138	140	**519**
Rejected or insufficient info	9	13	26	24	**72**
Spontaneous disclosures	74	160	341	385	**960**
Requests made	120	144	162	244	**670**
Requests made on behalf of domestic LEAs	18	84	158	236	**496**
MAS					
Requests received & acceded	43	48	144	146	**381**
Spontaneous sharing	12	17	25	26	**80**
Joint AML/CFT inspections	2	3	10	8	**23**
Requests made	33	77	307	182	**599**
Law enforcement cooperation					
CAD Requests received (via INTERPOL or LEA-LEA)	17	22	92	197	**328**
Active	0	0	2	4	**6**
Acceded to (in full or in part)	16	21	85	182	**304**
Rejected or insufficient info	1	1	5	11	**18**
CAD Requests made	107	256	622	485	**1 470**
CAD Joint investigations	11	52	47	16	**126**
CPIB requests received (8 ML related)	20	13	26	17	**76**
Granted	17	13	24	17	**71**
Refused	3	0	2	0	**5**
CPIB requests made	5	8	8	10	**31**

Types of requests/Year request received	2011	2012	2013	2014	TOTAL
CPIB Joint investigations	2	1	1	1	**5**
CNB requests received	-	16	63	55	**134**
CNB requests made	-	74	168	147	**389**
SPF requests received (through NCB Singapore to other INTERPOL member countries)	524	650	1 193	1 378	**3 745**
SPF requests made (through NCB Singapore to other INTERPOL member countries)	1 179	1 412	1 641	1 854	**6 086**
IRAS requests received	-	153	163	327	**643**
IRAS requests made	-	12	26	96	**134**
Customs requests received	108	87	47	65	**307**
Customs requests made	10	3	6	2	**21**

International exchange of basic and beneficial ownership information of legal persons and arrangements

419. Singapore shares basic and beneficial ownership (BO) information of legal persons and arrangements, although it can only share information that is required to be available in Singapore. Basic information is publicly available with payment of a small fee from the Accounting and Regulatory Authority's (ACRA) website, which LEAs will also share with their foreign counterparts at no cost. Other forms of assistance - STRO, CAD, CPIB – have responded to requests, including the use of non-coercive investigative powers to obtain additional BO information for foreign counterparts, such as arranging voluntary interviews on behalf of foreign counterparts and voluntary disclosure of documents. MAS has also provided beneficial ownership information under the IOSCO MMoU for regulatory enforcement of securities markets laws and regulations. IRAS has responded to 85 BO related requests from treaty partners between 2012 and 2014. Finally, MLA channels have been used when coercive measures are required, such as production orders for CDD information held by reporting entities, or search and seizure orders for information held by the company.

Case Example 11. **Exchange of beneficial owner information**

Person J, a British national, incorporated Company Y overseas and Company Z in Singapore and opened bank accounts through the use of Company Service Providers (CSPs).

In 2010 and 2011, criminal proceeds of more than EUR 452 000 (approx. EUR 298 140 or USD 317 350) from two unrelated investment scams in Europe were transferred to the Singapore bank accounts of Companies Y and Z, and thereafter, routed to other Asian countries within a short period of time. Investigations also revealed that one of the victims was cheated to remit funds to a bank account in Country A, an account of a company which bears a close resemblance to the name of Company Y.

The authorities in Country A submitted a request via Interpol informing CAD that they were investigating Person J, the beneficial owner of a company with a close name resemblance to

Company Y. They requested CAD's investigation findings on Company Y.

CAD commenced ML investigations against Person J and through shareholder information from ACRA, learned that Person J was a co-shareholder and co-director with Person T, another British national, for Company Z. CAD's investigations also confirmed that Person J was the sole beneficial owner of Company Y and the co-beneficial owner of Company Z with Person T and that Companies Y and Z were shell companies created as structures to intentionally obscure the source of the criminal proceeds. Person J was charged and convicted of dishonestly receiving stolen property and was sentenced to 15 months' imprisonment.

CAD provided Country A with information on the company, including director, shareholder and beneficial ownership information. Further, CAD provided Country A with details of fund flow from one of the victims, specifically the transaction amount, transaction dates and the receiving bank in Country A. CAD also updated its counterparts on Person J's conviction.

8

420. ***Singapore has achieved a substantial level of effectiveness for IO.2***

TECHNICAL COMPLIANCE ANNEX

This annex provides detailed analysis of the level of compliance with the FATF 40 Recommendations in their numerological 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 and the Follow-Up Report.

Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the previous Mutual Evaluation in 2008 and the Follow-Up Report in 2011. This report is available from:

www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20Singapore.pdf and
www.fatf-gafi.org/media/fatf/documents/reports/mer/FoR%20Singapore.pdf.

Recommendation 1 - Assessing Risks and applying a Risk-Based Approach

This is a new Recommendation.

Criterion 1.1 – Singapore published its first National Risk Assessment (NRA) report on 10 January 2014 following a 2-year government-wide ML/TF risk assessment exercise. The report is publicly available on government websites and was conducted under the ambit of the AML/CFT Steering Committee (see R.2) with participation of over 15 government agencies. The NRA analysed ML and TF risks, and covered 14 financial sub-sectors and 8 non-financial sectors.

Criterion 1.2 – The AML/CFT Steering Committee's mandate includes responsibilities to direct the national effort to combat ML/TF; determine Singapore's AML/CFT policy; oversee the effective co-operation and co-ordination between agencies on the development and implementation of policies and measures to combat ML/TF; and identify and mitigate ML/TF risks (e.g. through the NRA exercise). For major policy changes that require political endorsement, the AML/CFT Steering Committee tables the issues at Cabinet meetings for its endorsement. The Steering Committee is supported by the Inter-Agency Committee (IAC). The IAC makes policy recommendations to the AML/CFT Steering Committee for decision or guidance. The IAC meetings provide a forum for agencies' to share information such as emerging ML/TF and proliferation financing threats and trends, FATF typologies, best practices and other developments. The meetings also facilitate policy coordination across agencies.

Criterion 1.3 – The NRA will be updated regularly and Singapore has made a public commitment to do so earlier if circumstances warrant.

Criterion 1.4 – Industry associations and key stakeholders were involved in the development of the NRA report and industry focus groups were also convened prior to the report's publication to validate the NRA findings. The NRA is available on the websites of MHA, MOF and MAS and the key messages have been reinforced through speeches, such as the keynote address delivered at the Financial Crime Seminar organised by the ABS in Singapore in July 2014. Supervisors have also provided guidance to financial institutions and DNFBP entities on the relevance of the NRA findings to their own ML/TF risk assessments, which in turn inform the implementation of risk-based

AML/CFT controls and policies. These supervisory expectations are communicated via Guidelines or Circulars issued to the private sector. These are also available on CAD's and MAS' website. Please see response to criterion 1.7 for the regulatory references.

Risk mitigation

Criterion 1.5 – The authorities provided numerous examples of a risk-based approach being applied in practice for regulated sectors (financial supervisors, some law enforcement bodies and anti-corruption bodies). The AML/CFT Steering Committee is the formal body that oversees the national AML/CFT strategy. This includes applying a risk-based approach, at a national level, and directing the IAC to deploy resources to prevent and mitigate ML/TF based on the findings of the National Risk Assessment Report. Consequently, authorities apply the risk-based approach in the supervision for their respective sectors though their AML/CFT inspection methodology and operating procedures. However, the risk-based approach is not evenly applied and is missing in other high risk areas such as in relation to transnational money laundering, illicit financial flows, and cash couriers (two higher risk areas). This unevenness in the RBA may result from a lack of a national ML/TF strategy [or detailed policy] to implement the NRA's findings.

Criterion 1.6 – Lower risk measures are applied for Stored Value Facility (SVF) cards. For SVF, Singapore applies a threshold-based approach that is based on the FATF's Guidance for a Risk-Based Approach – Prepaid Cards, Mobile Payments and Internet-Based Payment Services. 58 out of a total of 69 SVF holders are currently exempted from preventive AML/CFT measures, with the exception of suspicious transaction reporting requirements under the CDSA and the TSOFA, in addition to the relevant provisions of the PSOA and MAS Act. While all 6 internet-based SVF holders are now subject to the full range of AML/CFT requirements, the amended MAS Notice PSOA-N02 does not exclude the possibility that future internet-based SVF be exempted from AML/CFT requirements. This might not be consistent with the higher risk character of this category of SVF identified in the NRA.

Criterion 1.7 – Financial institutions and DNFBPs are legally required to take a risk-based approach in mitigating ML/TF risks. Where higher risks have been identified and conveyed by the competent authorities (e.g. through the NRA or separate assessments), financial institutions and DNFBPs are required to consider those risks in their own risk assessments, and to take enhanced measures to manage and mitigate those risks.

Criterion 1.8 – As part of the risk-based approach adopted for financial institutions and DNFBPs, they may apply simplified measures where lower ML/TF risks have been identified by the financial institution or DNFBP. Simplified CDD may be conducted when the assessment of low risks are supported by an adequate analysis of risks by the financial institution and the simplified measures are commensurate with the level of risk, based on the risk factors identified by the financial institution. Simplified CDD measures are prohibited in higher risk scenarios, including where there is a suspicion of ML/TF, and in cases where the NRA identifies a higher risk.

Criterion 1.9 – See R.26 and R.28

For FIs and DNFBPs: risk assessment

Criterion 1.10 – All sectors, with the exemption of the SGPMX and PSMDs are legally required to undertake the measures required under this criterion (the regulations contain the exact language from this criterion).

Criterion 1.11 – All sectors are legally required to undertake the measures required under this criterion (the regulations contain the exact language from this criterion).

Criterion 1.12 – See criterion 1.8.

Weighting and Conclusion

Singapore has used cross-government coordination mechanism to conduct an NRA to identify and access its ML/TF risks and implement measures to mitigate identified risks. However, the risk-based approach is not evenly applied and is missing in some high risk areas such as in relation to transnational money laundering, illicit financial flows, international cooperation, and cash couriers.

Recommendation 1 is rated largely compliant.

Recommendation 2 - National Cooperation and Coordination

Singapore was rated compliant on national coordination (former Recommendation 31) in the previous report.

Criterion 2.1 – Singapore has a national AML/CFT policy statement, issued by the AML/CFT Steering group in May 2015 on the basis of the NRA. It consists of eight principles.

Criterion 2.2 – The AML/CFT Steering Committee is the national AML/CFT coordination authority. All relevant stakeholders participate. The Steering Committee was formed in 1999 and has its own terms of reference. At the operational level it is supported by the Inter-Agency Committee.

Criterion 2.3 – Besides the Inter-Agency Committee, several other coordination bodies and structures exist, including among law enforcement bodies, between STRO and MAS and other financial/DNFBP supervisors, for general counter-terrorism issues (including TF issues), for TF designations and for export control issues (IMC-EC, including PF issues). Where necessary, ad-hoc working groups are formed.

Criterion 2.4 – PF coordination issues fall within the competence of the Inter-Agency Committee and the aforementioned IMC-EC.

Weighting and Conclusion

Recommendation 2 is rated compliant.

Recommendation 3 - Money laundering offence

In its 3rd round MER, Singapore was rated partially compliant for Recommendation 1 and largely compliant for Recommendation 2 (ML offence). The main shortcomings were a lack of effectiveness, and technical inconsistencies with the Vienna and Palermo Conventions in relation to *mens rea* requirements.

Criterion 3.1 – ML is criminalised under sections 46 (dealing with benefits of drug offences) and 47 (dealing with benefits of criminal conduct) of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA). The revision of the CDSA in 2010 has brought Singapore in line with the requirements set by Vienna Article 3(1)(b) and (c) and Palermo Article 6(1). Sections 46 and 47of the CDSA adequately cover concealment or disguise, acquisition or possession of property (including correcting the deficiency of the additional purposive *mens rea* requirement), as well as conversion, transfer of property, its removal, with the adequate *mens rea* requirements (this corrects the deficiency of the missing alternative purpose element identified in the 2008 MER). In addition to knowledge, the ML offences extend to situations where a person has 'reasonable grounds to believe' that property constitutes the benefits of drug dealing or other criminal conduct.

ML type offences are also found in section 43 and 44 of the CDSA (assisting another to retain benefits of drug dealing / criminal conduct), section 6 of the Terrorism (Suppression of Financing) Act (TSOFA) (dealing with property of terrorists) and section 14(3A)(b) of the Moneylenders Act (assisting a person carry out unlicensed moneylending). This analysis focuses primarily on the main ML offences in sections 46 and 47 of the CDSA.

Criterion 3.2 / Criterion 3.3 – The CDSA applies a list approach to predicate offences, with drug dealing offences listed in the First Schedule and other serious offences listed in the Second Schedule. The list is comprised of more than 400 serious offences, which have a minimum penalty of four years imprisonment as required by the Palermo Convention, and cover all 21 categories designated by the FATF. There also predicate offences with a minimum sentence of less than four years so as to address ML derived from less serious offences (e.g. theft). The list is subject to regular review for potential broadening of its scope. Since its 2008 MER, Singapore has also criminalised human trafficking more comprehensively, by adopting the Prevention of Human Trafficking Act, which entered into force on 1 March 2015.

Criterion 3.4 – All ML offences extend to "property", which is defined under section 2(1) of the CDSA to include money and all other property, movable or immovable, including things in action and other intangible or incorporeal property. Sections 46 and 47 confirm that the offences extended to any property wherever situated that, in whole or in part, directly or indirectly, represents the benefits of drug trafficking or criminal conduct. There is no value threshold stipulated in the CDSA for property.

Criterion 3.5 – Section 47A(1) of the CDSA explicitly provides that the prosecution does not need to secure a conviction, or to establish that the particulars of an offence have been committed, in order for those assets to be considered proceeds of crime. The prosecution only needs to prove that a person knows or has reasonable grounds to believe that the whole or part of the property

constitutes, or directly or indirectly represents, the benefits of drug dealing or criminal conduct, without carrying the burden to prove the connection to a particular offence.

Criterion 3.6 – The criminalization of ML under the CDSA extends to the criminal conduct committed in another country. The criminal conduct ML offence (section 47) covers every act constituting a "serious offence" prescribed under the Second Schedule to the CDSA (such as bribery, corruption and tax evasion). Criminal conduct includes a "*foreign serious offence"*, which is defined under section 2(1) as "*offences against the laws of a foreign country where the act or omission constituting the offence or the equivalent act or omission would have constituted a serious offence had it occurred in Singapore*" and explicitly includes foreign serious tax offences. A special provision has been included in section 2(1) of the CDSA to recognise foreign tax evasion offence, so long as the offence has been criminalised in the foreign jurisdiction and is committed wilfully with intent to evade tax.[48] This same principle applies to the drug dealing ML offence (section 46).

Criterion 3.7 – The CDSA applies to persons that commit the predicate offence (sections 46[1] and 47[1] for drug dealing and criminal conduct respectively). Case law has confirmed this position (see *Public Prosecutor v Koh Seah Wee and another* [2012] 1 SLR 292).

Criterion 3.8 – Jurisprudence establishes that the intent and knowledge required to prove the ML offences can be inferred from objective factual circumstances (e.g. *Loh Kim Cheng v Public Prosecutor* [1998] 1 SLR(R) 512 and *Ang Jeanette v Public Prosecutor* [2011] 4 SLR 1).

Criterion 3.9 – Sections 46(6) and 47(6) of the CDSA provide that natural persons are liable to a maximum imprisonment of 10 years, and/or a fine not exceeding SGD 500 000 (approx. EUR 329 800 / USD 351 050) upon conviction. This is similar to other serious economic offences (e.g. forgery and falsification of accounts). However it is significantly less than the 20-30 years of imprisonment for drug trafficking offences. Nevertheless, these sanctions are sufficiently proportionate and dissuasive. Case law establishes that more severe penalties are applied on the basis of the level of fault (See: *Public Prosecutor v Ngiam Kok Min* [DAC 18666/2012 and others], where the defendant "knowingly" laundered funds).

Criterion 3.10 – Sections 46(6) and 47(6) provide that sanctions apply to legal persons in the same way as it does to natural persons (with a fine not exceeding SGD 1 million / approx. EUR 659 600 / USD 702 100)). A legal person convicted for ML may still be liable for civil damages from a person injured by their conduct (section 39 of the Interpretation Act) and administrative proceedings can be taken against them (e.g. section 253 and 254 of the Companies Act allows the relevant Minister to apply to court to wind up a company on the ground that it is being used for an unlawful purpose). This latter application can be made regardless of whether a company has been convicted of a ML offence. In pursuing legal persons for ML, criminal liability of the natural persons involved is not excluded (section 59 of the CDSA). The range of available sanctions allow for the imposition of proportionate sanctions. However, the criminal sanction (SGD 1 Million) is too low to be sufficiently dissuasive for legal persons. While a legal

[48] This is not withstanding that the foreign tax offence has no local equivalent in Singapore.

person convicted of multiple charges could receive a fine higher than SGD 1 million, Singapore advised that they did not consider such a fine would be sufficiently dissuasive for a legal person.

Criterion 3.11 – Common purpose (referred to as 'common intention') (section 34), abetting (sections 107 to 116), criminal conspiracy (sections 120A and B) and attempt (section 511) are clearly set out in the Penal Code. These general provisions apply to all criminal offences, including the ML offences in the CDSA. Section 107 makes it clear that the 'abetment' offences also include conspiracy (engage with one or one more person or persons), intentional aiding of an offence (by any act or illegal omission), or instigating an offence. Explanations in section 107 also make it clear that the concept of "aiding" includes facilitating. Case law (*Public Prosecutor v. Ng Ai Tiong* [2000] 1 SLR(R) 1) confirms that the "instigation" provision under the abetment provision also includes "counselling".

Weighting and Conclusion

While Singapore's ML offences generally meet the requirements of Recommendation 3, the criminal sanction available for legal persons convicted of the ML offence is too low to be sufficiently dissuasive.

Recommendation 3 is rated largely compliant.

Recommendation 4 - Confiscation and provisional measures

In its 3rd round MER, Singapore was rated largely compliant for former Recommendation 3. At the time, there were concerns in relation to effectiveness and the scope of the measures (with regards to instrumentalities and intended instrumentalities of crime). Singapore's seizure and confiscation regime is set out in sections 4 and 5 of the CDSA which have mirroring measures for the confiscation of benefits derived from drug dealing offences and criminal conduct (including ML, TF, and predicate offences). In some exceptional cases, non-conviction based confiscation is possible: where the person has absconded (section 27) and where the person has died before being convicted (section 28). Most seizures and confiscation occur under the CPC however.

Criterion 4.1 – Sections 4 and 5 of the CDSA, read in conjunction with sections 7 and 8, allow for the confiscation of all proceeds, laundered property, and property in the context of a terrorist organization (including TF) and property of corresponding value, regardless of whether the property is held by criminal or third parties. Sections 4 and 5 enable the court to make a confiscation order against a defendant in respects of benefits derived from drug dealing and criminal conduct and sections 7 and 8 outline the procedure for determining the 'benefits derived'. Confiscation of instrumentalities and intended instrumentalities of crime (ML or predicate offence) is covered under section 364(2)(a) of the CPC (which also could be used to confiscate laundered property). Confiscation of property of corresponding value to instrumentalities is specifically covered under section 29B of the CDSA. Additional confiscation powers are available under the provisions of the CPC (sections 319 and 370), TSOFA (sections 21 and 24), PCA (section 13) and the MDA (sections 27 and 28) for their respective indictable offences.

Criterion 4.2 – Singapore has implemented the following measures to enable confiscation and provisional measures:

- *Sub-criterion 4.2 a) (on identify, trace, evaluate property).*. Singapore law enforcement agencies [such as the CPIB, CNB and SPF (including CAD and STRO)] have powers to identify and trace property that may become subject to confiscation (sections 20, 32, 33 and 34 of the CPC and section 34 of the CDSA). An authorised officer under the CDSA can apply to a court for a production order (section 30); however production orders against financial institutions specifically must be made by the Public Prosecutor or their authorised representative to the High Court (section 31). Sections 7 and 8 also set out a number of measures to evaluate the value of property subject to confiscation (referred to as 'assessment of the value of benefits'). These powers are also listed in the CPC (sections 14-40 and 235), the TSOFA (sections 8-10A), the MDA (sections 24 and 26) and the PCA (section 22)

- *Sub-criterion 4.2 b) (on provisional measures)*. The legal framework contains a number of provisions related to provisional measures. Sections 15-16 of the CDSA and section 11 of the TSOFA allow for the making of restraint orders, which are made on an ex parte application to a judge (sections 16(4)(b) of the CDSA and 11(1) of the TSOFA). Seizure of property is also provided for under the CPC (section 35), CDSA (section 34(5)), PCA (sections 15 and 22) and MDA (sections 24 and 26).

- *Sub-criterion 4.2 c).* Law enforcement authorities are able to take measures to prevent or void actions that would prejudice Singapore's ability to freeze or seize or recover property that is subject to confiscation. Under section 35 CPC, authorities can seize suspected proceeds of crime from any person, including property that is no longer in possession of the offender (section 35(9)(b)). Section 16 CDSA allows the High Court to make restraint orders to prohibit persons from dealing with property. Section 16(8) specifically allows authorities to seize property the subject of a restrain order to prevent its dissipation from Singapore. To ensure Singapore is able recover property that is subject to confiscation, sections 12(7) and (8) of the CDSA void gifts of property which is or is part of the benefits derived by the defendant from drug dealing or criminal conduct. Under the TSOFA, a court may void transfers made to a third party after restraint was ordered unless the transfer was to a bona fide purchaser for value (section 29). TSOFA also allows for interim preservation rights (section 28).

- *Sub-criterion 4.2 d)*: The legal framework provides for a broad range of investigative measures in support of the existing confiscation powers listed in the CDSA, CPC, PCA, TSOFA and MDA (see criterion 4.2a). Refer to the analysis under Recommendation 31 for further information.

Criterion 4.3 – The rights of bona fide third parties are protected under the CDSA (section 13), and similarly under the TSOFA (sections 19 and 27-29) which contains a number of safeguard provisions that protect the rights of innocent third parties acting in good faith. Section 35(7) of the CPC allows a court to order the release of property seized under section 35 on the application of any person who is prevented from dealing with property, with seizures required to be reported to a Magistrate's Court (section 370 of the CPC). The Court of Appeal has held that any person who can show a *prima*

facie interest in seized property may claim a right to be heard when a seizure is reported pursuant to section 370 (see *Mustafa Ahunbay v PP* [2015] SGCA 10). Although the PCA and MDA do not have similar safeguard provisions, Singapore considers that there is a similar common law right to judicial review as outlined in *Ung Yoke Hooi v Attorney-General* [2009] SGCA 15.

Criterion 4.4 – The management of seized assets is handled by relevant investigative agencies (e.g. SPF has dedicated SOPs on the management and disposal process of seized assets). The Police General Order also sets out procedures for the management and control of property. The CDSA foresees the appointment of a 'receiver' to take possession of and manage any realisable property (section 16(6)). Court-ordered disposal of property procedures are also set out in the CPC (sections 364(2) and 370(2)) and the TSOFA (section 25).

Weighting and Conclusion

Recommendation 4 is rated compliant.

Recommendation 5 - Terrorist financing offence

In its 3rd round MER, Singapore was rated largely compliant for former Special Recommendation II. Aside from effectiveness issues, Singapore had insufficiently criminalised TF in line with the TF Convention, as not all offences in the Annex were terrorist acts and there was an additional purposive requirement. Singapore's criminalises TF in the Terrorism (Suppression of Financing) Act (TSOFA).

Criterion 5.1 – Singapore's TF offences are contained in sections 3 to 5 of TSOFA. Section 3 criminalises the provision or collection of property for terrorist acts, section 4 criminalises the provision of property and services for terrorist purposes and section 5 criminalises the use of possession of property for terrorist purposes. The definition of "terrorist act" as given by section 2(2) of the TSOFA largely meets the elements of article 2(1)(b) of the TF Convention. It covers the use or threat of action which is intended or reasonably regarded as intending to: (1) influence or compel a government or international organisation from doing (or refraining from doing) any act; or (2) intimidate the public or section of public. The Second Schedule to the TSOFA also includes a range of offences which also constitute terrorist acts for the purposes of section 2(2). This includes the offences listed in the UN Conventions and Protocols shown in the Annex to the TF Convention. With the finalisation of the accession to the 1988 Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf., Singapore has ratified or acceded to all the Conventions and Protocols in the Annex to the TF Convention.

Criterion 5.2 – Singapore's main TF offences are in sections 3 to 5 of TSOFA. Section 3 criminalises the provision or collection of property for terrorist acts, section 4 criminalises the provision of property and services for terrorist purposes and section 5 criminalises the use of possession of property for terrorist purposes. The required mental element for all offences is intent, knowledge or reasonable belief. Section 3 prohibits a person from directly or indirectly, wilfully and without lawful excuse, providing or collecting property intending or knowing, or having reasonable grounds to believe, that such property will be used, in whole or in part, in order to commit any terrorist act.

Under section 4, it is an offence to make property, financial and other related services available for terrorist purposes or to the benefit of a person who facilitates or carries out a terrorist act. This also applies in cases where property and services would be made available, knowing (or having reasonable grounds to believe) that they will be used by or will benefit any individual terrorist or terrorist entity. Section 5 prohibits the use or possession of property for the facilitation or commission of any terrorist act, thus going beyond the requirements of Article 2(1) of the TF Convention. No link to specific terrorist act or acts is required (see criterion 5.4 below).

Criterion 5.3 – The interpretation given to 'property' under section 2(1)(a) is identical to the definition of "funds" in Article 1 of the TF Convention. It covers both assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form. As such, the TF offences will apply to both legitimate and illegitimate assets.

Criterion 5.4 – Given the broad definition of "terrorist act" in section 2(2) includes the threat to carry out a terrorist act, it can be deduced that TF offences do not require that the funds were actually used to carry out or attempt a terrorist act. Sections 3 to 5 make reference to '*any terrorist act*' and *'any terrorist or any terrorist entity'*, thus dismissing the need for a link to a specific terrorist act or the designation of an organisation as terrorist, criminalising the financing of an individual terrorist 'for any purpose'.

Criterion 5.5 – Pursuant to sections 3 to 5, it is sufficient to prove that the person '*had reasonable grounds to believe*', thus allowing for inferring of knowledge and intent from objective factual circumstances of the case. As explained in criterion 3.8, case law allows for this as well.

Criterion 5.6 – The maximum penalty for natural persons (for offences committed under sections 3 to 6 of the TSOFA) is a fine of SGD 500 000 (approx. EUR 329 800 / USD 351 050), imprisonment of up to 10 years, or both. Singapore has increased these penalties since the 2008 MER to harmonize with penalties set out in the CDSA, and they seem to be proportionate and dissuasive. However, section 116 of the Penal Code limits the penalty for the offences ancillary of the attempted TF offence to one quarter of the maximum penalty of the TSOFA offences (2.5 years imprisonment). These are not sufficiently proportionate and dissuasive.

Criterion 5.7 – Criminal liability for TF offences applies to "any person", including legal persons. In addition, section 2(1) of the Interpretation Act defines "person" as '*any company or association or body of persons, corporate or unincorporated*'. Section 35 of the TSOFA also specifically deals with offences committed by '*a company, firm, society or other body of persons*'. Although the primary form of liability is criminal, there is nothing precluding legal persons from facing parallel criminal, civil and administrative proceedings (section 40 of the Interpretation Act) (see criterion 3.10). The maximum criminal fine available for legal persons is SGD 1 million (approx. EUR 659 600 / USD 702 100). The range of available sanctions would allow the imposition of proportionate sanctions. The criminal sanction however is too low to be sufficiently dissuasive for legal persons (for similar reasons outlined in Recommendation 3).

Criterion 5.8 – Section 2(1) of the TSOFA defines '*terrorism financing offence*' to include the conspiracy to commit, inciting, attempting , aiding, abetting, counselling or procuring the commission of the section 3 to 5 offences. This does not cover inciting, attempting, aiding, abetting, counselling or procuring the commission of an *attempted* TF offence. The ancillary offences to attempted TF offences are instead covered by the generic abetment offence in section 116 of the Penal Code. The definition of abetment section 107 covers the ancillary offences listed in the criterion.

Criterion 5.9 – The TF offences are designated offences for ML as they are listed in the Second Schedule to the CDSA.

Criterion 5.10 – TF offences apply regardless of the geographic location (section 2(4) of the TSOFA).

Weighting and Conclusion

Singapore has criminalised TF consistent with the TF Convention, as well as criminalising the financing of an individual terrorist for any purpose. However, the criminal sanctions available for legal persons convicted of the TF offence and persons convicted of TF ancillary offences are too low to be sufficiently dissuasive.

Recommendation 5 is rated largely compliant.

Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing

In its 3rd round MER, Singapore was rated largely compliant for Special Recommendation III. The main shortcoming related to the lack of an explicit legal framework for freezing under UNSCR 1373.

Criterion 6.1.

- *Sub-criterion 6.1(a).* Singapore has designated the Inter-Ministry Committee on Terrorist Designations (IMC-TD) as the competent authority for proposing designations pursuant to UNSCR 1267. The IMC-TD is led by MHA, with participation of SPF (CAD), MFA, AGC and MAS.
- *Sub-criterion 6.1(b)*. IMC-TD considers designations. The initial proposal is to be made by the ISD, and it is considered and designated by the members of the IMC-TD. The ISD has a specialised and dedicated team of investigators that collects and analyses intelligence in relation to all terrorism-related activities, including TF activities. Where there is a need to designate a person/entity based on the criteria in the UNSCRs, ISD will propose this to the IMC-TD. [
- *Sub-criterion 6.1(c)*. The standard for designation is based on reasonable grounds. The IMC-TD designates a terrorist based on a definition provided in Article 2 of the TSOFA.
- *Sub-criteria 6.1(d) and 6.1(e)*. Designations are proposed to the UN through MFA with information on the proposed name and a statement of case, and the standard UN designation

form. Authorities also indicated that the state(s) of residence and/or nationality of the individual/entity concerned will be contacted to seek additional information if required.

Criterion 6.2.

- *Sub-criterion 6.2(a)*. In the case of the designation in pursuant to UNSCR 1373, the ISD (Internal Security Department) is to make a proposal for designation, and the proposal is to be considered by the IMC-TD. Once the designation is made, the information is provided to reporting entities via MAS and supervisory authorities of DNFBPs. As of the time that this MER is adopted, [14] individuals have been designated in the First Schedule of the TSOFA.
- Sub-criterion 6.2(b). See 6.1.b.
- *Sub-criterion 6.2(c).* Authorities indicate that foreign requests for designations through MFA are considered promptly by the IMC-TD. The legal basis for designation is found in section 2 of the TSOFA and designation will depend on whether, based on reasonable grounds, the request meets the criteria in UNSCR 1373.
- *Sub-criterion 6.2(d).* Criminal proceedings are not required for designations, and designations are based on the criteria listed in the Interpretative Note to R6. The standard is the same as for domestic initiatives.
- *Sub-criterion 6.2(e).* Requests to other countries are supported by the name of the person/entity, the nature of the terrorist activities, the nature of the security risk and the affiliation to any known terrorist groups. The legal basis for designation requests to other countries is found in section 2 of the TSOFA and the requests will be based on the same criteria.

Criterion 6.3.

- *Sub-criterion 6.3(a)*. Law enforcement officers have powers under ISA, CPC and TSOFA to obtain information to determine if the person/entity meets the criteria for designation (see details in c.31.1).
- *Sub-criterion 6.3(b)*. There is no requirement to inform a potential designee of an upcoming designation.

Criterion 6.4 – Dealings with persons/entities listed in the First Schedule to the TSOFA are prohibited, and all of their assets are frozen in accordance with the TSOFA. All UN designations are automatically included in the first schedule; however, to take into account the time difference between Singapore and New York, the law only takes effect in Singapore on the following day of addition to the UN list. For domestic 1373 freezing, the freezing obligation takes effect after gazetting, but also not sooner than one day after enacting.

Criterion 6.5.

- *Sub-criterion 6.5(a).* The freezing obligation for designated persons/entities is contained in Section 6 of the TSOFA (prohibition to deal with property of terrorists).
- *Sub-criterion 6.5(b).* The obligation to freeze extends to all relevant persons and assets (TSOFA sections 3 - 6 and 21a).
- *Sub-criterion 6.5(c)*. TSOFA Sections 4 and 5 prohibit from directly or indirectly using, possessing and providing property and services for terrorist purposes, and section 6 prohibits dealing in property.
- *Sub-criterion 6.5(d)*. MAS and DNFBP agencies communicate designations to financial institutions and DNFBPs. This is done through the MAS webpage which contains guidance and links to the consolidated websites, including MHA's IMC-TD webpage/. Reporting entities can sign up for alerts for changes (listing and delisting). An email alert will be sent to the website subscribers. However, not all entities may have signed up (especially those in the PSMD sector) for this.
- *Sub-criterion 6.5(e).* The TSOFA (Section 8.1) contains an indirect reporting obligation that requires anyone in Singapore to report (suspected) terrorist property to the police. However, this catch-all obligation does not cover the direct requirement of R6.
- *Sub-criterion 6.5(f).* Sections 11, 19 and 24 allow for protection in the case of seizure or forfeiture, but not for freezing (the only element that is covered by Recommendation 6).

Criterion 6.6.

- *Sub-criteria 6.6(a), (b),(d) and (e).* Delisting procedures, including links and references to the UN Focal Point and Ombudsperson, are available on the website of IMC-TD. The website also contains the information for domestic delisting.
- *Sub-criterion 6.6(c).* In addition to administrative appeals, the person/entity designated may seek a judicial review in the High Court [Order 53 of the Rules of the Supreme Court].
- *Sub-criterion 6.6(f).* The website of IMC-TD contains information for persons inadvertently affected by freezing to contact IMC-TD.
- *Sub-criterion 6.6(g)*. While the TSOFA is applied to any person in Singapore and any Singaporean citizens, given that dealers in precious stones and metals (PSMDs) are not subject to adequate supervision (see Recommendation 28), it is assumed that appropriate mechanisms for communicating TF designations are not in place.

Criterion 6.7 – According to TCQ (p.10 of Rec 6), a judge may order that the frozen property is returned to the applicant (or a judge may revoke an order of restraint). The Minister has promulgated a General Exemption Order in 2013 which exempts "basic expenses" from being frozen

as long as a Notice is obtained from the Director of ISD (please see General Exemption Order 2013 attached).

Weighting and Conclusion

Singapore has an overall asset-freezing mechanism to implement obligations under UNSCRs 1267, 1373 and their successor resolutions. However, the law obliges any person to report terrorist property to the Commissioner of Police, and the competent authorities are to receive the information indirectly. In addition, not all PSMDs are subject to supervision by the competent authorities.

Recommendation 6 is rated largely compliant.

Recommendation 7 – Targeted financial sanctions related to proliferation

This is a new Recommendation.

Criterion 7.1 – Singapore implements provisions in relation to targeted financial sanctions pursuant to UNSCRs against Iran and DPRK in accordance with three MAS regulations (for financial institutions)[49] and two UN regulations (for the general public, including DNFBPs and money lenders).[50] Implementation is automatic, however, to take into account the time difference between Singapore and New York, the law only takes effect in Singapore on the following day of addition to the UN list.

Criterion 7.2.

- *Sub-criteria 7.2(a), (b) and (c).* Freezing obligations and prohibitions are covered by MAS and UN Iran and DPRK regulations (see section 5 for MAS, and section 8 and 9 for the UN regulations) and cover all types of funds and other assets, regardless of the type of ownership or possession (see section 5 for MAS, section 8 and 9 for the UN Iran regulation, and section 9 and 10 for the UN DPRK regulation).
- *Sub-criterion 7.2(d).* The UN Iran Regulations and the UN DPRK Regulations apply to any person in Singapore and any Singaporean citizen including financial institutions and DNFBPs. For details regarding communication to these sectors, see c.6.5 (d).
- *Sub-criterion 7.2(e).* The MAS and UN regulations all contain direct obligations for those who hold funds or knowledge about relevant transactions to inform MAS (MAS Regulations section 7 for Iran, section 6 for DPRK) or the police (UN Regulations section 17 for Iran and section 14 for DPRK). However, for dealers in precious metals and stones (PSMD), s*ee criterion 6.5 (d)*

[49] MAS Iran Regulations (2007), MAS DPRK Freezing Regulations (2009) and MAS DPRK Sanctions Regulations (2009).
[50] UN Iran Regulations (2014) and UN DPRK Regulations (2010).

- *Sub-criterion 7.2(f).* Bona fide third parties are protected by law for complying with any MAS regulation (section 27.A.3 MAS act) or UN regulation (section 3 UN Act).

Criterion 7.3 – For financial institutions, MAS supervises compliance with the Iran and DPRK regulations (section 27A.5 MAS Act). Breach of the regulations is considered an offence, punishable by a fine not exceeding SGD 1 million (approx. EUR 659 600 / USD 702 100). For DNFBPs, the UN Act sets out that any person who contravenes the regulations shall be liable on conviction, in the case of an individual, to a fine not exceeding SGD 500 000 (approx. EUR 329 800 / USD 351 050) or to imprisonment for a term not exceeding 10 years or to both; or in any other case, to a fine not exceeding SGD 1 million.

Criterion 7.4.

- *Sub-criterion 7.4(a).* The MAS website contains all the necessary information for delisting, including links to the UN (Focal Point).

- *Sub-criterion 7.4(b).* The MAS website contains the necessary information for those who have been inadvertently affected by an otherwise correct designation (i.e., for persons with the identical personal details as the designated person).

- *Sub-criterion 7.4(c).* For MAS regulations, the MAS Act (section 41C) allows MAS to grant exemptions to its regulations issued under the MAS Act such as the Iran and DPRK regulations, and they also contain the exemption conditions set out in UNSCRs 1718 and 1737. For non-MAS-regulated entities, the UN Regulations contain the correct conditional exemptions (section 21 for Iran and 18 for DPRK).

- *Sub-criterion 7.4(d).* The issue of communication relies on sign-up to MAS' webpage (or other alternative means, e.g. subscription to commercial database) is applicable to the mechanism for communicating de-listings to the financial institutions and the DNFBPs. Unfreezings will be resolved with the relevant parties, including the financial institutions and DNFBPs that mistakenly froze the funds and assets of the false positive.

Criterion 7.5 – Neither the MAS regulations nor the UN regulations have a provision that (i) permits access to the frozen accounts in relation to obligations that arose prior to the date on which accounts were frozen or (ii) permits a designated person to make any payment due under a contract entered into prior to the listing. These exemptions are left to the discretion of the MAS or the MinLaw in accordance with provisions under the MAS Act and UN Iran/DPRK Regulations respectively.

Weighting and Conclusion

Singapore has an overall mechanism to implement targeted financial sanctions in relation to proliferation pursuant to relevant UNSCRs. There is no provision in accordance with the exemptions under the UNSCRs and the implementation is left to discretion of the authorities.

Recommendation 7 is rated largely compliant.

Recommendation 8 – Non-profit organisations

In its 3rd round MER, Singapore was rated LC on former Special Recommendation VIII. Two comprehensive reviews had been undertaken at that time in relation to the NPO sector, although Singapore had not assessed the NPO sector to determine TF vulnerabilities. It was noted that the Commissioner of Charities (COC) had conducted a number of outreach initiatives and that NPOs were subject to effective oversight. Singapore was found to have developed and implemented mechanisms that allow authorities to obtain and share information on NPOs.

The NPO sector in Singapore comprises predominantly charities, as well as societies, Companies Limited by Guarantee (CLG) and mosques. The authorities in charge of the NPO sector are the Office of the COC for charities, the Registry of Societies (ROS) for societies, the Accounting and Corporate Regulatory Authority (ACRA) for CLGs, and the Majlis Ugama Islam Singapura (MUIS) for mosques.

Criterion 8.1 – Singapore has a strong capacity to obtain information on its sector which has allowed it to reasonably access which organisations based on their activities and characteristics are at risk of terrorist financing abuse. Singapore has reviewed the adequacy of the laws and regulations that relate to such organisations and has demonstrated that it does revisit such assessments when faced with the possibility of new threats.

Criterion 8.2 – The Office of the COC, ROS, and MUIS have all issued publications raising awareness about ML/TF risks for the respective organizations they regulate. While there have been targeted sessions using 'red flag' indicators for TF, the majority of guidance simply informs NPOs of their general obligations to comply with targeted financial sanctions and STR reporting obligations. .

Criterion 8.3 – As part of the general supervision of NPOs in Singapore, charities have to comply with transparency, integrity and public confidence related rules. None of these has been put in place for terrorist financing purposes, but the regulations are sufficiently comprehensive.

Criterion 8.4 – Singapore has standards in place that require NPOs to:

a. maintain information on: (i) the purpose and objectives of their stated activities; and (ii) the identity of person(s) who own, control or direct their activities, including senior officers, board members and trustees.
b. issue annual financial statements that provide detailed breakdowns of income and expenditure;
c. have controls in place to ensure that all funds are fully accounted for, and are spent in a manner that is consistent with the purpose and objectives of the NPO's stated activities;
d. be licensed or registered;
e. follow a "know your beneficiaries and associated NPOs" rule; and
f. maintain, for a period of at least five years, records of domestic and international transactions, and the information in (a) and (b) above, and make these available to competent authorities upon appropriate authority.

Criterion 8.5 – Although monitoring and sanctions provisions are in place for all NPOs, none of the monitoring relates specifically to terrorist financing. While Singapore has a good understanding of the types of NPOs defined in R.8, it hasn't matured its ability to assess which organizations are at particularly at risk for being abused for terrorist financing purposes.

Criteria 8.6.a), 8.6.b) and 8.6.c) – COC and other NPO supervisors work with STRO and SPF/CAD to share information. For example, STRO screens individuals and entities for risk for COC. Cooperation and sharing of such information also takes place through the Inter-Agency Committee. COC has the right to obtain any information from NPOs, and from any other person that may have relevant information. ACRA has similar powers, as does MUIS, for NPOs.

Criterion 8.7 – There are a variety of government institutions involved in the supervision of NPOs. While there is no clear articulation of a central contact point with respect to NPOs, Singapore has identified appropriate points of contact and procedures to enable cooperation and coordination mechanisms in place to respond to international requests relating to NPOs.

Weighting and Conclusion

Singapore's has taken steps to understand the makeup of their NPOs to identify the organizations that meet the FATF definition of NPO and face inherent risk for terrorist financing. While for the most part not specific to terrorist financing, Singapore has conducted outreach on broader issues of AML/CFT to their sector and has a good mechanism in place to reach those organizations at risk and conduct outreach. Singapore has the mechanisms and legal framework in place to receive information on those organizations at risk and therefore conduct monitoring and supervision. Singapore's ability to conduct TF investigations on organizations at risk could be enhanced by further knowledge on TF matters particularly within those institutions responsible for the supervision of NPOs. While there are a variety of government institutions involved in the supervision of NPOs and no clear articulation of a central contact point with respect to NPOs, Singapore has cooperation and coordination mechanisms in place to respond to international requests relating to NPOs.

Recommendation 8 is rated largely compliant.

Recommendation 9 – Financial institution secrecy laws

Singapore was rated compliant with Recommendation 4 in its 3rd round MER. Since the adoption of the 3rd round MER, the MAS amendment Act 2015 was adopted.

Criterion 9.1 – There are statutory confidentiality requirements for banks and merchant banks (s.47 of the Banking Act (BA)). However, the Third Schedule of the BA allows for confidential customer information to be accessed and obtained by competent authorities, including for combating ML, TF and associated predicate offences (BA: Third Schedule, Part 1 – Para. 1 and Part 2 – Para. 2 and 3). There are no statutory confidentiality requirements in any other financial sectors, as defined by the FATF. Competent authorities are able to share information, including protected information, domestically and with their foreign counterparts, pursuant to Part VC of the MAS Act. No legal

obstacle that would inhibit the implementation of the FATF Recommendations, including R.13, 16 and 17, was identified in the regime for correspondent banking, wire transfers and reliance on third parties.

Weighting and Conclusion

Recommendation 9 is rated compliant.

Recommendation 10 – Customer due diligence

In the Third Round, Singapore was rated largely compliant with the CDD requirements in Recommendation 5, and the MER identified four deficiencies (para. 349–406). Recommendation 10 was subject to significant revisions in 2012. The MAS Amendment Act 2015 was adopted, and the MAS Notices and Directives as well as the moneylenders PMFTR were recently amended to address some of the new requirements of R.10. CDD requirements do not apply to SVF holders (including internet-based SVFs) if they meet the requirements set out in MAS Notice PSOA-N02[51] (see Preamble above).

Criterion 10.1 – The use of anonymous accounts, numbered accounts, or accounts in fictitious names is prohibited. The moneylenders PMFTR 2009 does not explicitly prohibit anonymous and fictitious accounts, but it contains face-to-face CDD provisions which, in practice, prevent the use of such accounts by moneylenders.

Criterion 10.2 – CDD is required in the circumstances covered by c.10.2 (a), (c)-(e) – see also analysis regarding R.16 below. Banks, merchant banks, finance companies, and capital markets intermediaries are required to perform CDD for occasional transactions above SGD 20 000 (approx. EUR 13 192 / USD 14 042). The thresholds for moneylenders and money-changers are lower (disbursement of loans above SGD 3 000 (approx. EUR 1 979 / USD 2 106) and aggregate value not less than SGD 5 000 (approx. EUR 3 298/ USD 3 511), respectively), and for SVF holders for transactions exceeding SGD 5 000. Remittance agents perform CDD for all remittance transactions.

Criterion 10.3 – Identification and verification are required for a "customer" using reliable, independent source data, documents or information. The MAS Notices and Directives generally define "customer" to mean a person (whether a natural person, legal person, or a legal arrangement) with whom the FI establishes or intends to establish business relations (this constitutes permanent customers) or for whom the FI undertakes or intends to undertake any transaction without any account being opened (this constitutes occasional customers). The Schedule of CDD measures of the moneylenders PMTFR 2009 contains similar requirements for moneylenders. To ensure relevance to the various financial sub-sectors, the "customer" definitions are specifically customised in the respective MAS Notices and Directives, and in the PMFTR for moneylenders, but they do not deviate from the principles above.

[51]The relevant criteria are: (i) a load limit of under SGD 1 000;(approx. EUR 660 / USD 702), (ii) no cash withdrawal option; (iii) no cross-border transfers allowed; (iv) used only as a means of making payment for goods or services; and (v) funding from an identifiable source.

Criterion 10.4 – Reporting FIs are required to identify the natural person(s) appointed by a customer to act on his behalf in establishing business relations and when carrying out occasional transactions, on the basis of obtaining appropriate documentary evidence authorising the appointment of such natural person and the specimen signature of the natural person.

Criterion 10.5 – For all customers, there is a requirement to identify and verify beneficial owners. For customers that are legal persons, FIs are required to identify the natural persons (whether acting alone or together) who ultimately own the legal persons. When read together with the relevant Guidance documents, this provision appears to meet the definition of ultimately having a controlling interest in the legal person, set out in footnote 33 to c.10.10. The MAS Notices and Directives, and the PMFTR for moneylenders explicitly provide for exemptions in relation to this requirement. These exemptions, which relate to particular types of financial institutions and activities, are consistent with the example in footnote 31 to c.10.10.[52]

Criterion 10.6 – When processing the application to establish business relations, FIs are required to understand and as appropriate, obtain from the customer information as to the purpose and intended nature of business relations.

Criterion 10.7 – There are general requirements for ongoing monitoring, including scrutiny of transactions to ensure they are consistent with the FI's knowledge of the customer, its business and risk profile (and where appropriate the source of funds), and to ensure that documents, data, and information are kept up-to-date.

Criterion 10.8 – Financial institutions are required to understand the nature of the customer's business and its ownership and control structure.

Criterion 10.9 – Where the customer is a legal person or legal arrangement, FIs are required, as well as identifying the customer, to also identify the legal form, constitution and powers that regulate and bind the legal person or arrangement. In addition, FIs are required to identify the connected parties of the customer, by obtaining at least the following information of each connected party: (1) full name, including any aliases; and (2) unique identification number (such as an identity card number, birth certificate number or passport number of the connected party). Registered/business address or principal place of business is required, if appropriate. A connected party is defined as having "executive authority" in a legal person or arrangement, or being the partner or manager of a partnership. This includes those persons in a senior management position.

Criterion 10.10 – For customers that are legal persons, FIs are required to identify the natural persons (whether acting alone or together) who ultimately own the legal persons. As explained in

[52]The exemptions are : a Singapore Government entity ; a foreign government entity ; any entity listed on the Singapore Exchange; an entity listed on a stock exchange outside Singapore that is subject to (i) regulatory disclosure requirements; and requirements relating to adequate transparency in respect of its beneficial owners; a financial institution set out in Appendix 1 to the Notices and Directives; a financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with the FATF Standards; and an investment vehicle where the managers are financial institutions.

relation to c.10.5 above, this provision meets the definition of ultimately having a controlling interest in the legal person, set out in footnote 33 to c.10.10. As also mentioned above, the MAS Notices and Directives, and the PMFTR for moneylenders also explicitly provide for exemptions in relation to this requirement which are consistent with the example in footnote 31 to c.10.10.

To the extent that there is doubt as to whether the natural persons who ultimately own the legal person are the beneficial owners or where no natural persons ultimately own the legal person, FIs should identify the natural person, if any, who ultimately control the legal person or have ultimate effective control of the legal person. If still no natural persons are identified, the FIs are required to identify the natural persons having executive authority, or an equivalent similar position, in the legal person.

Criterion 10.11 – In the case of trusts, the MAS Notices and Directives, and the PMFTR for moneylenders require the identification of the settlor, trustees, protector (if any), beneficiaries (including every beneficiary that falls within a designated characteristic or class), and any other natural person exercising ultimate ownership, ultimate control or effective control over the trust (including through a chain of control or ownership). For other types of legal arrangements, the persons in equivalent or similar positions must be identified.

Criterion 10.12 – MAS Notice 314 to direct life insurers contains the necessary requirements to conduct CDD on the beneficiary of life insurance policies, as soon as the beneficiary is identified or designated, (including those beneficiaries designated by characteristics or by class or by other means) and the identity must be verified at the time of pay-out. Moreover, other FIs are also involved in the distribution and performance of certain CDD measures of life insurance and other investment-related insurance policies, and the beneficiary's identity could already be known at an earlier stage, before the direct life insurer becomes involved. Therefore, the MAS Notices to banks, merchant banks, finance companies, financial advisers, and capital markets intermediaries contain a specific requirement for these FIs to obtain, as soon as a beneficiary of a life policy is designated and is known to these FIs, sufficient information concerning the beneficiary to satisfy the direct life insurer that such direct life insurer will be able to establish the identity of the beneficiary at the time of pay-out.

Criterion 10.13 – MAS Notice 314 contains various provisions (Para. 6.14-6.20, 6.38(b), 8.2, 8.3, and 8.5-8.7) referring to specific circumstances where Enhanced Due Diligence (EDD) measures should be carried out (e.g. FATF listing, PEPs). Direct life insurers are explicitly required to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable.

Criterion 10.14 and 10.15 – This criterion does not apply to money-changers and remittance agents, central depository systems, and moneylenders because they are not allowed to establish business relations with a customer before completing identification and verification of the customer's identity. The MAS Notices and Directives for other FIs, and the PMFTR for moneylenders require FIs not to enter into any business relationship or perform any occasional transactions exceeding SGD 20 000 (approx. EUR 13 192 / USD 14 042) or an occasional cross-border wire transfer that exceeds SGD 1 500 (approx. EUR 989 / EUR 1 053) until they have complied with their due diligence

obligations for potential customers and their beneficial owners. The general exemption from this requirement provides that the circumstances which warrant postponing the verification must be such that the activities between the financial institution and the customer must not interrupt the normal conduct of business operations. In this case, the identity verification must be done as soon as reasonably practicable, and the ML/TF risks be effectively managed based on internal risk management policies and procedures. Therefore, FIs wishing to defer verifying a customer's identity shall develop and implement internal risk management policies and procedures concerning the conditions under which such business relations may be established prior to verification.

Criterion 10.16 – FIs are required to perform CDD measures in relation to their existing customers, based on their own assessment of materiality and risk, taking into account any previous measures applied, the time when the measures were last applied to such existing customers and the adequacy of data, documents or information obtained.

Criterion 10.17 – FIs are required to apply at least the following specific set of enhanced CDD measures for business relations with or transactions for any customer (i) who the FI determines based on the application of its internal risk management systems, policies, procedures and controls; or (ii) the Authority or other relevant authorities in Singapore notify to the FI as presenting a higher risk for ML or TF:

- obtain approval from the FI's senior management to establish or continue business relations with the customer;
- establish, by appropriate and reasonable means, the source of wealth and source of funds of the customer and any beneficial owner of the customer; and
- conduct, during the course of business relations with the customer, enhanced monitoring of business relations with the customer. In particular, the FI shall increase the degree and nature of monitoring of the business relations with and transactions for the customer, in order to determine whether they appear unusual or suspicious.

Criterion 10.18 – The various MAS Notices and Directives allow for simplified CDD measures to be performed if FIs are satisfied that the risks of ML and TF are low. The Notices and Directives prohibit simplified CDD measures to be applied in the following circumstances:

- where a customer or any beneficial owner of the customer is from or in a country or jurisdiction in relation to which the FATF has called for countermeasures;
- where a customer or any beneficial owner of the customer is from or in a country or jurisdiction known to have inadequate AML/CFT measures, as determined by the FI for itself or notified to FIs generally by the Authority, or other foreign regulatory authorities; or
- where the FI suspects that money laundering or terrorism financing is involved.

Based on paragraph 7.5 of MAS Notice 626 FIs are also allowed to perform simplified CDD measures in relation to a customer that is a financial institution set out in Appendix 2 to the Notice if the FI is satisfied that the ML/TF risks are low and simplified CDD is not prohibited. This provision satisfies the FATF requirements.

Criterion 10.19 – The Notices and Directives provide that where a FI is unable to complete relevant CDD measures, it shall not commence or continue business relations with any customers, or undertake any transaction for any customer. Financial institutions are required to consider if the circumstances are suspicious so as to warrant the filing of an STR.

Criterion 10.20 – Where a FI forms a suspicion of ML or TF, and reasonably believes that performing any of the CDD measures will tip-off a customer, a natural person appointed to act on behalf of the customer, a connected party of the customer or a beneficial owner of the customer, the FIs are permitted not to perform those measures. In such cases, FIs are required to document the basis for their assessment and file an STR.

Weighting and Conclusion

Singapore's CDD rules largely mirror the requirements of the FATF Recommendations. Amendments made during the on-site visit further enhanced the rules.[53]

Recommendation 10 is rated compliant.

Recommendation 11 – Record-keeping

Singapore was rated largely compliant with Recommendation 10 in its 3rd round MER because the requirements to maintain business correspondence were set out in other enforceable means, not law or regulation, and commodities futures brokers were not yet covered by the AML/CFT obligations. Since the adoption of the 3rd round MER, AML/CFT obligations were extended to commodities futures brokers. Singapore has recently amended the MAS Act and MAS Notices and Directives to implement the requirements of Recommendation 11. The moneylenders PMFTR 2009 implements record keeping requirements for moneylenders.

Criterion 11.1 – The Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA) and Monetary Authority of Singapore (MAS) Act require FIs regulated by MAS to maintain records for at least five years after the date on which the transaction takes place or the account is closed (CDSA: ss. 36 and 37 and MAS Act, s. 27B). There does not appear to be a general requirement to keep CDD records in the Moneylenders Act, but this is set out in the PMFTR 2009.

For FIs, other than moneylenders, specific details of the requirements on record-keeping are contained within the MAS Notices and Directives. For moneylenders, detailed requirements on record-keeping, including CDD, are contained within the moneylenders PMFTR 2009.

[53] These included amendments to the requirements for CDD for beneficiaries of life insurance policies and for SVFs.

Criterion 11.2 – The various MAS Notices and Directives and the moneylenders PMFTR contain the following requirements for record retention periods which cover all aspects of the criterion:

- for CDD information relating to the business relations, wire transfers and transactions undertaken without an account being opened, as well as account files, business correspondence and results of any analysis undertaken, a period of at least 5 years following the termination of such business relations or completion of such wire transfers or transactions;
- for data, documents and information relating to a transaction, including any information needed to explain and reconstruct the transaction, a period of at least 5 years following the completion of the transaction.

Criterion 11.3 – The various MAS Notices and Directives and the moneylenders PMFTR require transaction records to be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

Criterion 11.4 – Under the MAS Notices and Directives and the moneylenders PMFTR, FIs are required to ensure that:

- the MAS or other relevant authorities in Singapore and the internal and external auditors of the bank are able to review the FI's business relations, transactions, records and CDD information and assess the level of compliance with the Notice or Directive; and
- the FI can satisfy, within a reasonable time or any more specific time period imposed by law or by the requesting authority, any enquiry or order from the relevant authorities in Singapore for information.

Weighting and Conclusion

Recommendation 11 is rated compliant.

Recommendation 12 – Politically exposed persons

In its 3rd round MER, Singapore was rated compliant with Recommendation 6. Since then, the FATF Standards have changed and Singapore has amended the MAS Notices and Directives to implement the new requirements. The MAS Notices and Directives and PMFTR define domestic PEPs, foreign PEPs and international organisation PEPs consistent with the definition in the FATF Glossary.

Criterion 12.1 – For foreign PEPs, FIs are required to implement the four additional measures set out in R.12 (risk management systems, management approval, establishing the source of funds, and ongoing monitoring). The text of the Notices and Directives and PMFTR closely follows the text of R.12.

Criterion 12.2 – The various Notices and Directives and PMFTR provide that FIs may adopt a risk-based approach in determining whether to perform enhanced CDD measures and the extent of enhanced CDD measures to be performed for domestic PEPs, international organisation PEPs and

PEPs who have stepped down from their prominent public functions, taking into consideration the level of influence such persons may continue to exercise after stepping down from their prominent public functions. In cases where there is such a higher risk business relationship involved, FIs are required to implement the additional measures as set out in c.12.1 (b) to (d).

Criterion 12.3 – The relevant measures must be applied to family members and close associates of PEPs, with both terms defined in the Notices, Directives and PMFTR.

Criterion 12.4 – Singapore provides that this criterion is applicable to direct life insurers only and not to other types of FIs. While other FIs may be involved in the distribution and performance of certain CDD measures of life insurance and other investment related insurance policies, pay-outs of life insurance proceeds are made by direct life insurers and hence they are ultimately responsible for meeting the AML/CFT requirements in relation to beneficiaries of insurance policies. On that basis, MAS Notice 314 to direct life insurers contains requirements to take reasonable measures to determine if the beneficiary of a life insurance policy (or the beneficial owner) is a PEP or family member or close associate of a PEP prior to payment of the benefit. If higher risks are identified, FIs are required to inform senior management, conduct enhanced scrutiny of the entire business relationship, and increase the degree and nature of monitoring of the business relations with, and transactions undertaken in the course of business relations for, the customer, in order to determine whether they appear unusual or suspicious. In addition, in such instances, there is a direct requirement to consider making a suspicious transaction report.

Weighting and Conclusion

Recommendation 12 is rated compliant.

Recommendation 13 – Correspondent banking

In its 3rd round MER, Singapore was rated compliant with Recommendation 7. Since then, relatively minor changes were made to R.13, with criterion 13.3 being the only substantial addition. The financial institutions that engage in correspondent banking or other similar services are: banks, merchant banks; finance companies, capital markets intermediaries, central depository systems and banking entities under the financial holding companies.

Criterion 13.1 – The financial institutions mentioned above are required to apply the measures prescribed by R.13 in respect of cross-border correspondent banking relationships with respondent institutions from third countries, including gathering sufficient information to understand the respondent's business, assessing the respondent's AML/CFT controls, obtaining approval from a senior manager, and documenting the responsibilities of each institution.

Criterion 13.2 – There are requirements in the MAS Notices and Directives to ensure that: (1) the respondent bank has performed appropriate CDD measures on the third party having direct access to the payable-through account; and (2) the respondent bank is able to perform on-going monitoring of its business relations with that third party and is willing and able to provide customer identification to the correspondent bank upon request.

Criterion 13.3 – Financial institutions in Singapore are prohibited from entering into or continuing correspondent banking relations with a shell bank and are required to take appropriate measures to ensure their correspondents do not permit accounts to be used by shell banks.

Weighting and Conclusion

Recommendation 13 is rated compliant.

Recommendation 14 – Money or value transfer services

In its 3rd round MER, Singapore was rated largely compliant with Special Recommendation VI. The 3rd round MER considered that Singapore had implemented most elements of the Recommendation, but noted that: (i) the risk of unlicensed MVTS was not fully addressed; and (ii) deficiencies identified in other Recommendations (i.e. Recs. 5, 8, 10, 13, 14 and SRVII) had a cascading effect on the compliance with this Recommendation. Since then, Singapore has taken measures to address these deficiencies.

Criterion 14.1 – In Singapore, money-changing and remittance businesses are regulated and supervised by the MAS under the MCRBA. They need a licence to carry on their business (MCRBA ss. 5 to 9) and are subject to MAS Notice 3001. Their license has to be annually renewed.

Criterion 14.2 – Singapore uses a series of measures involving various agencies to identify natural or legal persons that carry out money-changing or remittance businesses without a licence and to raise awareness among relevant parties on this issue. The CAD (Commercial Affairs Department) is the agency that investigates unlicensed remittance activities and it works closely with MAS in this regard (for instance, to verify the status of the remittance business and in particular, whether a valid licence has been issued). These measures include: (1) physical surveillance through walkabouts; (2) detection via tip-offs; (3) analysis of STRs and other intelligence; (4) referral from other agencies; (5) raising awareness among investigators; (6) outreach to remittance licensees; (7) confidence-building measures for remittance customers; (8) outreach to the financial sector; (9) targeted efforts focused on higher risk areas/sectors; and (10) outreach to the general public. In addition, MAS has powers under section 23 of the MCRB Act to authorise a person to enter and inspect the premises, where it has knowledge or suspicion that the premise is being used to carry out unlicensed remittance activities.

Under section 6 of the MCRB Act, the maximum penalty for operating a remittance business without a licence is a fine not exceeding SGD 100 000 EUR (EUR 65 960 / USD 70 210) or imprisonment for a term not exceeding two years or both. The financial penalty on its own is relatively low as opposed to the financial penalty imposed to unlicensed banks (i.e., a fine not exceeding SGD 125 000 / EUR 82 450 / USD 87 763), and Singapore reports that MAS is reviewing the penalty framework for conducting unlicensed remittance activities, with the view to increasing the maximum penalties.

Criterion 14.3 – MAS has a dedicated team specialised in regulating and supervising holders of money-changers' and remittance licences. This team assesses all licence applications and renewals

and issues licences accordingly. Its core functions also include the performance of both off-site monitoring and on-site inspections to ensure that licensees comply with all necessary AML/CFT regulations (MAS Act: s. 27B; MCRB Act, ss. 7 and 8; and MAS Notice 3001, Para. 1.1).

Criterion 14.4 – Paragraph 11.1 of MAS Notice 3001 defines an agent as "*Any natural person or legal person (that is not a financial institution) that contracts with or is under the direction of a licensee to assist in the provision of remittance business, but does not itself carry out the remittance business.*" Based on Paragraph 11.4 of MAS Notice 3001, a licensee is required to maintain a current list of its agents that it engages and to make the list accessible to MAS and to other relevant authorities in the countries or jurisdictions where the agents operate, upon request. Singapore reports that only remittance businesses operating in Singapore use agents during the course of their business while money-changers are not permitted to use agents.

Criterion 14.5 – Paragraph 11.2(d) of MAS Notice 3001 provides that a licensee should include all its agents in its AML/CFT programme and monitor them for compliance with its programme.

Weighting and Conclusion

MVTS are licensed and supervised by the MAS, which has taken a number of initiatives to ensure that all MVTS are licensed. The financial penalty imposed on non-licensed MVTS is relatively low.

Recommendation 14 is rated largely compliant.

Recommendation 15 – New technologies

In its 3rd round MER, Singapore was rated largely compliant with Recommendation 8. The MER identified that: (i) requirements concerning non-face-to-face business for commodity futures brokers were not in place; and (ii) the recent implementation of relevant measures for moneylenders were too new to be assessed. Recommendation 15 of the FATF 2012 Recommendations focuses on new technologies and the requirements regarding non-face-to-face business are now included in R.10.

Criterion 15.1 – MAS has a dedicated team to monitor and assess the ML/TF risks of new technological developments across the financial sector. For moneylenders, the Registrar within the Ministry of Law identifies potential risk areas in the course of its supervision. The Registrar is an individual person, who is also the Registrar of Pawnbrokers, the Official Assignee, and the Public Trustee. In practice, it is the Insolvency & Public Trustee's Office (IPTO), a department within the Ministry of Law, that assists the Registrar with the regulation, supervision and monitoring of Moneylenders and Pawnbrokers. In addition, when conducting analysis, the FIU (STRO) comes across emerging typologies arising from new technologies, products and business practices and alerts the sector supervisors accordingly. When sector supervisors receive information on crime trends involving new products, businesses practices and technologies, they highlight the information to the STRO to consider strategic analysis. Where there are new technologies, products and business practices that introduce ML/TF risks that affect more than one sector, these are raised for broader consideration through an interagency coordination process, which will also involve the FIU.

Singapore provided concrete examples of ML/TF risk assessments of new products and technologies that it recently conducted.

The relevant MAS Notices and Directives require financial institutions to identify and assess the ML/TF risks that may arise in relation to: (i) the development of new products and new business practices, including new delivery mechanisms, and (ii) the use of new or developing technologies for both new and pre-existing products.

Criterion 15.2 – The MAS Notices and Directives, and moneylenders PMFTR 2009, require financial institutions to pay special attention to any ML/TF threats that may arise from new technologies and take appropriate measures to prevent their use for ML/TF purposes, and in such cases to conduct a specific analysis of possible ML/TF threats. The MAS Notices and Directives and PMFTR 2009 also oblige FIs to undertake a specific risk assessment prior to the launch or use of a new product, service, distribution channel, or technology, and to take appropriate measures to manage and mitigate the risks.

Weighting and Conclusion

Recommendation 15 is rated compliant.

Recommendation 16 – Wire transfers

In its 3rd round MER, Singapore was rated largely compliant with Special Recommendation VII. The MER noted that record keeping was not obliged and that technical limitations prevented the accompaniment of full originator information. Since then, Singapore has addressed these shortcomings. At the same time, the FATF has significantly updated the requirements for wire transfers.

The legal framework for wire transfers in Singapore applies to banks, merchant banks, finance companies, banking entities under the financial holding companies and holders of money-changer's licence and remittance licence. The applicable rules are enforced through MAS Notices 626 (banks), 1014 (merchant banks), 824 (finance companies), and 3001 (holders of money-changer's license and remittance license) and MAS Directive 17 (financial holding companies). The legal framework incorporates the language of the FATF Methodology for Recommendation 16, in most cases word for word.

Criteria 16.1 and 16.2 – The MAS Notices and Directive mentioned above oblige financial institutions to ensure that all cross-border wire transfers of SGD 1 000 (approx. EUR 660 / USD 702) or more are accompanied by accurate originator information and beneficiary information as specified in c.16.1. If cross-border wires are bundled in a batch, the MAS Notices and Directive oblige financial institutions to ensure that the batch contains all the required and accurate information and is traceable.

Criteria 16.3 and 16.4 – The MAS Notices and Directive oblige financial institutions to ensure that cross border wire transfers below the threshold of SGD 1 000 (USD 740 / EUR 670) are accompanied by accurate originator and beneficiary information.

Criteria 16.5 and 16.6 – For domestic wire transfers, the MAS Notices/Directives oblige ordering financial institutions to include information that is required for cross-border transfers. In case the information is not available, financial institutions are required to make this information available within three business days.

Criteria 16.7 - 16.12 – The MAS Notices and Directive oblige financial institutions to collect all originator and beneficiary information and to keep the information for five years. Incomplete wires may not be executed. FIs are not permitted to execute wire transfers unless they are able to comply with the requirements stipulated in the MAS Notices and Directive. Intermediary financial institutions are required to maintain all originator and beneficiary information with the wire, and where technical limitations prevent this with a domestic transfer, a record needs to be kept for 5 years with all of the information. Intermediary financial institutions are required to take reasonable measures to identify cross border wire transfers that lack the required information and they are obliged to have risk-based policies and procedures on how to deal with such wires.

Criteria 16.13 – 16.15 – The MAS Notices/Directive oblige beneficiary financial institutions to take reasonable measures to identify wires that lack the required information, and to verify the identity of a beneficiary of the wire (above SGD 1 000 and if not already identified). Beneficiary financial institutions are also required to take reasonable measures to identify cross border wire transfers that lack the required information.

Criteria 16.16 and 16.17 – MAS Notice 3001 obliges holders of money-changer's licences and remittance licences, including their agents, to comply with all of the requirements of Recommendation 16. In the case that a holder of a money-changer's and/or remittance licence controls both the ordering and beneficiary side of a wire transfer, that holder is required to: (i) take into account all of the information for both sides to determine whether an STR has to be filed, and (ii) to file an STR in any country affected by the suspicious wire transfer and to make relevant information available to the FIU.

Criterion 16.18 – The MAS Notices/Directive oblige financial institutions to screen all wire transfer originator and beneficiary information against lists and information provided by the MAS. MAS Act (Article 27A) also obliges financial institutions to take freezing actions against designated persons and entities.

Weighting and Conclusion

Recommendation 16 is rated compliant.

Recommendation 17 – Reliance on third parties

In its 3rd round MER, Singapore was rated largely compliant with Recommendation 9. The main deficiency identified in the MER was that there was no requirement for FIs to immediately obtain CDD information on introduced customers, in addition to commodities futures brokers not being subject to AML/CFT requirements. Since then, Singapore extended AML/CFT obligations to commodities futures brokers and the relevant MAS Notices and Directives, as well as the

moneylenders PMFTR, were amended to address the other technical deficiency. For regulatory references for compliance with the individual criteria of R.17 set out below, see Annexes.

Criterion 17.1 – MAS Notices/Directives oblige financial institutions to take measures consistent with R.17 in that reliance is not permitted for ongoing monitoring of the business relationship and, where reliance is permitted, ultimate responsibility for completing CDD remains with the relying FI. The conditions for allowing such reliance include that the third party make the relevant CDD information available and, when so requested, immediately forward copies of identification data and other documents to the relying reporting FI. Relying FIs are also required to ascertain that (i) the third party is subject to AML/CFT obligations; (ii) it is under supervision for compliance with these obligations, and (iii) it has adequate procedures for compliance with CDD and record-keeping requirements. This satisfies all the elements of the criterion.

Criterion 17.2 – The MAS Notices and Directives permit financial institutions to rely on a third party only when certain conditions are met. The conditions include that the third party is supervised for compliance with AML/CFT requirements consistent with the FATF Recommendations, and that it has adequate AML/CFT measures in place to comply with those requirements (MAS Notice 626 9.2(a)). The MAS Notices and Directives require FIs to take appropriate steps to identify, assess and understand the ML/TF risks particular to the countries or jurisdictions that the third party operates in.

The Moneylenders PMFTR 2009 does not permit moneylenders to rely on a third party for the performance of CDD measures unless it is approved by the Registrar. As part of the approval process, the Registrar reviews and assesses the ML/TF risks of the countries that such third parties are based in. Where ML/TF risks of a certain country or jurisdiction are assessed to be high, the Registrar has the necessary powers to prohibit moneylenders from relying on third parties from the particular country or jurisdiction. In addition, moneylenders are required to take appropriate steps to identify, assess and understand the ML/TF risks particular to the countries or jurisdictions that the third party operates in.

Criterion 17.3 – In Singapore, the FIs subject to consolidated/group supervision are banks, merchant banks, direct life insurers, financial advisers, capital markets intermediaries and financial holding companies. These FIs are not permitted to accord a different requirement with respect to third parties relied upon for CDD measures that are part of the same financial group. The AML/CFT Notices and Directives define a "third party" to include a FI's subsidiaries, branches, parent FI/corporation and other related corporations. In such scenarios, the relevant FIs are required to comply with the full Notice and Directive requirements in relation to performance of CDD measures by third parties, as set out in c.17.1 and 17.2 above.

Weighting and Conclusion

Recommendation 17 is rated compliant.

Recommendation 18 – Internal controls and foreign branches and subsidiaries

In its 3rd MER, Singapore was rated largely compliant with these requirements. At that time, commodities futures brokers were not yet subject to AML/CFT requirements and the provisions applying to moneylenders were very recent and their effectiveness could not yet be assessed. In Singapore, the relevant FIs for purposes of c.18.2 and 18.3 are banks, merchant banks, direct life insurers, financial advisers, capital markets intermediaries and financial holding companies.

Criterion 18.1 – MAS Notices and Directives and the moneylenders PMFTR require FIs to develop and implement adequate internal AML/CFT policies, procedures and controls, taking into account their ML/TF risks and size of their business, to help prevent ML and TF and to communicate them to their employees. These Notices and Directives and the PMFTR also require FIs to develop appropriate compliance management arrangements, including at a minimum, the appointment of a compliance officer who is at the management level and who is responsible for AML/CFT matters. In addition, FIs are required to maintain an audit function that is adequately resourced and independent and that is able to regularly assess the effectiveness of the financial institution's internal policies, procedures and controls, and its compliance with regulatory requirements. Moreover, FIs should have screening procedures in place to ensure high standards when hiring employees and appointing officers. Finally, FIs are required to take appropriate steps to ensure that their staff and agents, whether located in Singapore or overseas, are regularly trained on AML and CFT.

Criterion 18.2 – The MAS Notices require relevant FIs to put in place adequate safeguards to protect the confidentiality and use of any information that is shared. In addition, they oblige these FIs to develop and implement group policies and procedures for their branches and subsidiaries within the financial group, and to share information required for purposes of CDD and ML/TF risk management. Such policies and procedures include the provision, to the bank's group level compliance, audit, and AML/CFT functions, of customer, account and transaction information from its branches and subsidiaries within the financial group, when necessary for ML and TF risk management purposes.

Criterion 18.3 – Relevant FIs are required to ensure that their group policies on AML/CFT are strictly observed by the management of their foreign branches and majority owned subsidiaries. Where the AML/CFT requirements in the host country or jurisdiction differ from those in Singapore, FIs shall require that the overseas branches or subsidiaries apply the higher of the two standards, to the extent that the law of the host country or jurisdiction so permits. Where the law of the host country or jurisdiction conflicts with Singapore law such that the overseas branch or subsidiary is unable to fully observe the higher standard, the FI shall apply appropriate measures to manage the ML and TF risks, report to MAS and comply with any further directions given by it.

Weighting and Conclusion

Recommendation 18 is rated compliant.

Recommendation 19 – Higher-risk countries

In its 3rd MER, Singapore was rated largely compliant with these requirements, which are now incorporated into R.19. At that time, AML/CFT regulations did not apply to commodities futures brokers, and similar provisions applicable to moneylenders were too recent to be assessed. There was also concern that no enforceable powers had been exercised to require FIs to apply stringent or additional AML/CFT counter-measures against those countries which continue to insufficiently apply the FATF Recommendations. Both Singapore's requirements and the obligations of R.19 have changed significantly.

Criterion 19.1 – Financial institutions are required to implement appropriate internal risk-management systems, policies, procedures and controls to determine if business relationships with or transactions for any customer present a higher risk for money laundering and terrorism financing. If the FIs determine that customers or transactions present a higher ML/TF risk, including instances where the FATF has called for counter-measures or has identified a country as having weaknesses in its AML/CFT regime, they are required to apply at least a set of enhanced CDD measures as required by Para. 8.3 of the MAS Notices and Directives, and Para. 6E(2) of the PMFTR (see also c.10.17 above). These enhanced CDD measures shall be equally applied for business relationships with or transactions for any customer MAS or other relevant authorities in Singapore notify to the FI as presenting a higher ML/TF risk. However, concerns exist as to whether the required enhanced CDD measures in the MAS Notices and Directives, and the PMFTR, as opposed to enhanced CDD measures more broadly, provide for a sufficient wide range of measures that are proportionate to the risks in all instances. In addition, these measures will also depend on other factors such as MAS and IPTO notifying the FIs of the relevant FATF documents.

Criterion 19.2 – Singapore has powers to apply counter-measures against higher risk jurisdictions both in situations called upon to do so by the FATF and independently of any call by the FATF. Section 27B of the MAS Act, provides MAS with the power to issue legally enforceable directions or regulations to prevent money laundering and terrorism financing to the FIs regulated by MAS. Under sections 26(1) and 37(2)(i) of the Moneylenders Act, the Registrar has similar powers in relation to moneylenders. While these provisions do not explicitly refer to counter-measures, they are sufficiently broadly drafted to permit the imposition of counter-measures.

Criterion 19.3 – MAS's website contains a dedicated section on AML/CFT issues. This section is regularly updated to ensure that FIs are informed about the latest FATF public statements on countries and jurisdictions with strategic deficiencies in their AML/CFT regimes. In addition to its website, MAS also proactively disseminates key information, circulars and guidelines about ML/TF risks and concerns in relation to certain countries and jurisdictions to the FIs via a secure communications platform and via email. The Registrar uses a similar approach to advise moneylenders about weaknesses in the AML/CFT systems of other countries.[54]

[54] Ministry of Law (2015), Information for Moneylenders, Anti-Money Laundering and Countering the Financing of Terrorism, www.mlaw.gov.sg/content/rom/en/information-for-moneylenders/briefing-slides-for-moneylenders.html.

Weighting and Conclusion

Singapore has enacted changes to its system to comply with most of the requirements of Recommendation 19. However, concerns exist as to whether the required enhanced CDD provide for a sufficient wide range of measures that are proportionate to the risks in all instances.

Recommendation 19 is rated largely compliant.

Recommendation 20 – Reporting of suspicious transaction

In its 3rd round MER, Singapore was rated as largely compliant with Recommendation 13 and compliant with Special Recommendation IV. Deficiencies identified for Recommendation 13 were: (i) the scope of the predicate offences for STR reporting did not satisfy all the FATF designated categories of predicate offences, and (ii) certain clarifications of the law (reporting to the STRO and attempted transaction) were covered in "other enforceable means" but not in law or regulation. Singapore has since amended its laws and, Notices and Directives.

Criterion 20.1 – The Corruption, Drug Trafficking and other Serious Crimes (Confiscation of Benefits) Act (CDSA), s. 39(1) obliges any person, including financial institutions, to file an STR to the STRO (in the CAD) in the course of trade, profession, business or employment when he/she suspects any property may constitute drug dealing or criminal conduct, including TF (Second Schedule of the CDSA). The statistics provided do not allow conclusion on the timeliness of the reporting, this criterion requiring the "prompt reporting" of STRs.

Criterion 20.2 – The filing of STRs for attempted suspicious transactions is also explicitly covered (s. 39(1A) of the CDSA). The CDSA does not prescribe any monetary threshold on the reporting of suspicious transactions to the STRO. In addition, the MAS Notices and Directives require FIs regulated by MAS to promptly submit reports on suspicious transactions (including attempted transactions), regardless of the amount of the transaction, to the STRO and extend a copy to MAS for information (MAS Notices 626, 1014, and 824: Para. 14.2; MAS Notices 626A, 314, and FAA-N06: Para. 12.2.; MAS Notice 3001: Para. 15.2; CDP Directive: Para. 13.2; and MAS Directive 17 to DBSH and MAS Directive 31 to GEH: Para. 9.3). The moneylenders PMFTR (Para. 7) contains similar requirements for moneylenders with a copy to be extended to the Registrar for information.

Weighting and Conclusion

Recommendation 20 is rated largely compliant.

Recommendation 21 – Tipping-off and confidentiality

In its 3rd round MER, Singapore was rated largely compliant with Recommendation 14. At that time, the scope of the tipping-off provision did not include a case where an STR is in the process of being reported to the FIU. Singapore has since amended its laws and regulations.

Criterion 21.1 – FIs and their employees are exempted from criminal and civil liability when disclosing information on suspicious transactions to the competent authorities (i.e., the STRO or Commissioner of Police) in good faith: CDSA ss. 39(6), 40A and TSOFA ss. 8(5) and 10(3).

Criterion 21.2 – FIs, their directors, officers and employees are prohibited from disclosing the fact that an STR or related information is being filed with the STRO (CDSA ss. 48(1) and (2) and TSOFA ss. 10(B)(1) and 10(B)(2)). In addition, the MAS Notices and Directives provide that FIs regulated by MAS should keep in mind the provisions of the CDSA, in particular section 48 of the CDSA on tipping-off and implement appropriate internal policies, procedures and controls to meet their obligations under the law (MAS Notices 626, 1014, and 824: Para. 14.1 and 14.4; MAS Notices 626A, 314, and FAA-N06: Para. 12.1 and 12.4.; MAS Notice 3001: Para. 15.1 and 15.4; CDP Directive: Para. 13.1 and 13.4; and MAS Directive 17 to DBSH and MAS Directive 31 to GEH: Para. 9.2 and 9.6).

Weighting and Conclusion

Recommendation 21 is rated compliant.

Designated Non-Financial Businesses and Professions

Preamble: Scope of DNFBPs

Scope of Designated Non-Financial Businesses and Professions (DNFBPs) - The chart below gives an overview of the DNFBP sectors in Singapore as well as their regulator/supervisor.

Table 31. **Overview of the DNFBP sectors in Singapore and their regulator/supervisor**

Type of DNFBP entities	Regulator/supervisor
Casinos	Casino Regulatory Authority of Singapore (CRA)
Lawyers	Ministry of Law (MinLaw) and Law Society of Singapore (Law Society)
Trust Service Providers (TSPs)	MAS
Company Service Providers (SCPs)	Accounting and Corporate Regulatory Authority (ACRA)
Professional Accountants	ACRA for public accountants* and the Institute of Singapore Chartered Accountants (ISCA) for professional accountants
Real Estate Agents	Council for Estate Agencies (CEA)
Precious Stones and Metals Dealers (PSMD)	IPTO (pawnbrokers) but currently no supervisor for other PSMDs

* Public accountants are auditors and a subset of professional accountants in Singapore.

At the time of the 3rd round mutual evaluation, all DNFBPs were bound by the CDSA provisions on suspicious transaction reporting (s.39), tipping off (s.48) and protection from liability (s.39(6)). However, at that time, Singapore applied AML/CFT preventive measures only to trust companies (that are regulated as financial institutions) and lawyers. Since that time, AML/CFT requirements were extended to casinos (October 2009; amended in June 2015), real estate agents (November 2013; updated February, September, and November 2015), accountants (November 2014), and CSPs (May 2015). Since October 2014, PSMDs are required to file a cash transaction report for any transaction above SGD 20 000 (approx. USD 14 200 / EUR 12 800),

perform a limited set of CDD measures set out in regulation 5 of the CDSA (CTR) Regulations, and implement internal control measures set out in regulation 6 of the CDSA (CTR) Regulations. However, PSMDs are still not subject to the full range of AML/CFT obligations as required by the FATF Recommendations. Moreover, the Singapore Precious Metals Exchange (SGPMX) is only subject to the STR and record keeping requirements in the CDSA, as well as relevant provisions in the TSOFA. Singaporean authorities have assessed that the pawnbrokers industry in Singapore operates business activities that would fall within the definition of a PSMD. Pawnbrokers make up approximately 25% of the PSMD sector in Singapore. Therefore, Singapore has included pawnbrokers in this category of DNFBPs and recently made Pawnbrokers subject to AML/CFT preventive measures, including on CDD, which are contained in the Pawnbrokers Act and the Pawnbrokers Rules 2015. Pawnbrokers in Singapore can perform 2 types of business activities: (i) pawnbroking transactions, which constitute around 95 % of their business activities, and (ii) the selling of unredeemed pledges via auctions or via their second-hand dealing arms ("non-pawnbroking" activities). The second albeit limited part of their activities is not covered by the AML/CFT obligations. These exemptions for PSMDs present a scope issue.

While all categories of DNFBPs as described by the FATF have now become subject to AML/CFT obligations, there are some inconsistencies in the scope of these requirements across the sectors. With the exception of accountants, there are legally enforceable AML/CFT preventive measures for all categories of DNFBPs. Preventive measures for accountants are set out in the ISCA Ethics Pronouncement-200 (EP-200). While the document is issued by a competent authority (the ISCA) and uses mandatory language, there is no clear link to proportionate and dissuasive sanctions in case of non-compliance with these AML/CFT requirements. While Singapore refers to disciplinary sanctions in s.53 of the Accountants Act, these sanctions relate to breach of professional standards of conduct and are not linked to AML/CFT requirements, including on CDD. In addition, as spelled out in detail in the previous paragraph, 75% of PSMDs in Singapore are not subject to the full range of AML/CFT obligations as required by the FATF Recommendations.

Recommendation 22 – DNFBPs: Customer due diligence

In its 3rd round MER, Singapore was rated non-compliant with Recommendation 12. It was noted that AML/CFT measures for some of the DNFBPs were not consistent with the FATF standards: i.e., real estate agents; accountants; trust service providers (other than trust companies); company service providers (CSPs); and precious stones and metals dealers (PSMDs). In addition, CDD measures for lawyers had some deficiencies. Since then, Singapore has taken steps to enhance its AML/CFT requirements for real estate agents; accountants; licensed trust companies; and CSPs. However, some deficiencies in the scope of the measures still remain in relation to some DNFBPs, and therefore, the level of technical compliance of these governing statutes with Recommendation 22 varies across the DNFBP sectors. The following paragraphs describe the details of the deficiencies.

Criterion 22.1 [CDD].

(a) Casinos: The principle that casinos should conduct CDD is set out in s. 139(1) of the Casino Control Act. All other CDD requirements are included in the Casino Control PMLTFR. However,

the CDD threshold for certain transactions is higher than the USD/EUR 3 000 threshold in the FATF Standards and thus inconsistent with the FATF requirements: (1) SGD 10 000 (approx. EUR 6 596 / USD 7 021) when a patron conducts a cash transaction with a casino operator; and (2) SGD 5 000 (approx. EUR 3 298 / USD 3 521) when a deposit is made into an account of a casino operator.

(b) Real estate agents: CDD obligations are promulgated through the CEA (Council for Estate Agencies)'s Practice Circular. The CEA is the self-regulatory body for real estate agents with a role of regulating and supervising its members, and the Practice Circular meets the FATF requirements for other enforceable means (OEM). However, the principle to conduct CDD is only set out in the Circular but not in law, as required by the FATF Recommendations. CEA has, on 17 September 2015, updated the revised Practice Circular to require CDD to be performed where (i) a customer in a property purchase transaction is a foreigner; and (ii) the estate agent is aware that physical cash is used for the purchase or sale of the property. However, the CEA's Practice Circular only contains a general description of CDD measures and does not specify the detailed requirements such as verification of any person purporting to act on behalf of a customer (c.10.4), understanding of intended nature of the business relationship (c.10.6) and of ownership/control structure (c. 10.8).

(c) Dealers in Precious Stones and Metals (PSMDs): With the exception of pawnbrokers, Singapore has no laws or EM promulgating CDD obligations for PMSDs other than general provisions set out by the CDSA (Corruption, Drug Trafficking and Other Serious Crimes Act). The principle to conduct CDD is not set out in law but in the CDSA (CTR) Regulations. Moreover, the regulations only contain a general description of CDD measures and do not specify the detailed requirements in line with Recommendation 22. Pawnbrokers are required to undertake CDD measures before providing a loan exceeding SGD 20 000 (approx. EUR 13 192/ USD 14 042).

(d) Lawyers and accountants: For lawyers, the principle to conduct CDD is set out in s.70C of Part VA of the Legal Profession Act, while other CDD requirements are contained in the LP-MLFTR. The beneficial ownership requirements contain the same exemptions as identified above in relation to c.10.10. As explained in relation to c.10.10, these exemptions are wider than the example in footnote 31 to c.10.10. For accountants, CDD measures are set out in the ethics standards (ISCA EP-200) issued by the Institute of Singapore Chartered Accountants (ISCA), the SRB for accountants, but the ISCA EP-200 does not qualify as law or other enforceable means.

(e) Trust service providers (TSPs) and company service providers (CSPs): TSPs are regulated as FIs and detailed CDD requirements are set out in the legally enforceable MAS Notice TCA-N03. For CSPs, detailed requirements are set out in the Regulation to the ACRA (Accounting & Corporate Regulatory Authority) Act, including the principle to apply CDD. However, the beneficial ownership requirements contain the same exemptions as identified in relation to c.10.10 above.

Criterion 22.2 [record keeping] – For real estate agents and accountants, the principle that DNFBPs should maintain records on transactions and information obtained through CDD measures is not set out in law (respectively promulgated by CEA Circular for real estate agents and EP-200 for accountants). The other record keeping requirements in c.11.2-c.11.4 are covered by the various sub-sector specific statutes.

Criterion 22.3 [PEPs] – While the EP-200 contains the necessary requirements for accountants, these do not qualify as law or other enforceable means. In addition, PSMDs, which are not licensed as pawnbrokers, are not obliged to conduct CDD for PEPs as the CDSA does not contain any specific CDD requirements for PEPs.

Criteria 22.4 [new technologies] and 22.5 [third parties] – PSMDs which are not pawnbrokers are not subject to requirements on new technologies and reliance on third parties as the CDSA does not have any specific requirements for these aspects. Accountants are required to fulfil these requirements by the EP-200, but this Pronouncement does not qualify as law or other enforceable means.

Weighting and Conclusion

Except for PSMDs without pawnbroker's license and accountants, all DNFBPs are subject to enforceable CDD obligations. Moreover, the record-keeping obligation for real estate agencies is not provided by law.

Recommendation 22 is rated partially compliant.

Recommendation 23 – DNFBPs: Other measures

In its 3rd round MER, Singapore was rated as partially compliant with Recommendation 13. The MER identified deficiencies such as: (i) lack of understanding of the STR reporting obligations, resulting in low numbers of reports filed; (ii) DNFBP entities other than lawyers and trust companies not subject to AML/CFT obligations; (iii) narrow scope of suspicious transactions reporting obligations and tipping-off; and (iv) lack of obligation to require internal controls (former R.15) and special attention to high risk countries (former R.21). Since then, Singapore conducted more outreach sessions to the DNFBPs to increase AML/CFT awareness, and in particular to enhance their understanding of their reporting obligations. Furthermore, the AML/CFT requirements for most of the DNFBP sectors have been amended to include the obligations under the revised Recommendation 18 and Recommendation 19. However, some deficiencies remain as described in the following paragraphs.

Criterion 23.1 [STR] – The requirements to report suspicious transactions set out in relation to Recommendation 20 above equally apply to DNFBPs consistent with the qualifications set out in c.23.1 (a)-(c). The CDSA and TSOFA which oblige any person in Singapore to file an STR are equally applicable to DNFBPs.

Criterion 23.2 [internal controls] – For accountants, the ISCA EP-200 does not qualify as law or other enforceable means. PSMDs are only required to perform internal control measures when entering

into cash transactions set out in the CDSA Regulations, and these Regulations do not cover specific elements as set out in c.18.1 (a)-(d).

Criterion 23.3 [high-risk countries] – Relevant statutes oblige casinos, real estate agents, lawyers, and TCSPs to apply a specific set of enhanced CDD measures when they determine that customers or transactions present a higher ML/TF risk in relation to a specific country, including instances where the FATF has called for counter-measures or has identified a country as having weaknesses in its AML/CFT regime. However, concerns exist as to whether the required enhanced CDD measures in the various sector-specific statutes, provide for a sufficient wide range of measures that are proportionate to the risks in all instances (see also c.19.1 above). In addition, these measures will also depend on other factors such as the DNFBP supervisors notifying the DNFBPs of the relevant FATF documents. Finally, there are no such requirements for PSMDs (except pawnbrokers) and the ISCA EP-200 applicable to accountants does not qualify as law or other enforceable means.

Criterion 23.4 [tipping-off] – The tipping-off and confidentiality requirements set out in relation to R.21 equally apply to DNFBPs consistent with the qualifications set out in c.23.1 (a)-(c). The CDSA and TSOFA, which contain provisions on tipping-off and confidentiality, are applied to any person in Singapore, and they are equally applicable to DNFBPs.

Weighting and Conclusion

All DNFBPs except for PSMDs without pawnbroker's license are subject to obligations regarding internal controls, measures against higher-risk countries and tipping-off but the requirements for accountants are not enforceable. In relation to high-risk countries, the provisions in law or enforceable means do not necessarily provide a wide-range of measures proportionate to risks.

Recommendation 23 is rated partially compliant.

Recommendation 24 – Transparency and beneficial ownership of legal persons

Singapore was rated as partially compliant for Recommendation 33 (now Recommendation 24) in its 3rd round mutual evaluation report. The deficiencies identified were: (i) limited measures in place to ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons; (ii) information in the Accounting and Corporate Regulatory Authority's registers relates to legal ownership (as opposed to beneficial ownership), and is not verified and not necessarily reliable; (iii) foreign companies are not required to keep information on shareholders nor changes to shareholdings at their registered Singapore office unless one or more of the shareholders are Singapore residents; and (iv) limited liability partnerships are not required to collect shareholder information on partners that are bodies corporate.

Criterion 24.1 – Legal persons in Singapore consist of local companies, (including public companies), foreign companies, and limited liability partnerships (LLPs). Other business entities exist in Singapore (partnerships and sole proprietorships) but they are not legal persons. The process for the creation of legal persons and for obtaining and recording basic ownership information is set out in the Companies Act and the Limited Liability Partnerships Act. Mechanisms for the obtaining or

recording of beneficial ownership information (as that term is defined by FATF) beyond the immediate shareholder of a company or a direct interest in a LLP are publicly available.

Government agencies and the public can obtain information filed with ACRA in relation to any business entity for a fee, depending on the information purchased. Government agencies and the public can also obtain information about a business entity (e.g. its registered office address, issued and paid-up capital, particulars of its directors/shareholders/partners/managers/withdrawn partners and managers) from ACRA's website.

Criterion 24.2 – The NRA report does not consider the risk posed by all the forms of legal persons in Singapore (local, private, public, foreign and LLPs) nor does it assess each type separately for the risk they pose for money laundering and terrorist financing. The only concern expressed in the NRA report is in relation to "shell companies" which the report defines as companies formed within or outside Singapore with no legitimate business activity and minimum paid-up capital. The NRA notes that there is an increase in the number of shell companies used for money laundering in Singapore. Outside the content of the NRA report, Singapore appears to have assessed the risk of money laundering and terrorist financing for other types of legal persons however those assessments were internal departmental exercises and were not included in the larger NRA process nor were they subject to wider consultation beyond the department producing it. Consequently the key outcomes of these exercises are not a matter of public knowledge for the purpose of informing financial institutions and other entities of the risks posed by all forms of legal persons.

Criterion 24.3 – The Companies Act (Division 1 of Part III and Division 2 of Part XI) and the LLP Act (Part III) set out the information necessary for a valid registration and establishment of companies and LLPs under each Act.

- The Companies Act requires the local company name, address of the registered office, memorandum and articles of association, as well as the names and details of directors, managers, secretaries and auditors. This information is recorded and maintained by ACRA under section 19 of the Companies Act.
- The Companies Act requires a foreign company seeking to register a branch in Singapore to file with ACRA, among others: a certified copy of the certificate of its incorporation; a certified copy of its charter, statute, memorandum and articles of association or other instrument; a list of its directors containing similar particulars as required from directors of Singapore-incorporated companies; the names and addresses of 2 or more agents resident in Singapore; and registered office address in Singapore (section 368 of the Companies Act).
- The LLP Act (section 15) requires the name of the proposed LLP; the general nature of the business; the registered office; the name, identification number, nationality and usual place of residence of every person who is to be a partner; where any partner is a company, the corporate name, place of incorporation or registration, registration number and registered office of the company; and the name, identification number, nationality and usual place of residence of every person who is to be a manager in the LLP.

The information held by ACRA in relation to companies and LLPs is available to the public.

Criterion 24.4 – The Companies Act requires as follows:

- Public and private companies are required to maintain a shareholders register at the registered office (sections 190 and 191 of the Companies Act) containing the name and address of each shareholder; date at which shares were acquired; number and class of shares held. If shares are held in trust, the trustee may request that the shares be marked in the register as such (section 195(3)). The register is open to the public for inspection (section 192). If the register is not kept at the registered office, the company is required to notify ACRA where the register is kept (section 191).
- Listed companies are required to keep a register of substantial shareholders at their registered office, and the register must be open for inspection by a member without charge and by any other person on payment of a fee (section 88(2) of the Companies Act and section 137C of the Securities and Futures Act (SFA)). A substantial shareholder is a person who holds direct or deemed interest in 5% or more of the voting shares (sections 2 and 4 of the SFA).
- Foreign companies are not required to hold shareholder information in Singapore for either foreign shareholders or resident Singapore shareholders. If the shareholders of a foreign company are resident in Singapore and request their shares to be registered in the foreign company's branch register in Singapore (section 379 of the Companies Act), that information may be recorded but it is not required to be (only on request by the shareholders resident in Singapore). Section 381 of the Companies Act allows resident Singapore shareholders who have asked for their shares to be recorded in the branch register to apply to have them removed from the register.

Criterion 24.5 – The Companies Act and LLP Act provide as follows:

- For public and private companies, under section 197 of the Companies Act, a company must file an annual return with information updates including summary of share capital and shares including details of shareholdings, and particulars of directors and managers. In addition to the annual filing of returns, every Singapore-incorporated company is required to notify ACRA within one month after a person becomes or ceases to be a director of the company, or if the person who is a director of the company becomes disqualified from acting as such; after a person becomes or ceases to be a manager, secretary or auditor of the company; the information required in relation to these appointed persons; and if there is any change in the name, identification number or nationality of any director, manager or secretary (section 173).
- LLPs registered in Singapore are required to notify ACRA within 14 days of any change in the LLP's particulars, and cessation of partners and managers (section 28 of the LLP Act). An LLP must maintain accounts which sufficiently explain the transactions and financial position of the LLP (section 25 of the LLP Act). ACRA has the powers to require the LLP to produce the accounting records for inspection purposes (section 25(4) of the LLP Act).

- For foreign companies, information filed with ACRA in relation to a branch registered in Singapore is required to be updated within 1 month of any change (section 372(1) of the Companies Act). However, nothing in the annual filing requires updating in relation to shareholdings of the foreign company even where a resident Singapore shareholder has requested their shareholdings to be recorded in the foreign company's branch register (see above at c. 24.4).

ACRA may undertake enforcement action against companies and LLPs that fail to file annual returns and annual declarations respectively. Penalties for non-compliance include fines when breaches are addressed or court enforcement action when they are not.

Criterion 24.6 – Singapore uses a combination of mechanisms to ensure that beneficial ownership information is available: legal ownership information held by companies and beneficial ownership information required to be collected and maintained by company service providers (CSPs) in forming companies and as part of ongoing CDD; information held by ACRA; and information disclosed by listed companies relevant to beneficial ownership. In addition, law enforcement agencies, and regulatory and supervisory authorities may obtain beneficial ownership information from FIs, CSPs and other DNFBPs (e.g. lawyers and accountants) who must collect this information as part of their CDD processes.

Financial institutions are required to perform CDD when commencing a business relationship with a legal person, including enhanced CDD for higher-risk customers; identify and verify the identities of the beneficial owners of their customers; ensure that the information obtained is accurate and up-to-date; keep proper records; and update the CDD information, including beneficial ownership information, for existing customers. For instance, *MAS Notice 626* issued April 2015 under section 27B of the MAS Act defines "beneficial owner", in relation to a customer of a bank, as "the natural person who ultimately owns or controls the customer or the natural person on whose behalf a transaction is conducted or business relations are established, and includes any person who exercises ultimate effective control over a legal person or legal arrangement." Rule 6.14 under this notice requires banks, when opening accounts for legal persons, to identify the beneficial owner as defined. Information held by financial institutions is available to relevant authorities upon lawful order. MAS has powers to supervise and assess compliance with AML/CFT requirements, including requesting relevant information for AML/CFT purposes (sections 27B, 27C and 27D of the MAS Act).

Company service providers (CSPs) are subject to AML/CFT regulations which require them to perform the same CDD as listed above for financial institutions when engaging existing and new customers (section 28F(9) of the ACRA Act and Part II of the First Schedule to the ACRA [Filing Agents and Qualified Individuals] Regulations 2015, paragraphs 8 to 10 and 18). CSPs are also obliged to obtain beneficial ownership information from those who do not have *SingPass* access and who wish to create legal persons and act as directors of a company or partners of an LLP. ACRA has the power to require CSPs to provide information obtained by CSPs under section 31(1D) of the ACRA Act when investigating breaches of a CSP's terms and conditions of registration.

A listed company can, by notice in writing, require any member of the company to disclose whether the member holds any voting shares as beneficial owner or trustee, and if the shares are held by the member as trustee, to disclose the particulars of the beneficial owner (section 137F of the SFA). MAS can request for additional information via the company's notice to its member. A substantial shareholder has to notify the company in writing that he is a substantial shareholder or ceases to be so, and if there is any change in shareholding (sections 135 to 137 of the SFA). After the company receives such information, it has to disclose the information to the public (section 137G of the SFA).

Criterion 24.7 – Beneficial ownership information held by FIs and CSPs is required by law to be up-to-date and relevant.

Criterion 24.8 – Singapore-incorporated companies must have at least one resident director in Singapore. A foreign company must have an agent and a registered office in Singapore to which all communications and notices may be addressed (section 370 of the Companies Act). There is nothing in the Companies Act requiring foreign company agents to be accountable to competent authorities for providing beneficial ownership information beyond the registered shareholder.

Criterion 24.9 – While companies have to maintain information required under the Companies Act for as long as they are active, the Act does not require that the information must be kept for a minimum of five years after a company is dissolved, winds up or otherwise ceases to exist. For a liquidated company, the liquidator is required to keep the company's papers and books relevant to the company's affairs (it is not clear that this includes beneficial ownership information) at or subsequent to the commencement of winding up, for a period of only two years from the date of dissolution and may destroy them upon expiration of that period (sections 320(1) and (2) of the Companies Act). Similarly, when an LLP is wound up, all relevant information must be retained by the liquidator for two years (Fifth Schedule to the LLP Act, paragraph 67(2)). CSPs are required to maintain records (including beneficial ownership information) of their customers for at least five years from the end of a business relationship (Part II of the First Schedule to the ACRA [Filing Agents and Qualified Individuals] Regulations 2015, paragraph 18). Pursuant to the MAS AML/CFT Notices and Directions issued under section 27B of the MAS Act, FIs are required to retain CDD information (including beneficial ownership and other relevant information) relating to a business relation/transaction for a period of at least five years following the termination of such a relation/completion of such a transaction.

Basic information filed with ACRA in relation to companies and LLPs is stored permanently in ACRA's database.

Criterion 24.10 – Competent authorities, including ACRA, MAS, the Commercial Affairs Department and the Inland Revenue Authority of Singapore have wide powers to obtain the basic and beneficial ownership information held by relevant parties.

Criterion 24.11 – Bearer shares and bearer share warrants are prohibited from being issued by Singapore companies.

Criterion 24.12 – Under Singapore law, nominee shareholders and nominee directors are permitted. However, there does not appear to be any requirements in the Companies Act for nominees to disclose their status, or the identities of their nominators, to the company. And while CSPs that act as nominees in either case (director or shareholder) and subject to AML/CFT requirements, Singapore law does not require that they, or any other person who acts as a nominee shareholder or director be licensed to do so as a "nominee". This is also the case with LLPs: nominee partners or nominee managers are permitted but with no disclosure requirements or mandatory licencing.

Criterion 24.13 – There are limited fines for breaches of the requirements for reporting and updating the shareholders' registrar with beneficial ownership information under the Companies Act. Greater fines appear in the LLP Act for failure in the same respect, and greater fines and other sanctions are available for failure by CSPs and financial institutions and for regulatory breaches. The fines show some gaps in persuasiveness and consistency.

Criterion 24.14 – Singapore's ability to provide "rapid" international co-operation in relation to information on legal persons is described in recommendations 37 and 40. The scope of the available information covers access by foreign competent authorities to basic information held by domestic authorities and using competent authorities' investigative powers to obtain beneficial ownership information on behalf of foreign counterparts. Singapore is able to provide international co-operation in relation to basic and beneficial ownership information, where it can be obtained from FIs and from CSPs and other DNFBPs (e.g. lawyers and accountants).

Criterion 24.15 – All outgoing requests for assistance are tracked and filed electronically in the Central Authority's Electronic Legal Management System (ELMS). The ELMS has a case movement system which tracks the progress of the requests. The ELMS will automatically detect if no progress is made on an outgoing request according to pre-set parameters and prompt the assigned officer in the Central Authority to follow up on the request with the requested country. The Commercial Affairs Department and the Corrupt Practices Investigation Bureau also monitor the quality of assistance they receive from their foreign counterparts. Both agencies have a system in place to track all outgoing requests. The information tracked includes the date of sending the request, to whom the request was sent, and whether the request has been acceded to. Both agencies will send reminders to their foreign counterparts if no response is received.

Weighting and Conclusion

Singapore did not assess the ML and TF risks associated with all types of legal persons as part of its NRA exercise. There are gaps in foreign registered company information and residency requirements as well as gaps in the length of time that relevant company information must be kept. While Singapore permits nominee shareholders and nominee directors, Singapore law does not generally require disclosure to third parties of this status.

Recommendation 24 is partially compliant.

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

Singapore was rated partially compliant for the previous Recommendation 34 in its 3rd round MER in which it was noted that "…while competent authorities have powers to access information on beneficial ownership in trusts, availability of that information is limited by the fact that only trusts administered by trustee companies and trust company service providers are obliged to maintain such information."

Criterion 25.1 – Singapore does not generally require all forms of trustees of express trusts to obtain and hold adequate, accurate and current information on the identity of settlors, the trustees, protectors (if any), beneficiaries or class of beneficiaries, and any other natural persons exercising ultimate effective control over those trusts. Nor are there any requirements for any form of trustee to hold basic information on other regulated agents of, and service providers to, express trusts, including investment advisors or managers, accountants, and tax advisors. Business trusts established under the Business Trusts Act are a specific form of express trust whose trustee-managers may compel disclosure of identities of beneficial owners although the full range of AML/CFT requirements does not apply to Business Trusts Managers (see also R.1 and preamble on DNFBPs in section 5).

Professional trustees i.e. lawyers, accountants and trust companies do have obligations (including five-year record keeping obligations) as follows:

- Lawyers: required under section 70C of Part VA of the Legal Profession Act and Part 2 of the Legal Profession (PMLFT) Rules (specifically Rules 6 and 8) to conduct CDD in relation to their clients and where the client is a legal arrangement, in relation to the settlor, trustee(s), protector, beneficiaries or class of beneficiaries, and any other individual exercising effective control over the trust (including verification of identity).

- Accountants: required to conduct CDD in relation to their clients and where the client is a legal arrangement, in relation to the settlor, trustee(s), protector, beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including verification of identity). However, the collection of information in relation to beneficiaries is limited to the immediate beneficiary of a trust and not beyond, and if a beneficiary is a legal person or another trust there is no obligation to collect further BO information.[55]

- Trust companies: are FIs (by definition) and are regulated by MAS. Under MAS Notice TCA- NO3, trust companies are required to identify and verify the identities of "trust relevant parties" which include settlors, trustees, beneficiaries, and any other relevant party (Annex A).

Criterion 25.2 – There are no general obligations in Singapore for all trustees to keep accurate and up to date information in relation to trusts. For professional trustees as noted above the obligation

[55] Accountant's Ethics Pronouncement 200 (EP 200) does not contain enforceable sanctions as required by the FATF methodology notwithstanding that it addresses some of these requirements.

exists to keep information accurate and up to date but that information does not cover all elements of a trust (for lawyers and accountants it relates only to their clients and beneficiaries). For trust companies it extends to trust relevant parties.

Criterion 25.3 – If a trust company and lawyer acting as a trustee establishes any contact (including transactions) with another (financial) or business entity institution in Singapore or elsewhere, relating to the provision of any trust business services by the trust company to a trust relevant party, the trust company shall disclose to it that it is acting as a trustee (MAS Notice TCA-N03, paragraph 3.1(d); Rule 10(6) of the Legal Profession (Prevention of Money Laundering and Financing of Terrorism) Rules). However, similar provisions for other professional trustees (accountants) do not exist, nor do more general provisions applicable to all other trustees, who are not professional trustees, exist.

Criterion 25.4 – Trustees are not prevented by law or enforceable means from providing competent authorities with trust-related information.

Criterion 25.5 – Competent authorities including law enforcement (such as the Commercial Affairs Department and the Corrupt Practices Investigation Bureau), STRO and IRAS have powers to obtain information relating to trustees, beneficiaries, trustee's residence and assets managed under a trust.

Criterion 25.6 – International exchanges of trust-related information can be accomplished through MLA requests and where that information is available or could be accessed by domestic authorities, through informal channels. The Inland Revenue Authority of Singapore can exchange trust-related information with a tax authority of another jurisdiction under the Income Tax Act.

Criterion 25.7 – Trustees are required to perform their functions as trustees with a duty of care but the Trustees Act does not provide specific penalties for failing to meet this obligation. While fraud by a trustee is a criminal offence, there are no specific criminal liabilities attached to the duties of trustees. And while common law judicial remedies may apply to trustees for failing to perform their duties, including compensation, restitution and removal, these remedies are not dissuasive.

Criterion 25.8 – There are limited criminal penalties on conviction available to enforce the requirements to grant competent authorities access in a timely manner to information held regarding trusts. However, there do not appear to be any civil or administrative penalties in similar circumstances and therefore proportionate sanctions are lacking in Singapore.

Weighting and Conclusion

Singapore law does not go far enough to impose enforceable obligations on trustees (including professional trustees) to collect beneficial ownership information relating to a trust beyond the immediate beneficiary.

Recommendation 25 is rated partially compliant.

Recommendation 26 – Regulation and supervision of financial institutions

In its 3rd round MER, Singapore was rated largely compliant with these requirements. Deficiencies were that fit and proper tests did not apply to all senior management, and the risks of unlicensed money-changers and remittance agents were not adequately addressed. Since that time, both the FATF requirements and Singapore's legal framework have changed. Regulatory references for compliance with the individual criteria of R.26 set out below are included in Annexes.

Criterion 26.1 – MAS is the consolidated financial sector regulator that supervises the following financial institutions for AML/CFT: banks, merchant banks, finance companies, direct life insurers, money-changers, remittance agents, financial advisers, capital markets intermediaries, stored value facility (SVF) holders, non-bank credit card issuers, central depository systems and financial holding companies. However, future internet-based SVF could be exempted from AML/CFT requirements and could therefore remain outside the scope of AML/CFT rules and supervision for AML/CFT purposes.

The Registrar within the Ministry of Law is designated with the responsibility of regulating, supervising and monitoring moneylenders including for AML/CFT purposes. The Registrar is an individual person, who is also the Registrar of Pawnbrokers, the Official Assignee, and the Public Trustee. In practice, it is the Insolvency and Public Trustee's Office (IPTO), a department within the Ministry of Law, that assists the Registrar with the regulation, supervision and monitoring of moneylenders and pawnbrokers.

Criterion 26.2 – The Core Principles financial institutions in Singapore include banks, merchant banks, finance companies, direct life insurers, financial advisers, capital markets intermediaries, and banking entities and direct life insurers under financial holding companies. All Core Principles FIs are licensed or approved by MAS.

Other categories of FI are licensed, approved, registered, or designated by MAS. The Central Depository is the only central depository system in Singapore and is specifically designated in the Companies Act (Companies Act: ss. 130A and 130C).[56] Moneylenders are licensed by the Registrar.

There are no specific provisions in the Banking Act or MAS Regulations or Notices that prohibit the establishment of shell banks in Singapore. However, shell banks are prohibited from being established or operated in Singapore through implementation of MAS's licensing regime and standard operating procedural manuals.

Criterion 26.3 – Before granting any licences or approval, MAS screens the senior management, the Board of Directors, and substantial shareholders of the applying FI. Where MAS has concerns over any of the key personnel, it has powers to deny the FI a licence or approval. There are currently no fit and proper requirements for SVF holders, but Singapore provides that it is going to introduce amendments to the PSOA to address this. As far as moneylenders are concerned, the Registrar (IPTO) screens all individual applicants, partners and directors, substantial shareholders, and

[56]On 3 January 2016, the CDP Directive, which was issued under the Companies Act, was cancelled and re-issued as MAS Notice SFA03AA-N01.

managers and employees of the applicant before granting a licence or an approval. Where the Registrar (IPTO) has concerns over any of the personnel, it can request the applicant to remove the personnel from the application or to provide alternative personnel instead. Failing this, the Registrar (IPTO) has power to refuse to grant a licence or an approval to the applicant.

After the licence or approval has been granted, most FIs are required, on an on-going basis, to notify MAS of changes to their directors, senior management and substantial shareholders, who will also be checked and screened by MAS. As part of on-going supervision, MAS also monitors for any adverse information on these persons. However, while MAS conducts fit and proper tests on the directors and senior management of the two credit card / charge card licensees operating in Singapore (American Express and Diners Club) there is currently no legal requirement for this class of FI to give MAS prior notice if there are changes to their directors, senior management and controllers. However, MAS has recently issued licensing letters to impose these requirements on both entities. After the licence or approval has been granted, a moneylender is required on an on-going basis to notify the Registrar (IPTO) of changes to its business profile (i.e. directors, substantial shareholders, managers and employees) who will be screened by the Registrar (IPTO) accordingly.

Criterion 26.4 – Core Principles financial institutions are regulated and supervised in line with the Principles set by the BCBS, IOSCO, and IAIS. In 2013, the IMF assessed that "the Singapore financial system is highly developed and well regulated and supervised". The report noted that "Singapore shows a very high level of compliance with the Basel Core Principles", and MAS's "updated regulatory framework and supervisory practices show a high level of observance of the Insurance Core Principles", and "compliance with the IOSCO principles is generally high". For Banking, Singapore obtained "Compliant" for 12 of the 15 Principles relevant to AML/CFT and "Largely Compliant" for the remaining Principles. For Insurance, Singapore received "Observed" ratings for all the core principles relevant to AML/CFT. For Securities, Singapore was assessed as "Fully Implemented" for Principle 29, "Broadly Implemented for remaining Principles, and "Observed' for all the Responsibilities. MAS is also responsible for ensuring that Singapore-incorporated Core Principles FIs are requiring that their branches or subsidiaries overseas observe their group AML/CFT policy.

As set out in c.14.3 above, Money-changers and Remittance Agents are also regulated and supervised by MAS. While moneylenders are regulated by the Registrar (IPTO) and are subject to AML/CFT requirements, the monitoring of the implementation of these requirements is based almost solely on volumes rather than on ML/TF risk.

Criterion 26.5 – MAS's supervisory strategy and activities are based on MAS's Framework for Impact and Risk Assessment of Financial Institutions. This framework is primarily focused on prudential supervision but also impacts on the frequency and intensity of on-site and off-site AML/CFT supervision. In that context, Singapore reports that MAS has introduced tools and processes to enable it to define the institutions' ML/TF risk profile and to identify AML/CFT supervision priorities, individually for each institution or financial group, and for the various sectors more broadly. These tools and processes take into account the institution's or financial group's policies, and the internal control and procedures associated with the FI or the financing group, including risk

management systems and controls, operational management, internal audit and compliance, and oversight and governance arrangements. For moneylenders, the Registrar (IPTO) uses specific matrices to assess the ML/TF risk; however, the impact on the frequency and extent of inspections to be carried out is not clearly established.

Criterion 26.6 – MAS conducts risk assessments of each sector, and then of each institution, as a basis for preparing its AML/CFT supervision. Assessments are updated annually for systemically important FIs and at least once every two years for others. Singapore reports that MAS conducts a risk-based supervisory approach by which supervisory plans and resources can be allocated to the institutions according to their risk profile and their systemic importance. The supervisory approach is guided by the outcomes of the various assessments. The Registrar (IPTO) regularly reviews the risk profiles of the moneylenders it supervises; however, the extent to which ML/TF risk influences this assessment is not established.

Weighting and Conclusion

Singapore has covered most of the requirements of Recommendation 26, and **Recommendation 26 is rated largely compliant.**

Recommendation 27 – Powers of supervisors

In its 3rd MER, Singapore was rated largely compliant with these requirements, due to the fact that MAS' AML/CFT regulations did not apply to commodities futures brokers, and similar provisions applicable to moneylenders were too recent to be assessed. Since then, AML/CFT requirements also apply to commodities futures brokers.

Criterion 27.1 – MAS has a broad range of powers to supervise and monitor compliance of FIs with AML/CFT requirements, including powers of off-site surveillance, auditing and on-site visits and inspections (MAS Act: ss. 27B, 27C and 27D; and Companies [Central Depository System] Regulations: ss. 6 and 7).[57] MAS also uses financial institutions' internal and external auditors to review their institution's compliance with AML/CFT requirements. The Registrar is vested with the necessary powers to supervise and ensure compliance of moneylenders with AML/CFT requirements (Moneylenders Act: ss. 25 and 26, and PMFTR 2015, R.10).

Criterion 27.2 – MAS and the Registrar have the authority to conduct inspections and supervisory visits of FIs, including moneylenders, to examine their AML/CFT controls and procedures (MAS Act: ss. 27C and 27D; Companies [Central Depository System] Regulations, s. 7; and Moneylenders Act: ss. 25 and 26, and PMFTR 2015: R. 10).

Criterion 27.3 – MAS has authority to access all relevant information, and broad powers to require cooperation by the FIs it supervises, including the power to compel production of information (MAS Act: ss. 27B, 27C, and 27D; and Companies [Central Depository System] Regulations, ss. 6 and 7). The

[57] MOF (nd), Singapore's AML/CFT Policy Statement. www.mof.gov.sg/Policies/Anti-Money-Laundering-Countering-the-Financing-of-Terrorism-AML-CFT/Singapores-AML-CFT-Policy-Statement.

Registrar (IPTO) has similar powers under the Moneylenders Act; and the PMFTR 2015 (ss. 25 and 26, and s. 10 respectively). These powers to compel production of information or to obtain access to information for supervisory purposes do not require a court order.

Criterion 27.4 – Singapore has implemented a range of criminal, regulatory and supervisory measures to deal with natural or legal persons who are covered by the FATF Recommendations and fail to comply with their AML/CFT requirements. These include the power to withdraw, restrict or suspend the FI's licence. The regulatory and supervisory measures can be imposed by MAS for all FIs it regulates and by the Registrar for moneylenders. MAS's supervisory penalties and sanctions are guided by the AML/CFT Penalty Framework, which sets out the measures MAS can take against FIs, while the Registrar relies on IPTO enforcement guidelines which set out the measures IPTO may take against moneylenders, including imposing administrative and criminal sanctions. The situation is less clear for the Central Depository. ACRA has some sanctioning powers based on the Companies (Central Depository System) Regulations. It is however, unclear how they can be applied for breaches of the AML/CFT requirements because ACRA is not a competent AML/CFT supervisor for the Central Depository and MAS monitors compliance with the AML/CFT obligations included in its Directive to CDP. Singapore has recently made legislative changes to include the relevant provisions under the Companies Act in the Securities and Futures Act. Following that amendment, MAS has full responsibility for the supervision of CDP, including sanctioning powers. These legislative changes came into force in January 2016. See also analysis regarding R.35 below.

Weighting and Conclusion

Recommendation 27 is rated compliant.

Recommendation 28 – Regulation and supervision of DNFBPs

In its 3rd round MER, Singapore was rated non-compliant with Recommendation 24 as there were no AML/CFT supervisory regimes for real estate agents, PSMDs, accountants, and TCSPs (other than trust companies). The MER also noted that there was no comprehensive AML/CFT monitoring mechanism for lawyers. Since then, Singapore has taken steps to introduce AML/CFT requirements for real estate agents, accountants, CSPs, and PSMDs with a pawnbrokers licence, and implemented a cash transaction reporting regime for all categories of PSMDs. In addition, the AML/CFT obligations for casinos, licensed trust companies and lawyers have been updated to better meet the requirements of the revised FATF Standards. Regulatory references for compliance with the individual criteria of R.28 set out below are included in Annexes.

Criterion 28.1 – All casino operators in Singapore are required to be licensed by the Casino Regulatory Authority of Singapore (CRA). At the point of application for a casino licence and subsequent renewal of a casino licence, the CRA examines the eligibility of the applicant for a casino license, including an applicant's financial background, repute with respect to character, honesty and integrity. These background checks also extend to associates (being beneficial owners, substantial shareholders, board of directors and certain senior management personnel), and special employees (persons holding a licensable function). The CRA verifies criminal records when screening applicants

for a casino licence to prevent criminals or their associates from being a casino operator, as required by c.28.1(b). Casino operators are required to notify the CRA in writing when there are changes to the status of their associates and special employees. When informed of such changes, the CRA performs the necessary checks on the suitability of these associates and/or special employees. Casino operators are supervised for compliance with the AML/CFT requirements in the CCA, Casino Control (PMLTF) Regulations, Casino Control (Internal Controls) Regulations and Internal Controls Code.

Criterion 28.2 [competent authorities/SRBs] – For PSMDs, except for pawnbrokers, there is no designated competent authority or SRB responsible for monitoring and ensuring compliance with AML/CFT requirements. The relevant competent authorities/SRBs for the other categories of DNFBPs are:

- for lawyers: the Law Society of Singapore (MinLaw, Law Society)
- for trust service providers: the Monetary Authority of Singapore (MAS)
- for company service providers: the Accounting and Corporate Regulatory Authority (ACRA)
- for accountants: ACRA and the Institute of Singapore Chartered Accountants (ISCA) for professional accountants
- for real estate agents and salespersons: the Council of Estate Agencies (CEA)
- for pawnbrokers: the Insolvency and Public Trustee's Office (IPTO).

Criterion 28.3 – IPTO is the competent authority for pawnbrokers and carries out on-site AML/CFT inspections and off-site monitoring of pawnbrokers, However, the regulatory regime for PSMDs overall is at a nascent stage and there is only some monitoring of PSMDs' compliance with a limited set of AML/CFT measures (see c.22.1(c) above). While ACRA is the competent authority for monitoring AML/CFT compliance by public accountants, this authority has not yet the necessary powers to undertake AML/CFT inspections of public accountants – inspections currently take place on a voluntary basis. ACRA has put in place a system to monitor public accountants' compliance with the AML/CFT requirements. The other competent authorities and SRBs mentioned above in c.28.2 carry out on-site AML/CFT inspections and off-site monitoring of the other categories of DNFBPs.

Criterion 28.4 – *(a)* IPTO has powers to perform its functions, including powers to monitor compliance by pawnbrokers. However, while the CAD has the necessary powers to ensure compliance with the cash transaction reporting requirements by all PSMDs, there is no designated competent authority for 75% of the PSMD sector. In addition, ACRA does not yet have the necessary powers to inspect public accountants - inspections currently take place on a voluntary basis. Other competent authorities or SRBs have adequate powers to perform their functions. *(b)* The Law Society, MAS, and CEA have the necessary powers to prevent criminals or their associates from being accredited, or from owning, controlling, or managing a DNFBP; both at the time of registration and

when changes occur. ACRA has similar powers in relation to company service providers and accountants. With the exception of pawnbrokers, there are currently no fit and proper measures in place for PSMDs. *(c)* As explained in detail in relation to Recommendation 35 below, the financial penalty structure across the DNFBP sector is quite diverse, with different levels of sanctions applying to individual categories of DNFBPs, and it is not clear how each DNFBP sector warrants a different approach to proportionality and dissuasiveness of sanctions (see also c.35.1 below).

Criterion 28.5 – Consistent with the approach taken with regard to FIs, MAS conducts risk assessments for the TSPs sector as a whole and for individual LTCs, as a basis for preparing its AML/CFT supervision of this sector. The outcomes of these assessments form the basis for MAS to conduct a risk-based supervisory approach by which supervisory plans and resources can be allocated to the various LTCs according to their risk profile and their systemic importance. The supervisory approach is guided by the outcomes of the various assessments. The CRA, Law Society and IPTO conduct risk assessment exercises for casino operators, law firms and pawnbrokers, respectively, to guide their AML/CFT supervisory approaches, and the frequency and intensity of their inspection efforts. With the exception of STR requirements, other categories of DNFBPs only became subject to AML/CFT requirements very recently.

Weighting and Conclusion

All DNFBPs except for PSMDs without pawnbroker's license are subject to regulation and supervision by the competent authorities and SRBs. Given that the AML/CFT measures for the DNFBP sector have put in place recently, it is unclear and premature to conclude: (i) whether sanctions applied to individual non-compliant DNFBP sectors are proportionate and dissuasive enough, and (ii) whether the supervision is on a risk-sensitive basis. In addition, the lack of regulation and supervision over PSMDs without pawnbroker's license poses a threat to the overall AML/CFT systems, especially taking account of the potential magnitude of the sector.

Recommendation 28 is rated partially compliant.

Recommendation 29 - Financial intelligence units

In its 3rd round MER, Singapore was rated largely compliant for former Recommendation 26 as there were concerns about the operational independence of Singapore's financial intelligence unit (FIU), the Suspicious Transaction Reporting Office (STRO). Established in 2000, the STRO is now under the Intelligence Group (ING) of the Commercial Affairs Department (CAD) of the Singapore Police Force (SPF).

Criterion 29.1 – Section 3A of the CDSA confirms the establishment of STRO's responsibilities to receive, analyse and disseminate information. That information comprises all types of reports that reporting entities are required to file, as well as other relevant information that STRO obtains from government bodies and reporting entities upon request.

Criterion 29.2 – STRO serves as Singapore's central agency for the receipt of disclosures filed by reporting entities under the CDSA (Section 39). These disclosures include suspicious transaction

reports (STR), cash transactions reports (also by casino operators and precious stones and metals dealers), cross border movement of physical CBNI reports (Section 48 C).

Criterion 29.3.

- *Sub-Criterion 29.3 a)*. Section 3A(3) enables STRO officers to obtain additional information (including with no specific connection to a previously filed disclosure) from reporting entities for the purpose of performing its analysis. This requirement covers any document or information that may be required to conduct operational and strategic analysis.
- *Sub-Criterion 29.3 b)*. STRO's positioning within SPF gives STRO a direct online access to all enforcement information, including to the SPF-wide case management system 'CRIMES II' which contains information from all enforcement actions conducted by the SPF. STRO can also access databases of other government agencies and a wide variety of public records information.

Criterion 29.4. STRO's analytical branches focus on receiving and analysing information.

- *Sub-Criterion 29.4 a)*. Since the 3rd round MER, STRO has developed a Web-based Intelligence Analytical and Graphical Visualisation System (WINGS), which is a specialised analytical tool for examining and prioritising the reports received. WINGS integrates the various intelligence databases accessible to STRO. All reports received go through automated screenings against the STRO database, but also CRIMES II and commercial databases. The obtained results are analysed using an intelligent business rule-based engine to provide an automated assessment on whether a report requires further in-depth analysis, thereby expediting assignments and identifying urgent and higher risk reports.
- *Sub-Criterion 29.4 b)*. STRO conducts crime (such as shell companies, unlicensed money-lending crimes and since 2013 on tax crimes), industry (such as banking, capital market, remittance businesses and insurance sectors) and country (where priority is based on operational needs) related strategic analysis. To better understand and identify ML/TF-related trends and patterns, STRO refers to its database and also uses the additional information it can receive (see sub-criteria 29.3). The strategic analysis produced by STRO is later used in the NRA – and vice versa- the findings of the NRA also serve to prioritise the strategic analysis.

Criterion 29.5 – The dissemination by STRO of the results of its analysis is set out in Section 3A (1) b of the CDSA. A number of working arrangements facilitate the dissemination towards relevant law enforcement agencies and/or regulatory authorities. Guidelines on STRs referral by STRO to Customs, ICA and CNB are in place. Section 41 (1) of the CDSA provides, with conditions, the dissemination of information to foreign FIUs. Internal guidelines are in place to ensure this dissemination is made via dedicated, secured and protected channels.

Criterion 29.6 – STRO protects its information as follows:

- *Sub-Criterion 29.6 a*). Section 56(1) of the CDSA prohibits disclosure of STRO information, except in cases specified in the CDSA. STRO and LEAs officers are similarly bound to confidentiality by

the Official Secrets Act. STRO has also put in place internal guidelines conditioning the further dissemination of the information to their prior consent. Similar guidelines are in place for the dissemination of information to foreign FIUs.

- *Sub-criterion 29.6 b)*. STRO conducts security vetting on all STRO officers, as a pre-condition to perform their duties within the STRO [STRO also organises mandatory training of its staff on the understanding of their responsibilities in handling and disseminating sensitive and confidential information. STRO has also developed specialised standard operating procedure (SOP) in this regard.

- *Sub-criterion 29.6 c).* Information security is maintained within STRO through its password protected Suspicious Transaction Report Online Lodging System (STROLLS). STRs are uploaded on this portal in encrypted form. Access to WINGS (see sub-criterion 29.4 a) is strictly restricted to STRO officers, or with their prior consent. Regular audits are being conducted to assess whether security procedures are being enforced. Physical access to STRO facilities (which are being separated from all other non-STRO branches) is also limited to appropriately authorised officers.

Criterion 29.7.

- *Sub-criterion 29.7 (a)*. As a distinct division under the Intelligence Group of the CAD, STRO has the authority and capacity to undertake its functions freely. The dissemination of analysed information lies with the Head of STRO. Overall, the decision making process is made from within the STRO.

- *Sub-criterion 29.7 (b) (c) and (d)*. STRO can make arrangements for spontaneous, information exchange with domestic competent authorities and foreign counterparts, without prior approval. While it is located within the SFP, STRO has its own distinct core functions and structure. The status of STRO officers – as set up by Section 2 of the CDSA prohibits any non-FIU related duties. STRO also has its own distinct budget, allocated from the overall SPF budget. STRO receives resources and has full autonomy in deciding on its deployment to carry out its functions. An example of this would be the substantial increase in its manpower (tripled since its 2008 MER).

Criterion 29.8. STRO was recognized as a member of the Egmont Group in 2002.

Weighting and Conclusion

Recommendation 29 is rated compliant.

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

In its 3rd round MER, Singapore was rated largely compliant for the former Recommendation 27. The deficiencies related to effectiveness, namely the low number of ML investigations, as well as the limited use of STRs in the investigation of ML cases. Recommendation 30 contains much more detailed requirements than the former Recommendation 27.

Criterion 30.1 – The law enforcement agencies (LEAs) with responsibility for investigating ML/TF under Singapore's main AML legislation (the CDSA) are the Singapore Police Force (SPF), Central Narcotics Bureau (CNB) and the Corrupt Practices Investigation Bureau (CPIB). Within SPF, the Commercial Affairs Department (CAD) (which also hosts Singapore's FIU – see Recommendation 29) is the lead LEA for investigating ML/TF. CNB (which has a financial investigation division) is also responsible for investigating drug-related predicate offences and the CPIB (which also has a financial investigation branch) is responsible for investigating corruption[58] and bribery-related predicate offences. Immigration and Checkpoints Authority (ICA), Customs, the Inland Revenue Authority of Singapore (IRAS) and the Ministry of Manpower (MOM) are also competent agencies.

Within CAD, ML/TF investigation is the responsibility of a specific enforcement group, the *Financial Investigation Group (*FIG). FIG ensures that all ML/TF cases are properly investigated and provided with cross-jurisdictional assistance. Its manpower has tripled since 2007 (current strength of 68). Since FIG's reorganisation in 2013, there are now four Divisions, each comprised of two distinct branches: *Financial Investigation Branch I, II, and III* (FIB), *CFT Branch* (CFTB), *Asset Confiscation Branch* (ACB) and *International Cooperation Branch* (ICB). The other two branches within the fourth division deal with AML and financial crime policies & operations. FIG's investigations are carried out by a lead investigator. When the magnitude or complexity of the case requires it, a team-based approach will be adopted. Responsibilities within the FIBs include conducting enquiries into the financial aspect of a crime (i.e. identify organised crime groups and the networks used for ML) with a view to develop solid evidence. FIB III will investigate offences relating to false or non-declarations of cross border movement of cash and bearer negotiable instruments. CFTB is the dedicated unit dealing with the investigation of TF offences. This includes the tracing the assets of suspected terrorists to ensure that these assets are frozen in a timely manner. As Singapore takes a preventive approach to TF, TF investigations are led by the Internal Security Department (ISD) along with broader terrorism investigations. ISD works closely with CFTB, which has the lead on criminal TF investigations. This includes the tracing the assets of suspected terrorists to ensure that these assets are frozen in a timely manner and using formal police powers on behalf of ISD.

In terms of technical resources, FIG's investigators can access all existing SPF databases including SPF's case-management system (i.e. offences investigated, charged and convicted; sentencing details for convicted cases; contact information of the investigating units, etc.). FIG also works closely with STRO and CAD's Intelligence Division and can request information from their respective databases. CFTB also works closely with the ISD with respect to TF investigations.

Criterion 30.2 – SPF, CNB and CPIB are authorised under the CDSA (sections 2 and 55) to investigate ML cases. As the agency with prime responsibility, CAD conducts the majority of Singapore's ML investigations. As outlined in its SOPs on international cooperation, CAD's policy is to investigate all domestic ML offences, regardless of whether the predicate offence has been committed within or outside Singapore. SPF and CPIB also pursue ML investigations, together with the associated predicate offence, unless the case involves complex ML. In that circumstance, SPF will refer the case to CAD. CNB refers all ML cases to CAD as a matter of operational efficiency. Other competent

[58] Embezzlement offences (which in Singapore's context include CBT offences, theft offences and cheating offences under the Penal Code) falls under the purview of SPF.

authorities (e.g. ICA, IRAS, Customs and MOM) also refer all ML cases to CAD and there are SOPs in place to guide this process. Parallel financial investigations (e.g. identifying and tracing assets and funds) are conducted whenever proceeds of crime are involved. LEAs focus their financial investigations on major proceeds-generating offences on the basis of Singapore's context and risks. That determination is based not only on the actual amount involved, but also on other factors, such as the occurrence of a predicate offence, its tendency to generate ML activities and its possible social impact. ISD leads investigations into TF and will work closely with CAD's CFTB.

Criterion 30.3 – All LEAs authorised to conduct ML, TF and associated predicates offence investigations (described above) have the authority to identify, trace, and initiate freezing and seizing of property (and other financial benefits) that may have derived from criminal activities. Within the CAD's FIG, all relevant branches (FIB I II III, ACB, CFTB and ICB) deal with asset tracing (in the context of a financial investigation case). ACB, in particular, focuses on asset tracing and analysis of concealed incomes. ACB works closely with CNB and other competent agencies (such as IRAS) by way of multi-disciplinary investigation groups. Under their respective Acts, competent authorities such as Customs, IRAS and ICA are similarly equipped with powers to trace assets involved in offences under their respective purviews.

Criterion 30.4 – ICA, Customs, IRAS and MOM are not authorised under the CDSA to conduct a ML investigation or a TF investigation (under TSOFA's provisions). SOPs for referral of a case to the CAD are in place when these agencies have a suspicion of ML activities in the case under their purview.

Criterion 30.5 – CPIB is the sole and independent LEA for investigating offences under the Prevention of Corruption Act. As such, CPIB investigators are authorised to undertake both predicate and ML investigations [section 17(1) of the PCA and section 55(1) of the CDSA]. CPIB has sufficient powers to identify, trace and initiate freezing and seizing of assets (see Recommendation 4).

Weighting and Conclusion

Recommendation 30 is rated compliant.

Recommendation 31 - Powers of law enforcement and investigative authorities

In its 3rd round MER, Singapore was rated compliant for former Recommendation 28. Recommendation 31 contains much more detailed requirements than the former Recommendation 28.

Criterion 31.1 – The main LEAs which investigate ML, TF and associated predicate offences in Singapore (SPF, CNB, CPIB and ICA) are empowered under the CPC to exercise a variety of investigative powers. Officers of the CAD are given the same powers of investigation conferred to police officers under the CPC. CNB, CPIB and ICA officers are able to exercise the CPC investigative powers relating to their respective predicate offences (section 32 of the MDA; section 17 of the PCA and section 38 of the Immigration Act). The CDSA (section 2) provides SPF, CNB and CPIB officers with complementary powers of investigation and officers of the CAD have further powers under the TSOFA for TF investigations (section 2). These powers are available to police officers located in ISD.

The CPC provides for a range of traditional investigative methods, including the obtaining of documents (section 20), searching persons and premises (sections 32-34), taking and recording of witness statements (sections 22(1) and 23(1)) and seizures (section 35(1)). The CDSA enables authorised officers to apply to court for production orders (sections 30 and 31) and take witness statements (section 9). The CPC and CDSA both have more stringent requirements in order to obtain documents and records from FIs (see sections 20(2) and 31 respectively). Section 34(1) of the CDSA also empowers authorised officers to apply to the court for a search warrant for a specified premises in cases where there are reasonable grounds to suspect that a specified person has carried on or has benefited from criminal conduct (including ML, TF or associated predicate offences) and that there is material on the premises which is likely to be of substantial benefit to the investigation. The authorised officer is also allowed to seize and retain any material (other than items subject to legal privilege) for the purpose of the investigation, provided that it is likely to be of substantial value (by itself or together with other material) to the investigation (section 34(5) CDSA). Court-granted powers to search and seize in the context of TF investigations are set out in section 11(1) of the TSOFA.

Customs officials do not have access to the CPC powers, as they are classified as public servants and not police officers. Part XIII of the Customs Act sets out extensive search, seizure and arrest powers and section 88 sets out a general information gathering power. Sections 65B and 65D of the Income Tax Act and section 84 of the Goods and Services Tax Act provide extensive information-gathering powers to IRAS, including the ability to obtain information, enter premises and copy or take possession of information.

Criterion 31.2 – The CPC specifically empowers LEA officers to access computers and decryption technology (sections 39 and 40). The CDSA furthermore authorises an officer to consent to allowing a person to perform certain acts of ML for the purpose of gathering evidence (section 44(3)(a)(i) of the CDSA). While there is no legislation empowering LEAs to conduct undercover operations and controlled deliveries or intercept communications to target ML/TF, there is nothing preventing the LEAs using such techniques. Singapore provided LEA SOPs outlining the use of such techniques and *How Poh Sun v Public Prosecutor* and *PP V Muhammad Ali Hashim and Others* provide case law demonstrating the use of controlled delivery and undercover operations in investigations.

Criterion 31.3 – As described in criterion 31.1, there are mechanisms in place to identify assets without prior notification to the owner and who the natural or legal person who owns or controls a specific account is (without giving prior notice to the owner) in the context of an investigation (section 20 CPC). MAS is also able to order a sweep of all Singaporean bank accounts under section 27 of the Monetary Authority of Singapore Act and section 26 of the Banking Act to identify in a timely manner whether specific natural or legal persons own or control accounts. Singapore provided case examples showing it can receive responses from all banks in a timely manner.

Criterion 31.4 – The competent authorities investigating ML, TF and associated predicate offences are able to ask for all information collected and held in STRO's database (see criteria 29.2 and 29.3 for more detail on the scope of the database 3). Dissemination of such information is made on the basis of STRO's "*Guidelines on screenings request received from other agencies*". This information can also

be spontaneously provided by STROs, once an analysis of an STR has been completed (same reference document).

Weighting and Conclusion

Recommendation 31 is rated compliant.

Recommendation 32 – Cash Couriers

In its 3rd round MER, Singapore was rated LC on Special Recommendation IX. At that time, Singapore had just established its new declaration system for its cross-border cash movement reporting regime (CBCRR) and the lack of statistics didn't allow for a full assessment of the regime and its effectiveness.

Criteria 32.1, 32.2 and 32.3 – Since 2007, Singapore has had a written declaration system to detect cross-border movement of cash and bearer negotiable instruments (CBNIs) as defined by section 48(B) of the CDSA. Since 2014, the CDSA (section 48(C)) requires a cash declaration for all physical movement into or out of Singapore of CBNIs exceeding the SGD 20 000 threshold (approx. EUR13 192 / USD 14 042) or its equivalent in a foreign currency. The declaration threshold was previously SGD 30 000 (approx. EUR19 788 / USD 21 063). This includes movement by travellers or through mail and cargo. These reports, called Cash Movement Reports (CMRs), must contain full and accurate information as requested in the declaration form (sections 48(C) and (E)). The CMR for travellers requires the following information: bearer, owner, recipient, amount, nature, intended use, origin and destination country.

Criterion 32.4 – SPF's CAD enforces the reporting requirement with support from other government agencies such as the Immigration & Checkpoints Authority (ICA). ICA and CAD officers jointly exercise the powers of investigation listed in the CPC (see criterion 31.1). They can carry out intelligence checks on both incoming and outgoing travellers and can use specific powers under section 48(F) of the CDSA to request and obtain further information from the carrier with regard to the origin of the CBNIs and their intended use. They can conduct physical checks on travellers, their luggage, and any place (including any vehicle, carrier, train, vessel or aircraft). Failure to declare or false declaration cases will be referred to CAD for further investigations in line with the *Inter-Agency Standard Operating Procedures on the Enforcement of CBCRR* (CBCRR SOP).

Criterion 32.5 – A person found guilty of false declaration or a failure to declare will be liable to imprisonment of three years and/or a fine of up to SGD 50 000 (approx. EUR32 980 / USD 35 105) (sections 48C(2) and 48E(2) of the CDSA). These criminal sanctions appear to be proportionate and dissuasive. However, the lack of any civil or administrative sanctions for breaches of the CBCRR may inhibit Singapore from having a sufficient range of options to target non-compliance.

Criterion 32.6 – Information obtained through the declaration system is made available to STRO. Reports about cross-border movements of CBNIs are either submitted directly to STRO (section 48C(5)(c)(ii)) or submitted to an ICA officer (section 48C(5)(c)(i)). If submitted to an ICA officer, they are obliged to submit the report to STRO within a reasonable time (section 48D). While this

obligation only arises 'on request' from a STRO officer, the CBCRR SOP makes an ongoing request that ICA make all reports collected available to STRO daily. This is confirmed by a letter sent from STRO to ICA in October 2015. Reports about receipts of CBNIs from outside Singapore are submitted directly to STRO (section 48E(5)(c)). The information once collected is stored securely within STRO and is available upon request of any law enforcement agency and competent authority in Singapore.

Criterion 32.7 – Singapore has a domestic cooperation framework for the CBCRR that includes SPF, ICA and Customs. All three agencies are part of the Inter-Agency Committee which considers issues relating to the CBCRR, and reports to the AML/CFT Steering Committee. This Inter-Agency Committee meets regularly to share information and coordinate policy decisions and implementation issues. The CBCRR SOP and *Guidelines on investigation into offences involving Cross Border Movements of CBNIs* are in place to facilitate the referral of cases detected by STRO, ICA or Customs to CAD for further investigation. Also, STRO provides access to its information to all relevant LEAs (including SPF and ICA).

Criterion 32.8 – The detection of a false declaration or a failure to declare by travellers is mainly done by ICA officers at the land, air and sea immigration checkpoints. Upon detection of a false or non-declaration, ICA will refer the case to SPF for investigation following the procedure set out in the CBCRR SOP. The police stationed at check points (namely the Airport Police Division (APD) of the Police Land Divisions) will proceed with preliminary checks (such as asserting type and amount of cash), while the CAD is contacted. CAD officers will then conduct further interviews with the offender to establish the source of the CBNIs. In doing so, CAD aims at determining whether there is a suspicion of ML, TF or associated predicate offences. Where there has been a breach of the CBCRR, ICA and SPF officers are able to seize the CBNIs under section 48F(4) of the CDSA .If there has not been a breach of the CBCRR, but there is a suspicion of ML, TF or associated predicate offences, ICA and SPF officers can use the generic seizure powers in section 35 of the CPC to seize the CBNIs (see Recommendation 4). A set of guidelines 'on Investigation into offences Involving Cross Border Movements of Currency and Bearer Negotiable Instruments' The Guidelines on investigation into offences involving Cross Border Movements of CBNIs outline the course of action to be taken in cases of false reporting or failure to report, and in particular sets out rules on how to determine whether seized CBNIs may be linked to ML/TF.

Criterion 32.9 – STRO is able to share information contained in its database (which includes CMRs) with its foreign counterparts subject to a Memorandum of Understanding being in place (section 41(1) CDSA, subject to section 41(2) conditions). Information sharing is also possible with any foreign counterpart provided that the confidentiality of the information can be ensured, and by signing a letter of undertaking. All cases of false and/or non-declaration being investigated by CAD are stored in SPF's case-wide management system. This information can then be shared with CAD's foreign counterparts (through intelligence channels and upon the consent of the parties involved). This information is also accessible to STRO and therefore can be shared with foreign counterparts.

Criterion 32.10 – Safeguards are in place to prevent unauthorised dissemination of information by authorised officers (section 56(1) of the CDSA), which includes ICA, SPF and STRO officers. Failure to do so is subject to sanctions (fine and/or imprisonment). Moreover, SPF, STRO and ICA officers are

bound by section 5 of the Official Secrets Act, which prohibits them from communicating any information that is obtained by virtue of his/her service with the government in a manner which is contradictory to lawful directions issued in regard to the information or which is without reasonable care to the safety of the information (see criterion 29.6 for further information on STRO confidentiality and protection of data). The CBCRR SOP explicitly states that the CBCRR is not a currency control measure, as there are no restrictions on the type and amount of CBNIs which may be moved into or out of Singapore.

Criterion 32.11 – In the event of confirmed suspicion of ML/TF activity, the person carrying the CBNIs can be subject to the sanctions applicable to ML/TF offences, as set out in the CDSA and TSOFA (see description of sanctions under Recommendations 3 and 5). For CBNIs that are seized confiscation will be determined by the judicial authority under section 364 CPC or sections 4 and 5 CDSA (where there are criminal proceedings) or section 370 CPC (where there are no criminal proceedings).

Weighting and Conclusion

Recommendation 32 is rated compliant.

Recommendation 33 – Statistics

In its 3rd round MER, Singapore was rated LC for former Recommendation 32. The MER identified a tendency for Singapore not to distinguish statistics collected on cases - involving asset freezing, seizure and confiscation - between those deriving from a predicate offence and the ML investigations. Another weakness identified was the lack of statistics on the volume of international wire transfers. While the language of R.33 has not changed, this Recommendation has taken on more relevance in the context of assessing effectiveness.

Criterion 33.1 – The AML/CTF system is supported by statistics gathered and maintained in the case management systems set up by each key sector (namely the FIU, police and prosecution services).[59]

STRO maintains a wide range of comprehensive statistics relating to STRs received (including data on the reporting entities and their industry) and disseminated (including data on the type of offences and agencies receiving the STRs), as well as statistics on the outcome of the disseminated STRs (including ML/TF investigations, prosecutions, convictions and ML/TF seizures deriving from the STRs).

While Singapore has statistics on the amounts seized and confiscated, the material provided by Singapore has some omissions. While statistics were available in most cases, Singapore had difficulty in providing total amounts of seizure and confiscations, as well as the number of cases in which seizure and confiscation occurred.

[59]Attorney-General Chambers (AGC), Commercial Affairs Department (CAD) of the Singapore Police Force, Corrupt Practices Investigation Bureau (CPIB), Internal Security Department (ISD), and Suspicious Transaction Reporting Office (STRO).

Singapore collects very comprehensive statistics with regards to ML/TF investigations, prosecutions and convictions. National statistics on ML investigations, prosecutions, convictions and sanctions are available annually and can be disaggregated to show underlying predicate offending and the type of laundering involved. LEAs collect statistics to monitor the outcome of their investigations and to understand more about recent crime trends. These statistics are reported to the heads of the respective agencies, who then report them to the AML/CFT Steering Committee. The analysis of these reports then aims at guiding law enforcement actions.

With regards to MLA and other international cooperation requests statistics, Singapore maintains comprehensive statistics, such as the type of assistance sought, received, legal basis for the request and its nature.

With regards to other forms of international cooperation, Singapore collects statistics on the requests made, received and spontaneously exchanged. This includes a breakdown of the informal requests received by predicate offences and status of the requests.

Weighting and Conclusion

Although Singapore collects comprehensive statistics in certain areas, most notably ML/TF investigations, prosecutions and convictions, MLA/other international cooperation there are gaps in relation to total amounts of seizure/confiscations, and the number of cases in which seizure and confiscation occurred.

Recommendation 33 is rated largely compliant.

Recommendation 34 – Guidance and feedback

Singapore was rated largely compliant with Recommendation 25 in the 3rd round MER. The MER noted the lack of comprehensive guidelines for a number of DNFBPs and the absence of general or specific feedback to these DNFBPs concerning their suspicious transaction reporting obligation. Some DNFBP supervisors have now issued guidance documents to their industries. In addition, initiatives have been taken to enhance the DNFBP sectors' understanding of their STR filing obligations and provide STR related feedback.

Criterion 34.1 – Supervisors' guidance and outreach to financial institutions: MAS and IPTO (for money lenders) use a range of measures to provide guidance and feedback to the financial institutions they regulate and supervise to assist them with the understanding of and compliance with their AML/CFT obligations. MAS has issued a set of guidelines to complement each of the 13 MAS AML/CFT Notices and Directives issued to the FIs under its supervision. These guidelines contain references to international standards, and best practices and guidance issued by international organisations, including the FATF. The key topics covered in these documents are conducting risk assessment, CDD, correspondent banking, proliferation financing issues, and red flag indicators for STR filing. In addition, the guidelines also include details related to the MAS' supervisory expectations, good practices and common weaknesses observed during AML/CFT inspections. In addition, MAS also issued various Topical Guidance Papers, including on the NRA and Trade Finance. Similarly, IPTO

published in April 2015 an online information note to provide more guidance to the industry to complement the PMFTR 2009. This information note provides general background information on ML/TF and details on the NRA, United Nations Security Council Resolutions, and suspicious transaction reporting. Before considering further written revisions based on the September 2015 updates to the PMFTR, IPTO is looking to give the industry time to first focus on the revised PMFTR, to put in place the necessary controls and to better understand their concerns on the ground with the revised requirements. Therefore, the current guidance is presumably not complete.

Supervisors' guidance and outreach to DNFBPs: DNFBP supervisors have been providing guidance to the entities under their supervision with the aim to provide greater clarity and consistency in these sectors' understanding of their AML/CFT obligations, ML/TF risks and supervisory expectations. However, given the nascent stage of the AML/CFT regime for most of the DNFBPs (see preamble on DNFBPs above), this is still work in progress. At the time of drafting this TC Annex, MAS had issued guidance for TSPs consistent with its guidance for the financial sector; the Law Society had issued (in July 2015) an updated set of Practice Directions to provide guidance to lawyers and to supplement the Legal Profession (PMLFT) Rules 2015; the CRA had issued a Practice Note to provide guidance to the casino operators (in August 2015); [joint CEA-CAD guidance note]; ACRA had issued Guidelines that applied to the CSP sector; and the Commercial Affairs Department (CAD) had published a guidance note on internal controls, brochures, posters and an FAQ explaining the AML/CFT obligations for PSMDs. Singapore reports that DNFBP supervisors also held outreach sessions for their industries to raise the general level of AML/CFT and proliferation finance awareness.

Supervisors' feedback: Singapore reports that observations and findings from MAS' and IPTO's AML/CFT inspections are shared with the inspected entity to provide timely feedback on areas for improvement. In addition, collation of good practices and common weaknesses observed during MAS' AML/CFT inspections of regulated FIs are communicated to the industry. IPTO is taking a similar approach and is currently putting together the common weaknesses and best practices based on observations / findings made during its AML/CFT inspections. As far as TSPs and casinos are concerned, observations and findings from AML/CFT inspections and monitoring are shared with the entities to provide feedback on areas of improvements. Similarly as with the guidance, this is an area of work in progress for the other categories of DNFBPs.

Guidance and feedback by the STRO: The STRO works in partnership with financial and DNFBP sectors' supervisors to review and update the list of sector-specific red flag indicators for STR filing. These lists of red flag indicators, which are disseminated to the regulated entities via their supervisors, are also publicly available on STRO's webpage (ww.cad.gov.sg/aml-cft/suspicious-transaction-reporting-office/suspicious-transaction-reporting#3). FIs and DNFBPs can refer to the STRO's website for information on Singapore's NRA, STR forms, web links to their respective regulators' guidelines on AML/CFT regulations and standards, FAQs on STR reporting and STRO's AML/CFT handbook. The STRO also works with its law enforcement counterparts to develop crime-specific red flag indicators and guidance on STR filing. Together with the Suspicious Transaction Reporting Office (STRO), MAS and IPTO have also conducted joint outreach sessions for the financial sector to guide FIs on the reporting of suspicious transactions and the relevant ML/TF typologies. Similar initiatives have been conducted for the various DNFBP sectors.

Weighting and Conclusion

MAS and IPTO have a range of guidance covering the financial sector, although IPTO is waiting for the current rules to be tested before issuing further guidance on the most recent updates. The DNFBP sector is less well-covered, with supervisory guidance and feedback being a work in progress for most areas. STRO has issued a series of red-flag indicators and is working with MAS, IPTO and the DNFBP supervisors to conduct outreach sessions.

Recommendation 34 is rated largely compliant.

Recommendation 35 – Sanctions

Criterion 35.1 – Sanctions for Recommendation 6: Sections 3 to 6 of the Terrorism (Suppression of Financing) Act (TSOFA) set out the obligations which prohibit dealing with, and require all natural and legal persons to immediately and automatically freeze all assets belonging to a terrorist. Anyone who contravenes these provisions is liable on conviction: (1) in the case of an individual, to a fine not exceeding SGD 500 000 (approx. EUR 329 800 / USD 351 050) or to imprisonment for a term not exceeding 10 years or to both; or (2) in any other case, to a fine not exceeding SGD 1 million (approx. EUR 659 600/ USD 702 100). Even though an entity is liable, upon conviction, for a maximum fine of SGD 1 million (approx. EUR 659 600/ USD 702 100) for each offence committed, and TF offences committed by legal persons may also result in their officers/managers facing criminal sanctions for the same offences (CDSA), there are concerns that the sanctions for legal persons might not be dissuasive.

Sanctions for Recommendation 8: The Commissioner of Charities has powers to sanction violations of regulatory requirements, as set out in ss. 5, 24, 25, 25A, 26A and 26B of the Charities Act. These provisions offer a very wide range of administrative sanctions but financial penalties seem to be limited to instances of pretending to be a charity when you are not (s.43a). It is therefore unclear whether a range of financial penalties exists for other violations to allow for a set of proportionate sanctions which are also dissuasive (see also discussion regarding Recommendation 8 above). While it is likely that financial penalties can be imposed on trustees or directors/managers of charities based on common law judicial remedies, there are concerns that these are not dissuasive, as explained in detail with regard to R.25 above.

Sanctions for failure to comply with preventive measures in Recommendations 9 to 19 – financial institutions: AML/CFT requirements for FIs regulated by MAS are set out in the MAS Act and also in the MAS Notices and Directives issued under section 27B of the MAS Act. A financial institution that fails to comply with requirements set out under section 27B of the MAS Act, including requirements contained in the MAS AML/CFT Notices and Directives, would, upon conviction, be liable to a fine not exceeding SGD 1 million (approx. EUR 659 600/ USD 702 100) per offence and, in the case of a continuing offence, to a further fine of SGD 100 000 (approx. EUR 65 960 / USD 70 210) for every day during which the offence continues after conviction. MAS also has a broad range of administrative sanctions, such as the ability to issue a warning or reprimand letter, which could indicate specific deficiencies that need to be rectified, order a change in management, suspend or

withdraw a license, or issue a fine. These sanctioning powers can be found in the MAS Act and in the various FIs specific governing legislation (MAS Act: ss. 27B, 28, 28B, 41A; Banking Act: ss. 7, 20, and 57B and E; Finance Companies Act: ss. 6 and 15; Insurance Act: ss. 8 and 12; Money-changing and Remittance Businesses Act: ss. 7, 8 and 18; Financial Advisers Act: ss. 9, 13, 19, 59 and 97, Securities and Futures Act: ss. 86, 88, 95, 97, 101A, 289 and 292A; Securities and Futures Regulations 2005: s. 5; and Payment Systems [Oversight] Act: ss. 35 and 38). MAS' supervisory penalties and sanctions are guided by the MAS' internal AML/CFT Penalty Framework, which sets out the measures MAS can take against FIs.

For moneylenders, the AML/CFT requirements are set out in the PMFTR. A moneylender who is guilty of an offence under the PMFTR is liable to a fine not exceeding SGD 100 000 (approx. EUR 65 960 / USD 70 210) (PMFTR 2015: R. 11). According to s. 37(4) of the Moneylenders Act, a moneylender is also liable to lose his licence. The fine of SGD 100 000 appears to be relatively low but could, in combination with the broad range of administrative sanctions at the disposal of the Registrar and the fact that it can be imposed on a per offence basis, nevertheless provide for a sufficiently broad range of proportionate and dissuasive sanctions for breaches of AML/CFT obligations.

Sanctions for failure to comply with preventive measures in Recommendations 22-23 – DNFBPs: Overall, the financial penalty structure across the DNFBP sector is quite diverse, with different levels of sanctions applying to individual categories of DNFBPs, and it is not clear how each DNFBP sector warrants a different approach to proportionality and dissuasiveness of sanctions. For TSPs, which are regulated and supervised by MAS, the same sanctions as set out above in relation to FIs apply. These constitute a sufficiently broad range of proportionate and dissuasive sanctions. The sanctions which can be imposed on casinos and PSMDs appear to be equally proportionate and dissuasive but, as explained in detail in relation to R.28 above, there is currently no designated competent authority with sanctioning powers for PSMDs other than IPTO for pawnbrokers. The quantum of fines DNFBP supervisors can impose is tailored to each DNFBP sector's unique business environment, characteristics and activities. For instance, the maximum fine of SGD 100 000 (approx. EUR 65 960 or USD 70 210) on a per-offence basis which is applicable to public accountants and lawyers is relatively low, especially when compared with the maximum fine of SGD 1 million (approx. EUR 659 600 or USD 702 100) which can be applied to TSPs under the MAS Act. The maximum fine is SGD 25 000 (approx. EUR 16 490 or USD 17 553) in the ACRA Act for each compliance failure by CSPs. Similarly as with FIs, the DNFBPs' supervisory bodies have a range of administrative sanctions at their disposal, including imposing additional conditions on business activities; issuing written directions; revoking, suspension or refusal of renewal of registration or license.

In relation to Recommendation 20: The obligation to file STRs in section 39 of the CDSA is applicable to all natural and legal persons in Singapore. Anyone who contravenes the provisions is liable upon conviction to a fine not exceeding SGD 20 000 (approx. EUR 13 192 / USD 14 042). This penalty is attached to each instance of a failure to report. Failure to report STRs is also an illegal omission and could, depending on the circumstances, amount to an abetment of an offence of money laundering, which could result in fine of up to SGD 1 million (approx. EUR 659 600/ USD 702 100). Moreover, a

FI that fails to report a STR due to its failure or weaknesses in putting in place adequate systems and processes to detect and report STRs will have committed an offence under Section 27B of the MAS Act (i.e. breaching the relevant MAS AML/CFT Notice), and is liable to a fine of SGD 1 million (approx. EUR 659 600/ USD 702 100) per offence/breach.

In relation to Recommendation 21: The obligation against tipping-off in section 48 of the CDSA is applicable to all natural and legal persons in Singapore. Anyone who contravenes the provisions is liable upon conviction to a fine not exceeding SGD 30 000 (approx. EUR 19 788 / USD 21 063) or to imprisonment for a term not exceeding three years or to both. There are alternative sanctions for tipping off which would apply to the key stakeholders in preventing ML/TF; for example, a FI that tips off its client and is found to have committed an offence under Section 27B of the MAS Act in terms of breaching the relevant MAS AML/CFT Notice would be liable to a fine of SGD 1 million (approx. EUR 659 600/ USD 702 100) per offence/breach. The level of the fine is relatively low but for natural persons, when combined with imprisonment, it could be sufficiently dissuasive.

Criterion 35.2 – Section 28B(1) of the MAS Act imposes penalties and sanctions set out in section 27B of the MAS Act against an officer of an FI or TSP if the breach and offence committed was found to be committed with the consent or due to the neglect of the officer. In such cases, both the FI or TSP, and the officer shall be liable to be proceeded against and punished accordingly. A similar provision can be found in s.33 of the Moneylenders Act. The consent/neglect provision for natural persons is a criminal standard of proof. In terms of natural persons, DNFBP sectors such as lawyers, accountants and real estate agents comprise of professionals who are subject to the sanctions directly. Additionally, the self-regulatory bodies, including the Law Society and the Institute of Singapore Chartered Accountants (ISCA), are able to impose disciplinary sanctions on their members. As explained above in relation to R.28, directors and senior management of casino operators, who are performing licensable functions, are required to be licensed as special employees. Sanctions are imposed on casino operators and their special employees if found in breach of regulatory requirements. However, as far as CSPs are concerned, there do not appear to be direct sanctions for directors/senior managers (except refusal of registration).

Weighting and Conclusion

Although Singapore has penalties for breach of targeted financial sanctions for both natural and legal persons, there are concerns over the dissuasiveness of sanctions for legal persons. Whilst there is a range of administrative penalties available for NPOs, concerns remain over the dissuasiveness of the financial penalty regime. Singapore has a range of sanctions available for breaches of the preventative measures for FIs. Concerns remain over the level of financial penalties available for DNFBPs.

Recommendation 35 is rated partially compliant.

Recommendation 36 – International instruments

In the 3rd round MER, Singapore received a largely compliant rating for former R. 35. The deficiencies identified then were related to the addition of a purposive element to prove third party money laundering as well as a narrow definition of 'terrorist act' inconsistent with the 1999 UN Convention.

Criterion 36.1 – Singapore has ratified the Vienna Convention (on 23 October 1997), TF Convention (on 30 December 2002), Palermo Convention (on 28 August 2007), and the Merida Convention (on 6 November 2009).

Criterion 36.2 – The revision of the CDSA in 2010 has brought Singapore in line with the requirements set by the Vienna Article 3(1) (b) and (c) and Palermo Article 6(1) (see analysis under Rec. 3). Revisions to the TSOFA have similarly brought Singapore in line with the TF Convention (see analysis under Rec. 5).

Weighting and Conclusion

Recommendation 36 is rated compliant.

Recommendation 37 - Mutual legal assistance

In the 3rd round MER, Singapore received a largely compliant rating for both former Recommendation 36 and Special Recommendation V. On the basis of the ratings received, neither of the previous Recommendations were the subject of follow-up reporting by Singapore. Singapore has amended its main legislation – the Mutual Legal Assistance in Criminal Matters (MACMA) Act since the adoption of its MER.

Criterion 37.1 – Singapore has established several legal mechanisms and SOPs enabling competent authorities to rapidly provide a wide range of MLA. This legal framework is comprised of the MACMA, a number of MLA treaties (with USA, India and HK China), and membership to the ASEAN treaty on MLA. Since 2006, MLA can be provided on the basis of reciprocity even in the absence of a MLA treaty (section 16(2) of MACMA). The MACMA generally covers a broad range of MLA (sections 2, 2, 22, 26, 27, 29, 30, 33, 37, 38). Singapore laws don't require judicial proceedings to have been initiated in order for restraint to occur (Section 29(1)). In 2014, Singapore amended the MACMA to expand the scope of 'serious offences' and abolished the dual criminality requirement for certain forms of MLA.

Criterion 37.2 – The Attorney-General's Chambers (AGC) - and more specifically its International Legal Cooperation Team - is the central authority for processing MLA requests. A standard request form is available on the AGC website to facilitate and expedite the granting of MLA requests. The AGC has a set out SOPs and checklists to support the processing of MLA requests, which includes prioritization of requests-. There is a central repository and management system – Electronic Legal Management System (ELMS) - in place to track, assign and file requests, as well as to monitor requests and notify / remind case officers of any deadlines that are set.

Criterion 37.3 – The MACMA outlines twelve mandatory grounds (Section 20), these include requests of a political character and based on a person's race, religion, nationality, and four discretionary grounds to refuse assistance requests. On the basis of traditionally accepted grounds for refusal of MLA requests (e.g. requests national or public interest, double jeopardy), Singapore's grounds for refusal seem not unreasonable or unduly restrictive. For assistance requiring the use of coercive powers, Singapore will refuse assist if the foreign offence in question does not correspond to one or more of the listed offences in the MACMA Schedules (but see c.37.7), if the offence is one which is not punishable as a serious offence carrying a maximum sentence of at least four years' imprisonment under Singapore law, or the reciprocity undertaking from the requesting State is not met. A conviction is also not required before freezing/seizing assistance may be provided, same for the enforcement of foreign confiscation orders.

Criterion 37.4.

- *Sub-criterion 37.4 a)*. Since the 2013 revisions, tax offences are considered "serious" offences under the CDSA (Part XII of the Second Schedule), and as a result, they are also considered "serious offences" for MACMA purposes. In addition, "fiscal matters" being not listed under Section 20 (1) (2) (3) - which sets up grounds for refusal - it is assumed that MLA is not refused on the sole ground that the offence involves fiscal matters.

- *Sub-criterion 37.4 b)*. Assistance is not refused on the grounds of laws that impose secrecy or confidentiality requirements on FIs or DNFBPs (Section 23 (3)(b) and 23 (4)(b)). There is an exception for items subject to legal privilege (Section 23(4)(a)), and this is reserved for communications between lawyers and clients where such communications relate to the seeking of legal advice or preparations for legal proceedings.

C*riterion 37.5 –.* As a general rule, public officers in Singapore are bound by confidentiality. This is indeed required by the Official Secrets Act and the Government's internal guidelines governing the confidentiality of information received by public officers in the course of work. This extends to officers of the AGC and is applicable to the processing of MLA requests. The confidentiality of MLA requests is also reaffirmed by case law (*Re Section 22 of the Mutual Assistance in Criminal Matters Act [2009] 1SLR [R]* – where the Court of Appeal granted the AG's application for the production order of bank documents, while maintaining confidentiality of the request for assistance).

Criterion 37.6 – Dual criminality is a mandatory provision that applies to coercive measures requested under Divisions 2, 5 and 6 (these relate to taking of evidence before a Magistrate under compulsion (section 21 MACMA), issuance of production orders compelling the provision of things (section 22 MACMA), restraint and confiscation of assets (sections 29 and 30 of the MACMA) and search and seizure of things (section 33 of the MACMA). Dual criminality is not required for non-coercive forms of assistance, such as securing the voluntary attendance of a person as a witness in foreign country (section 26 MACMA), assisting in securing the custody of person in transit (section 27 MACMA), locating and identifying a person (section 37 MACMA) and service of a foreign process (section 38 MACMA) (under Divisions 3, 4, 7 and 8 of the MACMA). Dual criminality is also no longer needed for MLA pertaining to foreign tax evasion offences committed in countries that have an

Avoidance of Double Taxation Agreement, International Tax Compliance Agreement or an Exchange of Information arrangement with Singapore (sections 20(4) and 20(5) MACMA)..

Criterion 37.7 – Singapore assesses the alleged underlying criminal conduct to determine whether that conduct - had it taken place in Singapore- would constitute a serious offence or a drug dealing offence under Singaporean law (as described in Section 2(1) of the MACMA). Singapore does not place a focus on the terminology or category (label) of the offence.

Criterion 37.8 – Singapore has a range of powers and investigative techniques available in the context of MLA requests. The powers listed under the MACMA are exercised independently of a domestic investigation. The powers listed under MACMA include:

- *Sub-criterion 37.8 a).*The production, search and seizure of "*any thing*" – to include information, documents or evidence (including financial records) from financial institutions or other natural or legal persons - is covered by Section 22 and 33-36 of the MACMA.
- The power to take witness statements is only available to domestic authorities (not to foreign counterparts). However, if a trial or judicial proceeding for an offence has commenced in the requesting country, Singapore may permit MLA and compel a witness to attend before a Magistrate and give evidence (but not a suspect or the accused). Voluntary witness statements are also possible and in fact facilitated.
- *Sub-criterion 37.8 b).*Pursuant to the requirements of Article 11 of the UN 1988 Convention (see c.36.2), Singapore's law provides for a range of powers and investigative techniques, including joint investigations (domestically and with foreign counterparts). As Singapore does not have domestic provisions permitting interception of communications, this would not be provided to foreign jurisdictions.

Weighting and Conclusion

The power of domestic authorities to take a witness statement from the suspect or the accused, available to domestic authorities, is not available for use in response to a request for MLA for an accused or suspect. Interception of communications is not available domestically and therefore not available to foreign counterparts.

Recommendation 37 is rated largely compliant.

Recommendation 38 – Mutual legal assistance: freezing and confiscation

In its 3rd round MER Singapore was rated largely compliant with the requirements of this Recommendation.

Criterion 38.1 – On the basis of Sections 2, 29, 30, and the First, Second and Third Schedules to the MACMA, Singapore can identify, freeze, seize or confiscate the laundered property, proceeds of crime and instrumentalities used in money laundering, terrorism financing and predicate offences. The

legal framework does not capture instrumentalities 'intended for use' in ML, predicate offences, or TF. Singapore can undertake these actions expeditiously – within a matter of days – but only in cases involving the commission of a domestic offence where by law enforcement authorities will use their powers of investigation to identify and seize the assets. In cases that do not involve a domestic investigation, the identification and restraint of assets proceeds through MLA channels and can take two to three months.

Criterion 38.2 – On the basis of Sections 2, 29, 30, and the First, Second and Third Schedules to the MACMA, Singapore is able to provide assistance on identification, freezing, seizure, and confiscation of assets without the requirement of a conviction, including non-conviction based foreign orders. The definition of "foreign confiscation order" in MACMA does not distinguish between conviction and non-conviction based orders. In fact, Singapore has enforced non-conviction based foreign orders in two past cases.

Criterion 38.3.

- *Sub-criterion 38.3 a)*. Seizure and confiscation actions are coordinated by the AGC, as the central authority for mutual assistance in Singapore – by way of face-to-face meetings, video and tele-conference. Singapore's law enforcement agencies also coordinate with their counterparts in other countries in relation to seizure and confiscation actions.
- *Sub-criterion 38.3 b)*. The Third Schedule to the MACMA (Paragraphs 7 to 11) sets out rules concerning the management and disposal of frozen, seized and confiscated assets - pursuant to an MLA request. On the basis of Section 7(7) of the Third Schedule, MACMA, the High Court may appoint a Public Trustee as receiver in respect of restrained property and issue directions as to the management of that property. This provision is mirrored by Section 16(6) of the CDSA.

Criterion 38.4 – Singapore's legal framework allows the sharing of confiscated or forfeited assets with any country, also when it is the direct or indirect result of a co-ordinated law enforcement action [Paragraphs 10 and 11 of the 3rd Schedule to the MACMA]. Singapore uses a three-tiered asset-sharing framework: sharing ratios are determined by the level of contribution (assistance, resources) to the recovery process, but also on the basis of negotiated divisions on a case-by-case basis.

Weighting and Conclusion

The definition of "instrumentality order" does not include instrumentalities "intended for use" in money laundering, predicate offences, or terrorism financing. There can be significant delays in the restraint of assets, in particular cases where domestic enforcement powers (CPC) cannot be used to restrain the assets.

Recommendation 38 is rated largely compliant.

Recommendation 39 – Extradition

In its 3rd round MER, Singapore was rated compliant with the requirements of this Recommendation.

Criterion 39.1 – a) ML and TF are both extraditable offences in Singapore. ML is listed in First Schedule (No 26) to the Extradition Act [EA]. For ML, the legal basis for extradition extends only to the 40 declared Commonwealth countries of the London Scheme and bilateral treaty partners (United States; Germany; Hong Kong, China). An agreement was signed with Indonesia in 2007, but has yet to enter into force. Another higher risk country noted that its "list-based" treaty is outdated, too limited on the number of offences for which extradition may be granted, and does not cover ML. Extradition is possible for TF offences (Section 33(1) TSOFA), as well as with all countries having ratified the FT Convention. In addition, terrorist acts (e.g. murder, malicious and wilfully wounding) are covered by the general list of offences in the First Schedule - EA. Special expedited extradition arrangements exist between Singapore, Brunei Darussalam and Malaysia. b) Sections 11-13, 25, 27-28 of the EA outline clear timelines for the processing of extradition requests – to ensure a handling without undue delay. These timelines apply to all proceedings, including ML, TF, and predicate offences. c) There are no unreasonable or unduly restrictive conditions on extradition. The EA provides a number of universally accepted "extradition restrictions" (e.g. the restrictions related to offences of a political character (Section 7, 21) and prejudice on account of race, religion, nationality or political opinions, etc. (Section 8, 22).

Criterion 39.2 – a) Singapore can extradite its own nationals. The Extradition Act does not draw any distinction based on nationality. It has also been confirmed by case law (*Fatimah bte Kumin Lim v Attorney-General [2014] 1 SLR 547*). b) However, at the request of its treaty partners, Singapore has agreed to provide for nationality as a ground for refusal in its extradition treaties with Hong Kong SAR and Germany**.**

Criterion 39.3 – Dual criminality is a requirement for extradition in Singapore. Singapore uses a conduct-based approach (Section 2(1) of the Extradition Act), by analysing the underlying conduct as a whole. Technical differences in the manner in which another country categorises or denominates the offence accordingly does not pose an impediment to the provision of extradition.

Criterion 39.4 – The Central Authority of Singapore can process foreign requests for provisional arrests in urgent situations (real risk that a fugitive is likely to flee Singapore or commit other offences) pending the formal submission of an extradition request via diplomatic channels. Sections 10(1)(b) and 24(1)(b) of the Extradition Act outline the process for urgent situations. The Extradition Act also provides a number of simplified processes for Malaysia and Brunei Darussalam (Section 121 CPC).

Weighting and Conclusion

Singapore needs to improve its legal basis for extradition in ML cases, in particular by expanding the number of countries covered to include countries that are a greater risk for ML.

Recommendation 39 is rated largely compliant.

Recommendation 40 – Other forms of international cooperation

In its 3rd round MER, Singapore received a compliant rating for Recommendation 40. The Recommendation was significantly modified in 2012.

Criterion 40.1 – Singaporean LEAs and competent authorities including the Singapore Police Force (CAD and STRO), Customs, IRAS, and ICA can provide a range of information to their foreign counterpart authorities in relation to ML, TF and predicate offences. Information can be shared both spontaneously and upon request.

Part VC of the MAS Act provides MAS with the legal basis for AML/CFT supervisory cooperation. MAS is able to share information spontaneously (s. 30ZF), transmit any information in its possession (s. 30ZA), obtain information from FIs and domestic authorities (s. 30ZA), and allow home AML/CFT supervisors to inspect FIs in Singapore (s. 30ZG). Part X of the Securities and Futures Act and Part IIIA of the Insurance Act provide MAS the legal basis to cooperate in accordance with Singapore's obligations under the IOSCO MMOU and IAIS MMOU respectively.

While there is no specific lawful basis for IPTO to exchange information and cooperating with its counterparts, there is no specific legal prohibition either preventing IPTO to do this, where necessary. IPTO has not received any request from a foreign counterpart for assistance to address ML/TF risks thus far. This appears to be consistent with Singapore's understanding of the domestic nature of the industry and that group supervision is not required for the moneylenders (non-Core Principles financial institutions). However Singapore reports that IPTO is prepared to provide assistance to its foreign counterparts (e.g. sharing of information on moneylenders in Singapore or facilitating the conduct of inquiries in Singapore) should the need arise.

Criterion 40.2.

- *Sub-criterion 40.2 a)*. Competent authorities in Singapore have a lawful basis for providing cooperation. (STRO: Section 41 of the CDSA; Financial Supervisors [Part VC of the MAS Act – see c.40.1 – no specific lawful basis for IPTO]; Customs: Section 31 of the Regulation of Imports and Exports Act (RIEA; IRAS: Sections 6(4)(b), 6(4A); and part A of the Income Tax Act; ICA: Section 36B of the Immigration Act and 55 of the Passports Act). While there is no lawful basis for Customs to share information collected under the Customs Act with international partners (section 89), Singapore all information collected under that Act is also collected under the RIEA. There is no lawful basis for the LEAs (SPF, CNB, and CPIB) to cooperate (under legislation or Singaporean case law).
- *Sub-criterion 40.2 b)*. Nothing prevents competent authorities from using the most efficient means to cooperate.
- *Sub-criterion 40.2 c)*. All competent authorities use clear and secure gateways, or have mechanism or channels in place. STRO in particular uses Egmont's secure web as the primary channel for international exchange. STRO has also pre-agreed contact points and working arrangements with the foreign counterparts to send and receive information in a confidential

manner. LEAs also use established channels of cooperation such as INTERPOL, liaison channels, and also through inter-agency meetings and their SOPs limit communication to clear and secure pathway. For special enforcement operations initiated under WCO's Regional Intelligence Liaison Office (RILO), Singapore Customs exchanges the information through WCO's Customs Enforcement Network Communication (CENcomm) platform. ICA has an internal framework to guide officers when processing requests from third parties for ICA-owned information.

- *Sub-criterion 40.2 d)*. Competent authorities have processes for prioritising and executing requests. All of them have internal guidelines, procedures or instructions in relation the handling and prioritisation of requests (STRO, MAS, LEAs, Customs, IRAS, ICA).

- *Sub-criterion 40.2 e)*. Competent authorities have clear processes for safeguarding the information received. (STRO and LEAs: section 56(1) of the CDSA; MAS: section 14 of the MAS Act and MAS's operating procedures LEAs have SOPs in place which include confidentiality provisions. Customs has an internal Customs Departmental Orders, IRAS deals with the EOI framework and is also supported by section 6 of the Income Tax Act; and ICA: Section 36C of the Immigration Act, Regulation 20(f) of the National Registration Regulations; and Section 56(2) of the Passports Act.) Section 5 of the Official Secrets Act also applies to all public servants and section 3 of the Statutory Bodies and Government Companies (Protection of Secrecy) Act places secrecy obligations on members of MAS and IRAS.

Criterion 40.3 – STRO requires an MOU or letter of undertaking pursuant to section 41 of the CDSA and has signed 31 MOUs and two letters of undertaking. LEAs, Customs, ICA and MAS (as long as the conditions and requirements under section 30Z of the MAS Act are fulfilled) can all cooperate with their respective foreign counterparts without a need for MOUs. If MOUs are required by the foreign counterparts, competent authorities can also conclude bilateral and multilateral agreements (and protocols) as soon as possible. Tax-related cooperation is based on the OECD Model Tax Convention and the Model tax Information Exchange Agreement.

Criterion 40.4 – Competent authorities in Singapore can provide feedback through direct response to a feedback form or through bilateral meetings with their counterparts. There is a general practice at government level for agencies to respond within 7 working days on queries posed to it. A number of operating procedures are in place within STRO and MAS to comply with this requirement. The LEA SOPs do not reference this criterion.

Criterion 40.5 – Competent authorities (STRO: Section 41 of the CDSA; Financial Supervisors [Part VC of the MAS Act]; Customs: IRAS: Sections 6(4)(b), 6(4A); and part A of the Income Tax Act; ICA: Section 36B of the Immigration Act and 55 of the Passports Act) in Singapore do not prohibit or place unreasonable or unduly restrictive conditions on information exchange or assistance with foreign counterparts - as long as the request is within its scope of purview. The LEA SOPs only require that the nature and the purpose of the request should be specific and bona fide. Section 31 of the REIA however places very restrictive requirements on the ability to share information under that Act and may unreasonably inhibit Customs from assisting foreign counterparts. They similarly do not refuse requests for assistance on any of the four grounds listed in this criterion. Information sharing in

Singapore can be however conditioned to the requirement that foreign requests be clear, relevant and proportionate. The requesting party must also ensure the confidentiality and the proper use of the information shared.

Criterion 40.6 – Competent authorities in Singapore have the necessary confidentiality safeguards set out in standard operating procedures to ensure that information received is used only for the intended purpose, and by the authorities for whom the information was sought. If the information received is to be used for other purposes, prior authorisation from the requested authorities will be sought. For instance, STRO has dedicated guidelines and controls in place and also applies the Egmont Group's principles with regards to sharing of information. The LEAs will only share information with a trustworthy counterpart which is able to safeguard data confidentiality and CNB applies a standard confidentiality clause to all information it shares. MAS relies on its Procedures for Cooperation with Foreign AML/CFT Authorities for AML/CFT Supervisory Purposes'. When ordered by Court to disseminate the information received, MAS will notify the foreign counterpart in a timely manner to the extent permitted by law.

Criterion 40.7 – CAD's SOP for parallel investigations with foreign counterparts provides for the protection of confidentiality of information received from foreign partners. The SOPs for the other LEAs (e.g. CPIB, CNB) do not provide for any such reference. If a foreign partner cannot safeguard information provided to it by the LEAs, the SOPs advise the LEAs to refuse the request. For IRAS, the information received by EOI team is kept in a secured depository which can be accessed only by its staff for processing and reviewing.

Criterion 40.8 – Competent authorities in Singapore can conduct inquiries on behalf of their foreign counterparts and exchange with their foreign counterparts all information that would be obtainable by them if inquiries were being carried out domestically: STRO pursuant to Section 41 of the CDSA and by using the Egmont Group's framework; MAS pursuant to section 30ZA of the MAS Act; the LEA SOPs cover common types of assistance such as requests for information and interviewing witnesses, with the exception of witness statements from the suspect or the accused. Customs can assist its foreign counterparts by seeking the *trader's* voluntary cooperation when requesting countries seek commercial documents or request for an interview with local traders [section 89 of the Customs Act and Section 31 of the RIEA]; IRAS (EOI Team) is enabled to share the information relevant for the enforcement of Singapore's tax laws with foreign counterparts (Section 105F of the Income Tax Act).

Exchange of information between FIUs

Criterion 40.9 – Pursuant to Section 41 of the CDSA, STRO requires an MOU or LOU for exchanging financial intelligence contained in its database with its foreign counterparts. Under the LOU, the foreign FIU provides undertakings to protect confidentiality, ensures reciprocity and that the information will not be used as evidence in any proceedings (Section 41(2)). STRO can exchange intelligence regardless of its nature (administrative, law enforcement, judicial or other). The information requested needs to be relevant to the investigation conducted by the foreign authority - on issues related to ML, predicate offences and TF. As of November 2015, STRO has concluded 31 Memoranda of Understanding (MOUs) and 2 Letters of Undertaking (LOU) with its counterparts, a list which does not include several countries in the region. Singapore has invited 12 additional

countries to sign an LOU, in some cases due to the presence of financial intelligence. An MOU or LOU is required even for Egmont members despite the Egmont Charter and the "Principles of Exchange" which provide a platform for exchange among Egmont members without an MOU.

Criterion 40.10 – Pursuant to its internal guidelines [*Guidelines (STRO) on Outgoing request for assistance from STRO to foreign FIUs]*, STRO provides – upon request- feedback to its foreign counterparts on the use and usefulness of the information provided. As per these guidelines, the feedback must be provided within 2 weeks. Spontaneous feedback is also possible

Criterion 40.11 – STRO can communicate, directly or indirectly, all information -accessible or obtainable- with its foreign counterparts (section 41). This information would include information disclosed, given, forwarded or submitted to the STRO (under Sections 3A(3), 39(1), 48C(5), 48D and 48E(5), 48J(1) of the CDSA). It also includes information reported to STRO under the Casino Control Act.

Exchange of information between financial supervisors

IPTO has no specific legal basis for co-operation with its foreign counterparts. This has an impact on c.40.12 - 40.16.

Criterion 40.12 – MAS has an appropriate legal basis for co-operation with its foreign counterparts (MAS Act: Part VC; Securities and Futures Act: Part X; Insurance Act: Part IIIA).

Criterion 40.13 – MAS has broad powers to obtain information domestically, including information held by financial institutions, and exchanges it with foreign supervisors in a manner proportionate to their respective needs (MAS Act: ss. 30ZA(1), 30Z and 30Z(1)).

Criterion 40.14 – When relevant for AML/CFT purposes, MAS is in a position to exchange: (i) regulatory information; (ii) prudential information; and (iii) AML/CFT information (see also c.40.8).

Criterion 40.15 – MAS has broad powers to conduct inquiries on behalf of foreign counterparts and, as appropriate, to authorise or facilitate their ability to conduct their own inquiries in Singapore, in order to facilitate effective group supervision.

Criterion 40.16 – MAS is authorised to disseminate information exchanged only with the prior authorisation of the requested financial supervisor, and has controls and safeguards in place to ensure that information is used appropriately

Exchange of information between law enforcement agencies

Criterion 40.17 – Although there is no lawful basis for law enforcement authorities in Singapore to exchange domestically available information with their foreign counterparts (see criterion 40.2(a) above), this has and can be done in practice in line with the LEA's SOPs on informal cooperation requests. [. This cooperation covers the exchange of information such as company registration records, land ownership records, travel records. Information can also be shared through engagement in a joint investigation with foreign counterparts.

Criterion 40.18 – LEAs can use their powers to conduct inquiries (including investigative powers) and obtain information on behalf of their foreign counterparts as outlined in their SOPs on informal cooperation requests. This is however conditioned on the sending of a *bona fide* request, containing reliable and sufficient information on the foreign predicate offence, in connection to a possible ML offence in Singapore. If suspicion of ML is confirmed, Singaporean LAEs will initiate a domestic ML investigation and use their powers to obtain information. That information can be shared with their foreign counterparts, *subject to domestic legislative and operational framework* (e.g. requests for banking records would require an MLA requests).

Criterion 40.19 – As outlined in the SOPs, LEAs in Singapore can form joint investigative teams and establish bilateral or multilateral agreements where required and all agencies have made use of joint investigative teams.

Exchange of information between non-counterparts

Criterion 40.20 – Information can be exchanged indirectly with foreign authorities via the foreign authorities' counterpart in Singapore. STRO has developed SOPs, including Guidelines on Outgoing request for assistance from STRO to foreign FIUs and Guidelines (STRO) on International Request for Third Party dissemination. Section 30ZC of the MAS Act allows MAS to share information, upon request, with other domestic authorities for their investigation, enforcement action or supervisory action. Section 30ZF also enables MAS to spontaneously provide such information to a domestic authority. The LEAs provided case examples where information was exchanged between non-counterparts.

Weighting and Conclusion

STRO is limited in the number of foreign FIUs with which it can exchange information due to the low number of MOUs and LOUs. In addition, STRO is unable to access and share trade information and some tax information. Customs have some restrictive provisions on the exchange of information.

Recommendation 40 is rated largely compliant.

Summary of Technical Compliance – Key Deficiencies

TABLE OF COMPLIANCE WITH FATF RECOMMENDATIONS

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
1. Assessing risks & applying a risk-based approach	LC	• The risk-based approach is not evenly applied and is missing in some high risk areas such as in relation to transnational money laundering, illicit financial flows, international cooperation, and cash couriers.
2. National cooperation and coordination	C	The Recommendation is fully met.
3. Money laundering offence	LC	• The criminal sanction available for legal persons convicted of the ML offence is too low to be sufficiently dissuasive.
4. Confiscation and provisional measures	C	The Recommendation is fully met.
5. Terrorist financing offence	LC	• The criminal sanctions available for legal persons convicted of the TF offence and persons convicted of TF ancillary offences are too low to be sufficiently dissuasive.
6. Targeted financial sanctions related to terrorism & TF	LC	• Competent authorities only indirectly receive reports on assets frozen or actions taken in compliance with the prohibition requirements of relevant UNSCRs, including attempted transactions. • There are no measures which protect the rights of bona fide third parties acting in good faith when freezing terrorist assets. • Not all PSMDs are subject to supervision by the competent authorities. • There are concerns regarding the sanctions for legal persons not being sufficiently dissuasive.
7. Targeted financial sanctions related to proliferation	LC	There is no provision in accordance with the exemptions under the UNSCRs and the implementation is left to the discretion of the authorities.
8. Non-profit organisations	LC	• There is no outreach to NPOs specific to terrorist financing issues. • While there are monitoring provisions in place for all NPOs, none of the monitoring relates specifically to terrorist financing. • There is a range of administrative sanctions available for NPOs but concerns remain over the dissuasiveness of the financial penalty regime. • There is no clear central contact point with respect to NPOs to respond to international requests for information regarding particular NPOs suspected of TF or other forms of terrorist support.
9. Financial institution secrecy laws	C	The Recommendation is fully met.
10. Customer due diligence	C	The Recommendation is fully met.
11. Record keeping	C	The Recommendation is fully met.
12. Politically exposed persons	C	The Recommendation is fully met.
13. Correspondent banking	C	The Recommendation is fully met.

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
14. Money or value transfer services	LC	The penalty imposed on non-license MVTS is relatively low.
15. New technologies	C	The Recommendation is fully met.
16. Wire transfers	C	The Recommendation is fully met.
17. Reliance on third parties	C	The Recommendation is fully met.
18. Internal controls and foreign branches and subsidiaries	C	The Recommendation is fully met.
19. Higher-risk countries	LC	Concerns exist as to whether the required enhanced CDD provide for a sufficient wide range of measures that are proportionate to the risk in all instances.
20. Reporting of suspicious transaction	LC	The STR reporting requirement is not sufficiently clear with regard to the prompt reporting of STRs.
21. Tipping-off and confidentiality	C	The Recommendation is fully met.
22. DNFBPs: Customer due diligence	PC	• PSMDs without a pawnbroker's licence and accountants are not subject to enforceable CDD obligations. • The record-keeping obligation for real estate agents is not provided by law.
23. DNFBPs: Other measures	PC	• PSMDs without a pawnbroker's licence are not subject to obligations regarding internal controls, measures against higher-risk countries and tipping-off. • Accountants' obligations regarding internal controls, measures against higher-risk countries and tipping-off are not enforceable. • In relation to high-risk countries, provisions in law or enforceable means do not necessarily provide for a wide range of measures proportionate to the risk.
24. Transparency and beneficial ownership of legal persons	PC	• Singapore did not assess the ML and TF risks associated with all types of legal persons as part of its NRA exercise. • There are gaps in foreign registered company information and residency requirements as well as gaps in the length and time that relevant information must be kept. • While Singapore permits nominee shareholders and nominee directors, Singapore law does not generally require disclosure to third parties of this status.
25. Transparency and beneficial ownership of legal arrangements	PC	Singapore law does not go far enough to impose enforceable obligations on trustees (including professional trustees) to collect beneficial ownership information relating to a trust beyond the immediate beneficiary.
26. Regulation and supervision of financial institutions	LC	• There are currently no fit and proper requirements for SVF holders. • There is currently no legal requirement for credit card / charge card licensees operating in Singapore to give MAS prior notice if there are changes to their directors, senior management and controllers. • While moneylenders are regulated by the Registrar (IPTO) and are subject to AML/CFT requirements, the monitoring of the implementation of these requirements is based almost solely on volumes rather than on ML/TF risk. • For moneylenders, the impact of ML/TF risk on the frequency and

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
		extent of inspections to be carried out is not clearly established. • While the Registrar (IPTO) regularly reviews the risk profiles of the moneylenders it supervises, the extent to which ML/TF risk influences this assessment is not established.
27. Powers of supervisors	C	The Recommendation is fully met.
28. Regulation and supervision of DNFBPs	PC	• PSMDs without pawnbroker's license are not subject to regulation and supervision and this poses a threat to the overall AML/CFT system, especially taking into account the potential magnitude of the sector. • It is unclear and premature to conclude: o whether sanctions applied to individual non-compliant DNFB sectors are proportionate and dissuasive enough; and o whether the supervision is on a risk-sensitive basis.
29. Financial intelligence units	C	The Recommendation is fully met.
30. Responsibilities of law enforcement and investigative authorities	C	The Recommendation is fully met.
31. Powers of law enforcement and investigative authorities	C	The Recommendation is fully met.
32. Cash couriers	C	The Recommendation is fully met.
33. Statistics	LC	There are gaps in relation to the statistics regarding the total amounts of seizures/confiscations, and the number of cases in which seizures and confiscation occurred.
34. Guidance and feedback	LC	For most of the DNFBPs, guidance and feedback is an area of work in progress and is not yet fully developed.
35. Sanctions	PC	• With regard to targeted financial sanctions, there are concerns regarding the sanctions for legal persons not being sufficiently dissuasive. • While there is a range of administrative sanctions available for NPOs, concerns remain over the dissuasiveness of the financial penalty regime. • There are concerns regarding the level of financial penalties available for DNFBPs.
36. International instruments	C	The Recommendation is fully met.
37. Mutual legal assistance	LC	• The power of domestic authorities to take a witness statement from the suspect or the accused, available to domestic authorities, is not available for use in response to a request for MLA for an accused or suspect. • Interception of communications is not available domestically and therefore not available to foreign counterparts.

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
38. Mutual legal assistance: freezing and confiscation	LC	• The definition of "instrumentality order" does not include instrumentalities "intended for use" in money laundering, predicate offences, or terrorism financing. • There can be significant delays in the restraint of assets, in particular cases where domestic enforcement powers (CPC) cannot be used to restrain the assets.
39. Extradition	LC	There is a need for Singapore to improve its legal basis for extradition in ML cases, in particular by expanding the number of countries covered to include countries that are a greater risk for ML.
40. Other forms of international cooperation	LC	• STRO is limited in the number of foreign FIUs with which it can exchange information due to the low number of MOUs and LOUs. • STRO is unable to access and share trade information and some tax information. • Customs have some restrictive provisions on the exchange of information.

TABLE OF ACRONYMS

ABS	Association of Banks in Singapore
ACRA	Accounting and Corporate Regulatory Authority
ACU	Asian Currency Unit
AGC	Attorney-General's Chambers
AGM	Annual General Meeting
AMLA	Administration of Muslim Law Act
APEC	Asia-Pacific Economic Cooperation
ASEAN	Association of Southeast Asian Nations
ASEM	Asia-Europe Meeting
AT	Approved Trustees
BA	Banking Act
CA	Companies Act
CAD	Commercial Affairs Department
CBNI	Cash or Bearer Negotiable Instrument
CBT	Criminal Breach of Trust
CC-PMLTFR	Casino Control (Prevention of Money Laundering and Terrorism Financing) Regulations 2009
CCA	Casino Control Act
CCP	Central Counterparty
CDP	The Central Depository
CDSA	Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act
CEA	Council for Estate Agencies
CF	Corporate Finance
CFTB	Counter Financing of Terrorism Branch, Commercial Affairs Department
CID	Criminal Investigation Department, Singapore Police Force

CIS	Collective Investment Schemes
CLG	Company Limited by Guarantee
CMI	Capital Markets Intermediaries
CMR	Cash Movement Report
CNB	Central Narcotics Bureau
COC	Commissioner of Charities
COH	Controller of Housing
CPC	Criminal Procedure Code
CPIB	Corrupt Practices Investigation Bureau
CRA	Casino Regulatory Authority
CSD	Central Securities Depository
CT	Counter-Terrorism
CTR	Cash Transaction Report
CU	Charities Unit
CUSTOMS	Singapore Customs
DLI	Direct Life Insurers
EAA	Estate Agents Act
EOI	Exchange of Information
EP 200	Ethics Pronouncement 200
FA	Financial Advisers
FAA	Financial Advisers Act
FCA	Finance Companies Act
FIG	Financial Investigation Group, Commercial Affairs Department
FHC	Financial Holding Company
FMC	Fund Management Company
HDCLA	Housing Developers (Control & Licensing) Act

IA	Insurance Act
IAC	Inter-Agency Committee
IB	Insurance Broker
ICA	Immigration and Checkpoints Authority
IMA	International Market Agent
IMC-CT	Inter-Ministry Committee on Counter Terrorism
IMC-EC	Inter-Ministry Committee for Export Control
IMC-TD	Inter-Ministry Committee on Terrorist Designation
ING	Intelligence Group, Commercial Affairs Department
INTERPOL	International Criminal Police Organisation
IPC	Institutions of a Public Character
IPTO	Insolvency and Public Trustee's Office
IRAS	Inland Revenue Authority of Singapore
IR	Integrated Resort
ISCA	Institute of Singapore Chartered Accountants
ISD	Internal Security Department
ISP	Industry Sound Practices
JI	Jemaah Islamiyah
LawSoc	Law Society of Singapore
LEA	Law Enforcement Authority
LLP	Limited Liability Partnership
LOU	Letter of Undertaking
LP	Limited Partnership
LPA	Legal Profession Act
LP-PMLFTR	Legal Profession (Prevention of Money Laundering and Financing of Terrorism) Rules 2015

LTC	Licensed Trust Company
MACMA	Mutual Assistance in Criminal Matters Act
MAS	Monetary Authority of Singapore
MB	Merchant Banks
MCCY	Ministry of Community, Culture and Youth
MCRB	Money-changing and Remittance Businesses
MDA	Misuse of Drugs Act
MFA	Ministry of Foreign Affairs
MHA	Ministry of Home Affairs
MinLaw	Ministry of Law
MLA	Mutual Legal Assistance
MMB	Mosque Management Board
MMOU	Multilateral Memorandum of Understanding
MOF	Ministry of Finance
MOM	Ministry of Manpower
MPA	Maritime and Port Authority of Singapore
MSF	Ministry of Social and Family Development
MTI	Ministry of Trade and Industry
MUIS	Majlis Ugama Islam Singapura
OSA	Official Secrets Act
OTP	Option to Purchase
PBIG	Private Banking Industry Group
PBA	Pawnbrokers Act 2015
PBR	Pawnbrokers Rules 2015
PCA	Prevention of Corruption Act
PCG	Police Coast Guard

PCR	Professional Conduct Rules
PMFTR	Moneylenders (Prevention of Money Laundering and Financing of Terrorism) Rules 2009
PSMD	Precious Stones and Metals Dealer
PSOA	Payment Systems (Oversight) Act
QFB	Qualifying Full Bank
RIEA	Regulations of Imports and Exports Act
ROS	Registry of Societies
S&PA	Sale and Purchase Agreement
SAICSA	Singapore Association of the Institute of Chartered Secretaries and Administrators
SAP	Statement of Auditing Practice
SCPA	Sale of Commercial Properties Act
SFA	Securities and Futures Act
SGX	Singapore Exchange
SLA	Singapore Land Authority
SME	Small and Medium-Sized Enterprises
SOP	Standard Operating Procedure
SPF	Singapore Police Force
SSS	Securities Settlement System
STA	Singapore Trustees Association
STRO	Suspicious Transaction Reporting Office
SVF	Stored Value Facility
TCA	Trust Companies Act
TFC	Terrorist Financing Convention
TSOFA	Terrorism (Suppression of Financing) Act
UML	Unlicensed Moneylending

URA	Urban Redevelopment Authority
WCO	World Customs Organisation

[1] *Acronyms already defined in the FATF 40 Recommendations are not included into this Glossary.*

www.fatf-gafi.org | www.apgml.org

September 2016

Anti-money laundering and counter-terrorist financing measures - Singapore
Fourth Round Mutual Evaluation Report

In this report: a summary of the anti-money laundering (AML) / counter-terrorist financing (CTF) measures in place in Singapore as at the time of the on-site visit on 17 November - 3 December 2015. The report analyses the level of effectiveness of Singapore's AML/CTF system, the level of compliance with the FATF 40 Recommendations and provides recommendations on how their AML/CFT system could be strengthened.