Mutual Evaluation of Singapore

Anti-money laundering and countering the financing of terrorism and proliferation financing measures

May 2026

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 (CFT) standard.

For more information about the FATF, please visit www.fatf-gafi.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.

How to read this mutual evaluation report

The Financial Action Task Force (FATF) has revised its assessment methodology to place an even greater focus on effectiveness, to ensure that countries are implementing and making use of the laws, regulations and policies that are being passed, as well as a greater emphasis on the major risks and context. This round of mutual evaluations is operating on a six-year cycle, significantly shorter than earlier rounds, and includes time-bound Key Recommended Actions roadmaps for countries that need to improve in key areas.

Effectiveness has been assessed according to the 11 immediate outcomes that an effective anti-money laundering/countering the financing of terrorism/countering proliferation financing (AML/CFT/CPF) framework should be able to deliver. The extent to which a country is taking effective action in this area is reflected in ratings that range from low to high level of effectiveness (see Chapters 2 – 11).

Technical compliance has been re-assessed in line with the FATF Recommendations where: (i) the country has made legal, regulatory or operational framework changes since its last mutual evaluation or follow-up report with technical compliance re-ratings and (ii) there has been a change in the FATF Standards for which the country has not previously been assessed. Where technical compliance has been reassessed, the relevant section is clearly indicated in the Technical Compliance Annex. Where a Recommendation has not been re-assessed, the previous assessment is included under a grey heading (see Annex A. Technical Compliance).

A glossary of key terms is available at the end of the report.

Citing reference:

FATF (2026), *Mutual Evaluation Report of Singapore*, FATF, Paris and APG, Sydney, www.fatf-gafi.org/content/fatf-gafi/en/publications/Mutualevaluations/mer-singapore-2026.html

Table of contents

Executive summary

1. This report provides a summary of the anti-money laundering and counter-terrorist financing (AML/CFT) measures in place in Singapore as at the date of the end of the on-site visit (18 July 2025). This report analyses the level of compliance with the FATF 40 Recommendations and the effectiveness of Singapore's AML/CFT system and provides recommendations on how this system could be improved.

Key Findings

a) Singapore is a globally significant International Financial Centre (IFC) with low levels of violent crime and high levels of wealth and trust in institutions. These characteristics have led Singapore to face unique money laundering/terrorist financing/proliferation financing (ML/TF/PF) risks, in particular ML and PF risks that are disproportionate to their violent crime rate. Political stability, a mature financial sector and connectivity offer a platform to launder the proceeds from predicate offences occurring in foreign jurisdictions, with Singapore acting as a passthrough/integration point for illicit flows. The threat actors attempting to misuse Singapore's financial system generally sit outside of Singapore's borders.

b) High-profile cases like the 3 billion dollar Case in 2023 (3B$ Case) underscore Singapore's attractiveness to criminals, and the scope and scale with which they attempt to misuse Singapore's system. In this case, Singapore used financial intelligence to detect, investigate and prosecute a complex case where foreign persons brought billions derived from foreign remote gambling offences, representing one of the world's largest crackdowns on money laundering in 2023. This case highlights the quality of Singapore's law enforcement. As a result of the 3B$ case, Singapore exemplified its high-level political commitment to preventing the misuse of its financial system and set up an inter-ministerial committee to review and improve Singapore's AML/CFT/CPF system. This committee, and the measures it has put in place, including innovative amendments to AML/CFT legislation and new information/data sharing mechanisms, represent the clearest manifestation of Singapore's ongoing and active implementation of incremental and unique measures to take on those attempting to misuse Singapore's financial system.

c) Singapore has a coordinated structure implementing its dynamic risk assessment and mitigation approach that it uses to develop an understanding of ML/TF risks and quickly react to environmental changes. The dynamic risk assessment process structure is ultimately accountable to the AML/CFT Steering Committee (AML/CFT SC). This Committee is made up of the most senior decision makers from relevant agencies who are empowered to take decisions to meet the identified risks. Singapore's competent authorities are well-resourced in relation to AML/CFT/CPF measures. There are numerous positives to this institutional set-up, allowing Singapore to have a reasonably sound understanding of its ML/TF risks. However, the approach can be enhanced in terms of the robustness of structures that take a more holistic view of risks. Singapore considers individual risks identified by participants and does not produce prioritised mitigation measures proportionate to risks, particularly for lower risk situations. This risk assessment and mitigation process is supported by policy and operational co-operation and co-ordination that are the strength of Singapore's AML/CFT/CPF regime and are likely some of the best in the world. This coordinated and cooperative regime drives collective outcomes but does

so without clear documentation of tracking of mitigation measures and key performance indicators.

d) Since its last Mutual Evaluation Report (MER), Singapore has made significant investment in technology, data integration and process automation. This investment has seen significant increases in the production of financial information that can be accessed directly or automatically disseminated to the law enforcement agencies (LEAs) and other competent authorities, and financial intelligence that can and has been used to identify and investigate financial crimes and pursue criminal assets. Financial intelligence is produced reasonably in line with Singapore's risks. Financial intelligence from Suspicious Transaction Reporting Office (STRO) (Singapore's FIU) is being used to initiate and support investigations into ML, associated predicate offences and TF to a good extent but more could be done to leverage financial intelligence for higher risk offences (except fraud). Competent authorities regularly use financial information to support investigations, develop evidence, identify and trace criminal proceeds or instrumentalities, including high-value and significant ML cases, but do not use financial intelligence to support investigations to the same degree.

e) Singapore has chosen to actively pursue all offences affecting its citizens within its borders, where it has the greatest influence to take criminal justice measures, but this approach has limited impact on pursuing the complex transnational organisations that are targeting Singapore's citizens. Singapore commenced a very significant amount of money laundering (over 11 000 in five years) and terrorist financing investigations (126 in five years). The high number of ML investigations is almost entirely in response to Singaporean victim complaints from cyber-enabled fraud (CEF), Singapore's highest risk, which are investigated as standalone money laundering cases. Consequently, the average ML case in Singapore is smaller, befitting lower penalties and where there are limited assets to recover. Where they have pursued more significant and complex cases, Singapore's LEAs have shown adeptness at bringing cases to successful conclusions, including recovering significant criminal assets. However, penalties are low for ML, which undermines dissuasiveness, but more appropriate for TF. To secure these results, Singapore engages in strong international co-operation with counterparts, which is important in the context of the foreign risks faced by Singapore. Singapore generally provides effective international co-operation but there can be delays, and Singapore could make better use of formal co-operation channels.

f) Singapore has a number of contextual factors and attributes which make it one of the jurisdictions most vulnerable to PF: its geographical position, and its status as an IFC and a hub for trade, transport, maritime and virtual assets. While Singapore has a strong legal framework to implement PF targeted financial sanctions and has in place a comprehensive ban on trade with the DPRK, there are limited risk mitigation measures considering Singapore's exposure. Singapore conducted a PF national risk assessment (NRA) in 2024 but like the ML and TF NRAs, there were limited risk-based mitigation measures identified within the PF NRA. Representation offices of foreign flag States operating in Singapore have a very low level of understanding of their obligations. Reflecting a better understanding, reporting entities have filed a very significant number of PF-related suspicious transaction reports (STRs) with STRO. Singapore has successfully prosecuted 22 natural persons and eight legal persons for breaches of the UN (Sanctions – DPRK) Regulations and other export control regulations. Penalties for these breaches were relatively low.

g) Supervisors demonstrate a solid understanding of risks across its mature financial and DNFBP sectors, and in its emerging digital payment token service provider (DPTSP) sector, at the sectoral level. The Monetary Authority of Singapore (MAS) supervises the most material sectors in Singapore, notably most FIs, DPTSPs and Licensed Trust Companies (LTCs). MAS establishes an institutional-level risk understanding for the financial and DPTSP sectors through three

separate components and the day-to-day consultation and co-ordination between its AML specialist department and other prudential supervisors. This process is not thoroughly systematised and documented and does not result in residual risk ratings on an institutional level to inform strategic planning of supervisory activities. For the non-financial sectors, supervisors demonstrate varying yet improving understanding of ML/TF risks they face at the country- and sector-level. There was stronger awareness and compliance of AML/CFT obligations observed in sectors subject to regulation for longer periods while others have a less granular but improving understanding and implementation of their AML/CFT obligations. Supervisors have excellent outreach and engagement with their regulated population in terms of raising awareness on ML/TF risks and AML/CFT obligations.

h) MAS' supervision of financial institutions, DPTSPs and LTCs is also based on the three separate risk assessment components. These three components allow MAS to respond to risks in an agile manner. However, the planning of supervisory activities based on institutional level residual risks can be better documented and systematised across MAS. There is limited coverage of the supervised population for the FIRA and risk surveillance based supervisory activities. Singapore does not track complete statistics on the scope and/or findings of controls-based supervisory activities, which account for almost all of MAS' supervisory activities, to develop an understanding of the effect that supervisors are having on their supervised population. Nonetheless, the broad coverage of controls-based supervisory activities can, based on the case studies provided to demonstrate their rigour, be considered effective to a reasonable degree in supervising FIs/VASPs. Non-financial sector supervisors generally implement risk-based supervision, but it is recent in some sectors. There is a centralised mechanism for resource allocation; however, some lower risk sectors being subject to a higher intensity of supervision than some higher risk sectors. All supervisors employ a mix of remedial measures, while sanctions against institutions and individuals remain infrequent and are not proportionate to the risks identified. Overall, Singapore needs to strike a better balance between supporting reporting entities and preventing non-compliance.

i) Singapore is a hub for company formation and for wealth management, where trusts are used. Singapore demonstrates a reasonably good understanding of risks of how their domestically incorporated companies can be misused but a more limited understanding of risks, and accompanying mitigation measures, for legal arrangements, Unregistered Foreign Companies and complex structures. Basic and beneficial ownership (BO) information for legal persons is available but is largely unverified beyond customer due diligence (CDD), making the accuracy of the information questionable. Singapore's approach to transparency of BO information in relation to trusts largely relies on the access of BO information through a regulated entity, and this information has only been accessed for the small number of cases where there were suspicions of the misuse of trusts. There are limitations in the measures adopted by Singapore to ensure that the BO information is accurate and up to date. Enforcement against breaches of requirements relating to basic information of legal persons is robust but much less developed where there are lapses in BO transparency measures. The sanctions implemented are not yet dissuasive as increased penalties were very recently enacted.

j) Overall, Singapore faces unique threats. These financial crime challenges are being met by a competent and coordinated Singapore regime that is willing to try new solutions. There have been some successes in Singapore's fight against financial crime, but their AML/CFT/CPF system must be sharper in producing demonstrable and consistent risk-based results.

Ratings for effectiveness and technical compliance

	Effectiveness		Technical Compliance	
Risk mitigation through policy, co-ordination and co-operation				
Assessment of risk, co-ordination and policy setting	**IO.1**	Substantial	**R.1**	Largely compliant
			R.2	Compliant
International co-operation	**IO.2**	Substantial	**R.36**	Compliant
			R.37	Compliant
			R.38	Compliant
			R.39	Compliant
			R.40	Largely compliant
Cross-cutting requirements			**R.33**	Compliant
Prevention, detection & reporting of illicit funds across sectors				
Financial sector and virtual asset supervision and preventive measures	**IO.3**	Substantial	**R.9**	Compliant
			R.10	Compliant
			R.11	Compliant
			R.12	Compliant
			R.13	Compliant
			R.14	Compliant
			R.15	Largely compliant
			R.16	Largely compliant
			R.17	Compliant
			R.18	Compliant
			R.19	Largely compliant
			R.20	Compliant
			R.21	Compliant
			R.26	Compliant
			R.27	Compliant
Non-financial sector supervision and preventive measures	**IO.4**	Substantial	**R.22**	Compliant
			R.23	Largely compliant
			R.28	Largely compliant
Transparency and beneficial ownership	**IO.5**	Moderate	**R.24**	Partially compliant
			R.25	Partially compliant
Cross-cutting requirements			**R.34**	Compliant
			R.35	Largely compliant
Detection and disruption of threats, sanctions & deprivation of illicit funds				
Financial intelligence	**IO.6**	Substantial	**R.29**	Largely compliant
Money laundering investigations and prosecutions	**IO.7**	Moderate	**R.3**	Compliant
Asset recovery	**IO.8**	Substantial	**R.4**	Largely compliant
			R.32	Largely compliant
Terrorist financing investigations and prosecutions	**IO.9**	Substantial	**R.5**	Largely compliant
Terrorist financing preventive measures and financial sanctions	**IO.10**	Moderate	**R.6**	Largely compliant
			R.8	Compliant
Proliferation financing financial sanctions	**IO.11**	Moderate	**R.7**	Largely compliant
Cross-cutting requirements			**R.30**	Compliant
			R.31	Compliant

Note: Effectiveness ratings can be either a High-HE, Substantial-SE, Moderate-ME, or Low-LE, level of effectiveness. Technical compliance ratings can be either a Compliant-C, Largely compliant-LC, Partially compliant-PC or Non-compliant-NC. While the technical compliance findings can be relevant across the effectiveness immediate outcomes (for example, R.1 or R.40), the table above illustrates the main technical compliance findings specific to each effectiveness immediate outcome and cross-cutting requirements for each of the intermediate outcomes. For more detail on the relevant technical compliance requirements relevant to each effectiveness immediate outcome, see the relevant paragraph at the beginning of each chapter. See also paragraphs 53 and 54 of the FATF 2022 Methodology for links between effectiveness and technical compliance ratings.

Risks and general situation

2. Singapore has been a sovereign state since 1965 and is located in Southeast Asia, just south of the Malaysian peninsula. Singapore has a consistently low violent crime rate, a generally low crime rate and is frequently rated one of the safest countries in the world. However, Singapore's ML and PF risks are disproportionate to its domestic crime environment.

3. Singapore's open economy, large trade flows, status as an IFC and a hub for company formation and wealth management make it attractive to businesses, foreign criminals, as well as those looking to launder their funds and enjoy them in a stable environment. The characteristics of Singapore's economy can offer a platform to launder the proceeds of certain predicate offences. This includes Singapore most prominent ML threat i.e. fraud, particularly scams and other CEF, including those orchestrated by syndicates typically located overseas. Other prevalent predicate offences include: corruption, organised crime (including illegal gambling where operations can be based outside Singapore but services are targeted at Singapore residents), as well as tax crimes. High-profile cases like the 3B$ case underscore the scope and scale of the misuse of Singapore's financial system to launder the proceeds of crime.

4. Singapore is vulnerable to terrorism financing at the global and regional levels. The country is situated in a region where several terrorist groups operate actively, some of whom have carried out attacks regionally in the last 10 years. The TF threat of raising and moving funds for terrorists and terrorist activities overseas remains pertinent in Singapore's context, with self-radicalised individuals continuing to present the most salient TF risk. Singapore's status as an IFC and a hub for trade, transport, maritime and virtual assets makes it susceptible to the risks relating to the proliferation of weapons of mass destruction and PF. There are a number of legal persons operating in the maritime industry that sit outside of the population with AML/CFT obligations that are exposed to PF risks, particularly representation offices of foreign flag States.

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

5. Singapore employs a *dynamic approach* to identifying and assessing ML and TF risks, which has led to a reasonably sound understanding of its ML and TF risks. The dynamic approach is an agile approach that allows Singapore to identify changes in risks but is an approach that identifies and assesses individual risks on a case-by-case basis. Where significant changes of risks are identified, risk information is communicated to the private sector to strengthen risk awareness. Singapore's ML and TF NRAs are a synthesis of the findings made through the dynamic approach but lack some nuance and detail around certain risk areas, such as cross border flows and trade-based ML (TBML). Singapore demonstrates strong political commitment and has established robust governance structures to address ML/TF risks. However, there is a lack of systematic connection and prioritisation between risk identified in NRAs and the national AML/CFT strategies, which also did not include specific or detailed actions, deliverables and implementation timelines. Mitigation efforts are applied to individual risks as they arise without a comprehensive view of the overall risk landscape and the relative seriousness of the risk being addressed. Actions taken are reported through the RTIG and AML/CFT SC/IAC mechanism. As a result, competent authorities are actively engaged in the dynamic approach process with objectives generally aligned to identified risks, though there remain some inconsistencies in operational alignment and supervisory coverage.

6. Enhanced measures are well-developed and effectively applied in higher-risk scenarios, including dealings with complex legal persons, DPTSPs, and high-risk jurisdictions. While Singapore's legal framework allows simplified customer due diligence (SDD) and exemptions in lower risk areas, Singapore adopts a cautious approach to (i) simplified measures, which is reasonable and (ii) exemptions, and the

mechanism can be used more consistently. This reflects a broader weakness in Singapore's dynamic approach, which tends to prioritise higher risks flagged by authorities but lacks mechanisms to consistently identify and assess lower-risk scenarios for simplified measures/exemptions.

7. Singapore's AML/CFT/CPF system is underpinned by extensive domestic co-ordination and co-operation through high-level and working-level committees that ensure cross-agency collaboration, policy alignment, and risk monitoring, supported by subject-specific interministerial committees. The system reflects a well-integrated whole-of-government approach, with active engagement from supervisory authorities and industry associations. Singapore has strong operational co-ordination and co-operation mechanisms, including AC3N and AML/CFT Industry Partnership (ACIP), which facilitate inter-agency and public-private collaboration on AML/CFT efforts. These frameworks have led to largely effective case co-ordination and improved risk understanding, making policy co-operation a key strength of Singapore's AML/CFT regime.

International co-operation (Chapter 2; IO.2; R.36-40)

8. International co-operation is critical for Singapore as an IFC with primary threats abroad.

9. Singapore has a sound legal and operational framework to provide and seek a broad range of assistance. This is supported by bilateral and multilateral treaties, standard operating procedures (SOPs), recent legislative amendments and a simplified extradition mechanism with Malaysia and Brunei. Singapore is generally responsive to formal co-operation requests.

10. Singapore's central authority takes a collaborative approach and applies a prioritisation system for international co-operation. Singapore provides effective international co-operation to a reasonable extent, having executed a majority of mutual legal assistance (MLA) it receives and refusals are rare. Singapore received 988 MLA requests, of which 34% remain pending/partially addressed and are at different stages of execution (8% of these pending requests remaining entirely unaddressed). Singapore's legal threshold for granting co-operation may cause some delays. Feedback from the Global Network generally suggest Singapore is proactive and provides timely and effective co-operation, although there are indications that the process to clarify the nature of the requests and whether they meet the legal threshold may cause delays.

11. Singapore seeks international co-operation in more modest ways and makes four times fewer MLA requests than it receives despite acknowledging that its primary risks lie abroad. Authorities seek modest formal co-operation for ML when considering the significant number of ML investigations. Formal and informal co-operation aligns with risks to some extent, as it is sought almost exclusively for fraud and ML cases, while fewer requests were made in respect of other higher-risk crimes and typologies such as tax crime, corruption and TBML.

12. Singapore has shown some success using international co-operation for asset recovery purposes. Singapore is responsive to requests and enforces a small number of confiscation orders which leads to repatriation of assets in a limited number of cases. The need to verify legal requirements under Mutual Assistance in Criminal Matters Act 2000 (MACMA), can delay asset recovery efforts and increase the risk of asset dissipation to some extent, however LEAs can use Criminal Procedure Code (CPC) powers simultaneously to seize/freeze assets. While Singapore has sent a very modest number of MLAs to recover assets, Singapore actively engages in informal forms of co-operation, often in support of formal co-operation. Competent authorities actively engage in a broad range of bilateral and multilateral channels to pursue criminals and criminal property. This co-operation is generally timely, effective, and aligns with risks to some extent.

Financial sector and virtual asset supervision and preventive measures (Chapter 3; IO.3, R.9-21, 26, 27, 34 & 35)

13. Singapore has been ranked by the International Monetary Fund as one of 29 systemically important financial centres in the world. In addition to its large, important and complex financial institutions with global reach, Singapore has, since the last report, developed into one of the most significant virtual asset services providers hubs in the world. MAS supervises all financial institutions except for moneylenders, who are supervised by MinLaw.

14. Singapore has a robust licensing framework in place to ensure that criminals and their associates are not beneficial owners or hold controlling interests in FIs and VASPs to a very large extent. SPF investigates unlicensed activities on the basis of referrals from supervisors but the penalties for conducting unlicensed activities could be more effective, proportionate and dissuasive.

15. MAS has a robust understanding of country-level and sector-level ML/TF risks from its involvement in the dynamic approach. MAS identify institutional-level ML/TF risks through three separate components: (1) inherent risk assessment (FIRA) and (2) risk surveillance managed by the dedicated AML Department (AMLD); and (3) AML/CFT controls information managed by AMLD and the nine prudential supervisory departments. MAS' understanding of institutional-level ML/TF risks is varied and was established through day-to-day consultation and co-ordination between AMLD and the nine supervisory departments. These three components are useful in considering different risk information, but this process is not thoroughly systematised and a net view on institutional residual risk has not been consistently documented. This impacts MAS' ability to develop and implement a supervisory strategy with a comprehensive assessment of residual risks at the institutional level.

16. MAS' work to ensure that FIs and VASPs understand ML/TF risks and AML/CFT obligations is a strength of Singapore's system. FIs and VASPs have a solid understanding of ML/TF risks. FIs and VASPs generally demonstrated a comprehensive understanding of AML/CFT obligations and risk control measures. STRs are generally appropriately reported, but there may be underreporting in some higher risk sectors (e.g. DPTSP).

17. MAS' supervision of FIs/VASPs selects entities for supervisory activities through the three separate risk assessment components identified above. The three components allow MAS to address potential vulnerabilities and respond to emerging threats in an agile manner, however they are not systematically planned in accordance with institutional-level residual risks in a fully consolidated and documented manner. The vast majority of MAS' supervisory activities consist of day-to-day controls-based activities that are not risk-based. There is a good level of coverage for these activities in terms of frequency, but they vary in scope and depth significantly, and Singapore does not track complete statistics of their scope or outcomes to develop an understanding of the effect that supervisors are having on their supervised population, even though Singapore was able to demonstrate the rigour of these activities through case studies. Periodic supervisory activities based on FIRA and risk surveillance respond to risk, but the coverage of resulting supervisory activities is limited.

18. MAS adopts a range of remedial and enforcement actions depending on the severity of breaches. MAS has increased its enforcement actions since the last MER, particularly against individuals and such actions are generally published for deterrent effect. Overall, the number of enforcement actions remains relatively low and the level of financial sanctions remains not proportionate when considering the size of relevant FIs/VASPs, the serious nature of breaches, as well as Singapore's risk and context. MAS' enforcement actions are complemented by Singapore's extensive remedial measures and close monitoring, strong industry engagement and public-private partnership that have shown improvements in compliance behaviour.

Non-financial sector supervision and preventive measures (Chapter 4; IO.4, R.22, 23, 28, 34 & 35)

19. Singapore covers all non-financial sectors required to be covered for AML/CFT obligations by the FATF Standards (DNFBPs). CSPs, prominent in the formation of legal persons in Singapore, and LTCs, prominent in the formation of legal arrangements in Singapore, play important roles as gatekeepers to legal persons and arrangements and in making basic and BO information available.

20. Singapore has implemented robust market entry controls and fit and proper tests to prevent criminals and their associates from being the beneficial owners or holding a controller position in these non-financial sectors. DNFBP supervisors, which are mostly sector-specific, actively detect and investigate unlicensed activities under their respective regulatory remit, and SPF investigates into unlicensed activities, such as illegal gambling.

21. Singapore's DNFBP supervisors demonstrate varying yet improving understanding of ML/TF risks they face at the country- and sector-level. Singapore has taken efforts to promote a good understanding of AML/CFT obligations across the DNFBP sectors with most DNFBPs demonstrating a reasonable understanding of their ML/TF risks. There was stronger awareness and compliance of AML/CFT obligations observed in sectors subject to regulation for longer periods (e.g. LTCs, CSPs, accountants, and casinos), while others (e.g. Precious Stones and Precious Metals Dealers (PSMDs)) have a less granular but improving understanding and implementation of their AML/CFT obligations.

22. While DNFBP supervisors generally implement risk-based supervision models, this implementation is recent in some sectors (e.g. developers). There is a centralised mechanism for resource allocation; however, this has not led to fully consistent approaches to supervision across the DNFBP sectors with some lower risk sectors being subject to a higher intensity of supervision than some higher risk sectors. Supervisors use a range of remedial and enforcement actions depending on the nature and severity of issues observed. Where sanctions were applied, the level of financial penalty is usually not dissuasive, especially taking into account the relative scale of company and transactions. Supervisory tools have been shown to demonstrate improvements in risk understanding and execution of AML/CFT controls in some sectors.

Transparency and beneficial ownership (Chapter 5; IO.5, R.24 & 25)

23. Singapore is a major IFC, and a hub for company formation and for wealth management, where trusts are used. Far fewer trusts are formed and used in Singapore compared to companies. Singapore conducted risk assessments for legal persons (LPs) and legal arrangements (LAs) in 2024 and demonstrates a strong understanding of the risks stemming from Singapore incorporated companies but can further enhance their understanding of the risk posed by legal arrangements, Unregistered Foreign Companies (UFCs) and the misuse of multi-legal person/arrangement structures. Singapore's efforts to mitigate risks associated with LPs and LAs focuses on transparency requirements, registration requirements with ACRA (for LPs), and licensing, supervision and monitoring of reporting entities. Singapore's implementation of these is a positive step towards mitigating the risk of misuse of LPs/LAs; however, these measures have deficiencies or were too recently implemented to be effective.

24. Singapore has implemented a central BO registry though ACRA, for all legal persons, except VCCs and Unregistered Foreign Companies, which includes information from almost all companies and LLPs. There are limited mechanisms to ensure the information on the registry is accurate. Beyond basic validation checks, Singapore does not verify BO information at the point of filing into the central BO registry; they instead rely on the CSPs conducting proper CDD to identify the BO and to ensure accuracy of information filed. Competent authorities have direct and immediate access to the central BO registry, but it is not

publicly available. BO information related to VCCs and UFCs is not available in a timely manner in all cases or at all in the limited cases where a foreign legal person is recorded as the beneficial owner in the central BO registry. Where information is not available through the ACRA central registry, there are alternative mechanisms that can make the information available if LEAs can identify which reporting entity to inquire with. ACRA has a robust and automatic enforcement regime for non-compliance with annual report obligations which contain basic information. Enforcement for breaches of BO information requirements is more nascent but is progressively improving. The sanctions implemented are not yet dissuasive as increased penalties were just enacted.

25. Singapore's approach to transparency of BO information in relation to trusts has been to rely on the access of BO information through an LTC or PTC (where their services were engaged), FIs, (if a bank account is maintained for the trust in Singapore) and/or DNFBPs (if other professional services are required), and this has only been done in practice in a few cases. These gatekeepers are legally required to conduct CDD and cannot commence or continue business relations with a customer unless CDD is completed. There are limitations in the measures adopted by Singapore to ensure the BO information is accurate and up to date as this is done by MAS during supervisory activities. The supervisory coverage targeting BO requirements for LTCs is low. All wakafs must be registered with MUIS who makes the information available to competent authorities. MUIS is the legal owner and administrator of all wakafs, the trustee-equivalent and registrar for wakafs.

Financial intelligence (Chapter 6 ; IO.6, R.29-32)

26. Singapore's FIU (STRO) is well resourced and leverages on sophisticated systems to produce financial intelligence. Although there is some ambiguity about the FIU's operational independence, that did not have an observed effect on STRO's ability to conduct its business.

27. Singapore places priority on cross-government data integration, as a result competent authorities have access to a broad spectrum of reports, data and information. Competent authorities have access to a broad and expanding range financial information (e.g. STRs, CMRs and CTRs), data and other information. STRO plays an important role generating financial information (MASDs and self-screening) and intelligence (Fin-IRs and financial intelligence packages). Its disseminations generally support the needs of LEAs, as shown through case studies and interviews with the authorities but could be more aligned with Singapore's risks.

28. 30 918 STRs (11% of those received) were disseminated as Fin-IRs, and 469 financial intelligence packages (2023-2024) were disseminated mostly to LEAs. 26% of financial intelligence packages (17% of Fin-IRs) initiated an investigation, and 14% (14% of Fin-IRs) supported investigations (Table 3.8). Financial intelligence from STRO is being used to initiate and support investigations into ML, associated predicate offences and TF to a good extent but more could be done to leverage financial intelligence for higher risk offences (except fraud). Competent authorities regularly use financial information to support investigations, develop evidence, identify and trace criminal proceeds or instrumentalities, including high-value and significant ML cases, but do not use financial intelligence to support investigations to the same degree.

29. STRO and competent authorities regularly and proactively co-operate with each other, as exemplified in AC3N and ACIP. They routinely exchange financial intelligence and information and co-ordinate on joint operational planning and responses, which has resulted in detecting, investigating and prosecuting cases.

Money laundering investigations and prosecutions (Chapter 7; IO.7, R. 3, 30 & 31)

30. Singapore has an appropriate legal and operational framework to identify and investigate ML (including in complex cases), supported by competent, well-resourced and trained LEAs. LEAs opened 11 189 ML investigations. Over 80% of ML investigations were initiated from victims' complaints in relation to CEF. Other sources, especially financial intelligence, referrals from predicate agencies, and international co-operation, are underutilised to identify ML. While LEAs focus on laundering of the proceeds from fraud to an overly appropriate extent, there are significantly fewer investigations into other higher-risk areas like tax crimes, corruption and TBML, which aligns with Singapore's risk and context only to some extent.

31. Singapore can pursue different types of ML (including third party, and standalone ML). As demonstrated by the 3B$ case, Singapore has shown an ability to conduct ML investigations into higher-risk predicates and complex investigations (both domestic and foreign), including organised crime, tax, and TBML. Singapore experienced challenges converting ML investigations into prosecutions, owing to both the nature of the investigations pursued (money mule investigations with a foreign nexus) and legislative challenges. Of the 11 189 ML investigations, competent authorities referred 7 594 ML investigations to the AGC for prosecution. Only 682 natural persons were prosecuted during the review period, a conversion rate of less than 10%, considering that an investigation can be conducted into multiple natural persons simultaneously. Once cases are prosecuted though, Singapore achieves a good conviction rate (82%), including in complex cases, although the majority of sanctions are made for low-level money mule cases, rather than professional syndicates, professional intermediaries, and legal persons. Convictions are largely the result of guilty pleas, which undermines the overall deterrence of sanctions.

32. Singapore, to some extent, employs a combination of criminal, administrative and regulatory tools as alternative measures when it is not possible to secure ML convictions. Some of these (like CDSA S55A(1), the 'Money Mule Offence') were recently introduced and it is premature to assess effectiveness.

Asset recovery (Chapter 8; IO.8, R. 1, 4 & 32)

33. Asset recovery is a high-level political priority, supported by the National Asset Recovery Strategy (NARS), SOPs, and WoG approaches. Singapore has a strong operational and legal framework for asset recovery, including to manage and return assets, which is regularly reviewed. Effective agency structures and co-operation mechanisms enable the use of government data, public-private partnerships (e.g. RTIG, AC3N, etc.), and international co-operation to facilitate broad and effective information exchange to trace assets.

34. LEAs proactively and routinely identify and trace criminal property. However, some deficiencies in the types of ML cases pursued, difficulties in mounting ML prosecutions for foreign predicate offences and insufficient targeting of complex structures and professional intermediaries, affect the scope and quantum of assets identified and pursued. LEAs actively freeze and seize criminal property to prevent the dissipation of assets, including through expeditious measures, seizing approximately SGD 6 billion (USD 4.4 billion) over the review period, including in high-value and complex cases (e.g. the 3B$ case). About a third of ML investigations lead to seizures. 95% of the seizures stem from lower-value non-ML cases and align with risks to a reasonable extent.

35. Singapore achieves a positive seizure to confiscation rate (61 %) and has obtained a significant amount of confiscation: SGD 3.9 billion (USD 2.9 billion) between 2020 and 2024. LEAs demonstrated they can confiscate a wide variety of assets across complex cases using a combination of CBC, NCB and tax recoveries in criminal cases. Confiscations align with risks to a reasonable extent.

36. While authorities proactively seek assistance from foreign counterparts through informal mechanisms, Singapore is less proactive in its use of formal international co-operation. They do not seek

enforcement of its own confiscation orders abroad, especially concerning considering the volume of predicate and ML investigations. This depresses the chances of final confiscation or repatriation of assets to Singapore.

37. While Singapore has a solid legal framework for cross border cash reporting regime, there are issues with its enforcement, particularly the detection of violations. Most individuals who fail to file or file a false declaration are first-time offenders, and the authorities have only been able to link one offender to broader criminality out of 439 cases, showing an issue with follow-up investigations and use of the system for asset recovery leads. Sanctions for smuggling violations are proportionate and dissuasive in rare cases when offenders are linked to ML, TF or predicate offences, but when links are not established, sanctions are neither proportionate nor dissuasive.

Terrorist financing investigations and prosecutions (Chapter 9; IO.9, R. 5, 30, 31 & 39)

38. The identification and investigation of TF is carried out by ISD, CFTB and STRO, who co-ordinate closely and cooperatively. Financial intelligence is actively utilised in TF investigations. Investigative techniques are sound; however, there are opportunities for broader range of investigations including potential organisational TF and through concealed income analysis.

39. Singapore has opened 126 TF investigations into 213 natural and legal persons over the past five years. From these investigations, they have prosecuted six cases of TF over the reporting period that all display the same typology which involves individuals sending small amounts of their salary overseas to support global terrorist activities. While this is largely in line with Singapore's risk and context, there is an absence of CTF activity in relation to funds transiting through Singapore via the banking sector or DPTSPs, which has been identified by Singapore as one of its highest TF risks.

40. Only six of 126 TF investigations were brought to prosecution, but all prosecutions have resulted in conviction, with five involving a guilty plea and one case proceeding to a full trial. The AGC prosecutes TF offences in cases where they determine the evidential threshold to be conclusively met. This high evidential threshold has likely led to some cases not being prosecuted. Where prosecutions are secured, sanctions are proportionate and dissuasive. Singapore undertakes preventive measures including immigration controls and incorporates rehabilitation and de-radicalisation to counter recidivism. These are actions to prevent terrorism and terrorist financiers, and not alternative measures when a TF conviction was not practicable.

41. Singapore has strategic, policy and operational committees in place which utilise information from TF investigations to inform national CT efforts, contribute to TF threat assessments and the ML/TF NRA, as well as providing policy guidance.

Terrorist financing preventive measures and financial sanctions (Chapter 10; IO.10, R. 1, 4, 6 & 8)

42. Singapore's framework for proposing designations for TF TFS is capably led by the IMC-TD and appropriately governed by TSOFA. There are multiple intermediaries between an alert from the UNSC on changes in listings and dissemination by Singaporean authorities to reporting entities. This has the potential to cause multiple potential points of failure to communicate designations and has caused delays in implementation.

43. FIs and VASPs in Singapore demonstrated a sound understanding of their obligations in relation to TF TFS, including to freeze assets without delay. Understanding of TF TFS obligations across DNFBPs was

varied, with scope for improvement across virtually all DNFBPs. Singapore's FI, VASP and DNFBP supervisors do not have appropriate supervisory coverage for TF TFS obligations. FIs and VASPs are subject to a very significant number of controls-based supervisory engagements that rectify compliance deficiencies, but it is unknown how many of those were in respect to TF TFS. There were limited more intensive supervisory examinations. Where there were supervisory activities, a reasonably high deficiency rate was observed. Identified deficiencies are generally addressed with non-punitive remedial measures.

44. During the assessed period, Singapore froze a net value of SGD 1.3 million (USD 962 000) of assets listed under Singapore's domestic TFS regime (i.e. UNSCR 1373), with approximately SGD 3.97 million (USD 2.9 million) of assets frozen overall currently, but no assets have been identified or frozen under the UNSCR 1267 regime.

45. Singapore uses a strong programme of guidance and outreach to mitigate its medium-low risk of TF abuse of NPOs within the FATF definition. The approach is focused, proportionate and not unduly disruptive to the legitimate activities of NPOs in Singapore.

Proliferation financing financial sanctions (Chapter 11; IO.11, R.7)

46. Singapore has a number of contextual factors and attributes which make it one of the jurisdictions most vulnerable to PF: its geographical position, and its status as an IFC, and a hub for trade, transport, maritime and virtual assets. Singapore has a strong legal framework for PF TFS obligations, with the AML/CFT SC providing co-ordination and policy leadership allowing Singapore to convene quickly to discuss PF issues and co-ordinate as needed. The IMC-EC which leads Singapore's counter-proliferation and export controls regime plays an active role in Singapore's PF (including PF TFS) risk mitigation.

47. Singapore's 2024 PF NRA identifies its PF TFS risks. The threats, vulnerabilities and risks have largely been appropriately identified but the PF NRA could be strengthened with more granular contextual data specific to Singapore's context. The risk mitigation measures as set out in Singapore's CPF Strategy are general, are not proportional to risk and are largely already being conducted as part of Singapore's CPF regime. Singapore's PF NRA also highlights higher risk areas that have no or negligible mitigation measures identified.

48. The communication mechanisms and obligations for PF TFS are identical to what is described under IO.10 for TF TFS. There were some instances over the assessment period where processes were not able to react without delay.

49. Singapore's FIs and VASPs broadly have a good understanding of their obligations to comply with PF TFS, and most subscribe to commercial sanctions-screening software. DNFBPs demonstrated an uneven understanding of obligations. Reporting entities lodged around 1 900 STRs related to PF, with 732 related to the DPRK during the assessment period and five financial intelligence packages related to UNSC DPRK sanctions were disseminated to relevant competent authorities. Other at-risk entities, particularly representation offices of foreign flag States, which are not AML/CFT-obliged entities, have very low awareness of the PF TFS obligations.

50. Singapore is not systemically identifying and addressing non-compliance with PF TFS through risk-based supervisory activities. FIs and VASPs are subject to a significant number of controls-based supervisory engagements but it is unknown how many of those were in relation to PF TFS.

51. Singapore's AGC successfully prosecuted 22 natural persons and eight legal persons for PF-related/proliferation-related breaches of Singapore's UN (Sanctions – DPRK) Regulations and other export control regulations. No natural or legal person has been prosecuted for PF TFS breaches. MAS has imposed a financial penalty on an FI for PF TFS breaches. Overall, penalties for breaches of or failure to comply with CPF-related obligations are relatively low and cannot be considered proportionate and dissuasive in all

cases. SGD 22.3 million (USD 16.2 million) has been frozen in one case during the reporting period. This does not accord with Singapore's risk and context or the number of STRs relating to the DPRK and PF-related/proliferation-related prosecutions in the reporting period.

Roadmap of key recommended actions (KRAs)

1. Singapore underwent a Mutual Evaluation of its anti-money laundering / countering the financing of terrorism / countering proliferation financing (AML/CFT/CPF) measures in place during its on-site visit to the country from 1-18 July 2025. This evaluation was based on the 2012 FATF Recommendations (as updated from time to time) and was prepared using the 2022 Methodology.

2. The Mutual Evaluation Report identifies the strengths and weaknesses of Singapore's AML/CFT/CPF system, including both the level of effectiveness and the level of technical compliance, and recommended actions for improvement. The highest priority measures are identified as Key Recommended Actions (KRA) are included in this KRA Roadmap.

3. The following presents the KRA Roadmap for Singapore as adopted by the FATF Plenary in February 2026. Based on Effectiveness and Technical Compliance Ratings, Singapore is placed in regular follow-up. This KRA Roadmap also serves as the basis for Singapore's follow-up process.

Singapore should:.

IO.5 (Transparency and beneficial ownership)

a) Review and enhance the risk assessments of legal persons and arrangements in Singapore to ensure a robust and practical understanding of risks. Risks should be identified, analysed and understood to mitigate significant risks more quickly including for:
   a. Unregistered Foreign Companies maintaining bank accounts, investing in funds and/or purchasing real estate (and whether, on the basis of ML/TF/PF risk, this constitutes a sufficient link).
   b. Trusts not formed in Singapore, trusts not formed through an LTC; and whether the current supervisory intensity to LTCs ensures accuracy of BO information and mitigates the misuse of trusts.
   c. Legal persons not operating in line with original policy intent (e.g. VCCs not being used as CIS).
   d. Complex arrangements comprising multiple types of legal persons and/or arrangements.

b) Review, enhance, and implement additional mechanisms to ensure accuracy (i.e. verification and triangulation) of BO and nominee information in ACRA's central registries to improve the registries' accuracy.

c) Based on findings arising from review of risk assessment, identify and implement necessary enhancements to Singapore's multi-pronged approach to trusts.

IO.7 (Money laundering investigations and prosecutions)

d) Review and refine the process for prioritising ML investigations (particularly in relation to CEF) to better consider Singapore's risk and context, and pursue complex, high-value investigations.

e) Pursue investigations and prosecutions for local directors and professional intermediaries who are facilitating ML activity within Singapore's borders.

f) Ensure that effective and dissuasive sanctions are applied proportionately to the offence, including tailored sentencing guidelines for ML.

IO.10 (Terrorist financing preventive measures and financial sanctions)

g) Ensure communication of TF TFS without delay using a more streamlined approach to reach all competent authorities and reporting entities.

h) Use a wider range of information and skill sets including BO information, concealed income analysis and complex network analysis to ensure the funds and assets of natural and legal persons subject to TF TFS pursuant to UNSCR 1267 are identified.

i) Ensure that funds and assets related to TF are immobilised, rather than only immobilising the individual when under investigation for TF offences.

IO.11 (Proliferation financing financial sanctions)

j) Improve supervisory coverage and intensity, and engagement specific to PF TFS for higher risk sectors, particularly VASPs and CSPs.

k) Deepen context-specific understanding of PF TFS evasion risks and implement further risk and context-specific risk mitigation measures.

l) Increase PF TFS engagement with representation offices of foreign flag States to increase awareness of obligations and the risks associated with DPRK-related financial flows and complex PF TFS sanctions evasion techniques.

Preface

This report summarises the anti-money laundering / countering the financing of terrorism / countering proliferation financing (AML/CFT/CPF) measures in place as at the date of the on-site visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the AML/CFT/CPF system and recommends how the system could be strengthened.

This evaluation was based on the 2012 FATF Recommendations (as updated from time to time) and was prepared using the *2022 Methodology*. The evaluation was based on information provided by the country, and information obtained by the evaluation team during its on-site visit to the country from 1-18 July 2025.

The evaluation was conducted by an assessment team consisting of:

- Ms. Nicola Critchley, Department of Home Affairs, Australia.
- Ms. Diana Soraya Noor, Pusat Pelaporan dan Analisis Transaksi Keuangan, Indonesia.
- Mr. Qipeng Xu, People's Bank of China, People's Republic of China.
- Ms. Avril Wadelan, Ministry of Justice, New Zealand.
- Mr. Smarak Swain, Department of Revenue, India.
- Ms. Alison Kelly, His Majesty's Treasury, United Kingdom.

with the support from the FATF Secretariat of Ms. Jenny Chan, Mr. Mat Tromme and Mr. Mike Fowler and the Asia Pacific Group on Money Laundering of Ms. Margaret Stone and Ms. Mitali Tyagi.

The report was reviewed by Ms. Ailsa Hart, World Bank; Mr. Niko Salonen, Ministry of Finance, Finland; and Tamar Waldman, Israel Money Laundering and Terror Financing Prohibition Authority, Israel.

Singapore previously underwent a Mutual Evaluation in 2016, conducted according to the *2013 FATF Methodology*. The 2016 evaluation and 2019 *follow-up report* have been published and are available at https://www.fatf-gafi.org/en/countries/detail/Singapore.html

That Mutual Evaluation concluded that the country was compliant (C) with 18 Recommendations; largely compliant (LC) with 16 Recommendations and partially compliant (PC) with 6 Recommendations. Singapore was rated C or LC with 5 of the following 5 Recommendations which were triggers for enhanced follow-up during the last round: R.3, 5, 10, 11 and 20.

Based on these results, Singapore was placed in enhanced follow-up. Since its last evaluation, Singapore achieved 4 technical compliance re-ratings:

- 1 Recommendation upgraded from PC to C: R.25;
- 2 Recommendations upgraded from PC to LC: R.23, R.24;
- 1 Recommendation upgraded from LC to C: R.3.

Based on this progress, Singapore remains in enhanced follow-up for both technical compliance and effectiveness deficiencies. In total, 3 Recommendations (Recommendation 22, Recommendation 28 and Recommendation 35) remain rated PC since the last evaluation of Singapore.

Introduction to money laundering and terrorist financing risks and context

52. Singapore has been a sovereign state since 1965 and is located in Southeast Asia, just south of the Malaysian peninsula. Singapore is an island state with a land area of about 715 square kilometres; one of the smallest countries in the world, and the smallest in the ASEAN region. The population of Singapore stands at 6.11 million as of 2025, of which around 69% are Singapore residents. A multi-racial and multi-religious society, the three largest ethnic groups are Chinese, Malay and Indian.

53. Singapore is a republic operating on a Westminster system of unicameral parliamentary government.

54. Parliament, the legislature, comprises Members of Parliament (MPs) who are elected by voters in a general election held every five years. In terms of composition, the Singapore Parliament consists of elected MPs, as well as a small number of non-elected MPs. Elected MPs are candidates who have won seats at the general elections while non-elected MPs are appointed by the President of Singapore to provide independent and non-partisan views in Parliament.

55. The executive authority of Singapore is vested in the elected President. Following the Westminster system of parliamentary government, the President acts in accordance with the advice of the Cabinet in general. The Cabinet, under the helm of the Prime Minister, is collectively responsible to Parliament.

56. The judiciary is one of the three constitutional pillars of government along with the legislature and the executive. The judiciary is safeguarded by the Constitution and as an organ of state, the judiciary's function is to independently administer justice. Singapore operates on a common law system which is characterised by reliance on judicial precedent in interpreting the law. The judiciary comprises the Supreme Courts (the Court of Appeal and High Court), the State Courts (including the Magistrate and District Courts) and the Family Justice Courts. The highest court of the land is the Court of Appeal, which hears both civil and criminal appeals emanating from the High Court and the State Courts. In accordance with the doctrine of judicial precedent, the ratio decidendi found in the decisions of the Singapore Court of Appeal are strictly binding on the Singapore High Court, the District Courts and the Magistrate Courts.

ML/TF/PF risks and scoping of higher-risk issues

Overview of ML/TF/PF risks

57. Singapore has a consistently low violent crime rate, a generally low crime rate and is frequently rated one of the safest countries in the world. However, Singapore's ML/TF/PF risks are disproportionate to its domestic crime environment.

58. Singapore's open economy, important financial sector and large trade flows make it attractive for business, foreign criminals, as well as those looking to launder their funds and enjoy them in a stable environment. The characteristics of Singapore's economy can offer a platform to launder the proceeds from certain predicate offences. This includes most prominently fraud, particularly scams and other CEF, including those orchestrated by syndicates typically located overseas. Other prevalent predicates offences include: corruption, organised crime (including illegal gambling whose operations can be based outside Singapore but targeting services towards Singapore residents), as well as tax crimes. Trade, or the movement of value through trade, remains an attractive vector for money launderers. This inherent vulnerability is magnified by the other characteristics of open access to Singapore's financial system.

59. Singapore's primary ML risk largely emanates from foreign offences and offences with a foreign nexus. Illicit funds are primarily channelled into Singapore's economy through a mature and connected banking sector, which is exposed to a diverse set of ML vulnerabilities. Banks, DPTSPs (VASPs in the FATF Recommendations) and payment service providers with cross-border money transfer services (PSPs with CBMT Services) have been misused in a variety of manners to transfer illicit funds into and out of Singapore.

60. Singapore is an IFC that is a hub for company formation and for wealth management, where trusts are used. Singapore experiences significant ML risk through the use of gatekeepers or intermediaries to access its financial system. These actors can provide foreigners access to Singapore's economy through their services, and include: corporate services providers (CSPs) (TCSPs in the FATF Recommendations), which have been misused by foreign criminal groups to create shell/front companies and is assessed as Singapore's highest-risk DNFBP sector; LTCs, which can create complex structures and deal in significant volumes of funds; external asset managers (EAMs), which deal with higher-risk customers offering bespoke investment services and manage assets in the private wealth space, including to foreign clients; and real estate agencies, salespersons and developers, given the attractiveness of Singapore's real estate market.

61. Lastly, legal persons and arrangements in Singapore are able to provide a number of personal, commercial, wealth management and asset retention services, including single family offices, which provide services to high-net-worth individuals. These legal persons and arrangements can be created with relative ease and can be used to access Singapore's significant and far-reaching economy. Legal persons and arrangements in Singapore are generally at higher risk when they include a foreign dimension, either through being associated to foreign individuals or conducting foreign business.

62. Singapore is vulnerable to terrorism financing at the global and regional levels. Singapore is situated in a region where several terrorist groups operate actively, some of whom have carried out attacks regionally in the last 10 years. Singapore's key TF threats stem from: (i) terrorist groups such as the Iraq and Syria (ISIS), Al-Qaida (AQ), and Jemaah Islamiyah (JI), with potential spillovers from the ongoing Israel-Hamas conflict and tensions in the Middle East, and (ii) radicalised individuals who are sympathetic towards the cause of these terrorist groups, particularly ISIS. Far-right extremism is also a growing security concern in Singapore. The TF threat of raising and moving funds for terrorists and terrorist activities overseas also remains pertinent in Singapore's context, with self-radicalised individuals continuing to present the most salient TF risk.

63. Singapore’s status as an IFC and a hub for trade, transport, maritime and virtual assets makes it susceptible to the risks relating to proliferation of weapons of mass destruction and PF. Singapore is

exposed to the key PF threats of misuse of legal persons, ship-to-ship transfers, movement of dual-use goods, export of luxury goods, and misuse of virtual assets. Key PF vulnerabilities amongst the entities having AML/CFT obligations are observed in banks, which are exposed to higher PF risks given the wide range of services they provide and large volume of transactions that they process on a daily basis; DPTSPs, which are exposed to some PF risks given their activities dealing with virtual assets that are known to be misused by individuals and entities involved in the proliferation of WMD and PF; as well as remittance agents, maritime insurers, and CSPs, whose services can be vulnerable to PF. There are a number of legal persons operating in the maritime industry that sit outside of the population with AML/CFT obligations that are exposed to PF risks, particularly representation offices of foreign flag States.

Country's risk assessment and scoping of higher-risk issues

64. Singapore monitors its ML/TF/PF risks through the Risks and Typologies Inter-Agency Group (RTIG), which allows relevant competent authorities to identify and share information on surveillance and risk observations to enable co-ordinated mitigation actions. Singapore published separate ML, TF and PF NRAs in 2024, following its last ML NRA in 2014. Through RTIG and engagement with the private sector, Singapore has also published various public thematic assessments on the misuse of legal persons (2019 and 2024), Virtual Assets (2020 and 2024), TF Non-Profit Organisations (NPOs) Risk Assessment (2019), legal arrangements (2024) and environmental crime ML (2024).

65. Singapore assessed the following key ML threats: (i) fraud (particularly, CEF and scams), (ii) organised crime, (iii) corruption, (iv) tax crimes, and (v) TBML. Illicit funds flowing into or through Singapore are observed to be most commonly laundered via bank accounts. Legal persons (particularly, shell companies) are misused for laundering of illicit funds, including from corruption and tax ML. In particular, networks of Singapore-incorporated companies created and ultimately controlled by criminal networks have been used for ML purposes. Singapore assesses the banking sector poses the highest ML risk to Singapore. The role of banks in facilitating transactions in the financial system, and their wide networks through which cross-border transactions are conducted, make banks a common channel which criminal exploit. In addition, banks are exposed to a larger proportion of customers with higher ML risks (including those from higher ML risk jurisdictions), high volume of cross-border transactions, and a range of complex products and structures. DPTSPs, PSPs with Cross Border Money Transfer Services and EAMs are also observed to be higher risk for similar reasons. Among the DNFBP sectors, CSPs are assessed to pose higher (i.e. medium high) risks given the role they play in providing upstream services such as incorporation of companies.

66. Singapore assesses that its key TF threats stem from: (i) terrorist groups such as the ISIS, AQ, and JI, potential spillovers from the ongoing Israel-Hamas conflict and tensions in the Middle East, and (ii) radicalised individuals who are sympathetic towards the cause of these terrorist groups, particularly ISIS. Considering the key threats and vulnerabilities, money remittances (i.e. cross border money transfer service providers) including unlicensed money remittances and cross-border online payments are assessed to pose the highest risks, while banks and DPTSPs pose medium high risks given their roles in facilitating cross border transactions.

67. Singapore is exposed to the key PF threats of misuse of legal persons, ship-to-ship transfers, movement of dual-use goods, export of luxury goods and misuse of virtual assets. Banks are exposed to higher PF risks, as compared to other sectors in Singapore given the wide range of services they provide and the large volume of legitimate trade and trade financing transactions that they process on a daily basis. Among the DNFBP sectors, CSPs are exposed to some PF risks given their role in the formation of companies and the procurement of nominee directors. DPTSPs are also exposed to some PF risks based on Singapore's risk surveillance and international typologies including those featured in the United Nations Security Council Panel of Experts' reports.

68. In terms of scoping for increased focus, the Assessment Team prioritised measures addressing the measures designed to mitigate cross-border risk of ML derived from foreign predicate offences, foreign organised crime and offences with a foreign nexus, such as CEF and scams. This includes increasing focus on access points into and through Singapore's economy, such as the parts of the financial sector enabling cross-border financial transactions, gatekeepers and intermediaries servicing foreign access, and the misuse of legal persons and arrangements to provide access and obfuscate identity in Singapore's economy. The Assessment Team also focused on regulated sectors that have heightened PF risks with a view to ensuring that they understand their exposure to PF TFS evasion and that preventative measures are in place and prevent PF activity through these exposed sectors, as well as entities unregulated for AML/CFT such as representation offices of foreign flag States.

69. The Assessment Team identified the following areas for decreased focus on sectors covered for AML/CFT requirements that have a lower risk and/or materiality, including non-bank credit card companies, approved trustees for collective investment schemes, direct life and composite insurers, securities depository, licensed moneylenders, pawnbrokers and accountants. The Assessment Team also decreased focus on designated offences with low prevalence and legal persons and arrangements with lower risk and/or materiality.

Materiality

70. Singapore is a wealthy ASEAN member state with the world's 26th largest economy[1] (GDP was about USD 537.68 billion in 2024, +73% since previous MER). The national currency is the Singapore dollar (SGD), which is also accepted as customary tender in Brunei Darussalam. Singapore has had average inflation rate of 1.76% per annum since the FATF's previous onsite visit in 2015[2]. The population stands at about 6.04 million (+11% since last onsite visit), or about 115th largest population in the world, of which approximately 70% (4.2 million) are Singapore citizens and permanent residents[3]. The remaining 30% (1.88 million) are non-residents working, studying or living in Singapore on a non-permanent basis.

71. Singapore has been ranked by the International Monetary Fund as one of 29 systemically important financial centres in the world[4], offering a wide variety of financial products and services and serving a broad and diverse customer base, and has significant international funds flows. At the end of 2024, assets under management in Singapore totalled SGD 6.07 trillion (USD 4.5 trillion) while 77% of assets under management in Singapore were sourced from outside Singapore and 88% of all assets under management were invested outside of Singapore[5].

72. Total currency-in-circulation stood at 9.1 of nominal GDP in 2024. The total value of retail cashless payments (bank transfers, direct debits, card and e-money payments) grew by 18% each year on average over 2021 to 2023. Based on information collected from financial institutions, the value of ATM withdrawals as a percentage of payment transactions has decreased from approximately 8% in 2019 to approximately 4% of in 2023 (based on transaction value).

73. Singapore is one of the busiest ports in the world, as well as a financing, trading and transportation hub, supported by 11 Free Trade Zones (FTZs), as well as several Zero GST Warehouses (ZGW).

[1] World Bank https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?most_recent_value_desc=true

[2] SGD 100 (USD 74) in 2015 would translate to SGD 117.58 (USD 87) at the end of 2024.

[3] Department of Statistics Singapore https://www.singstat.gov.sg/find-data/search-by-theme/population/population-and-population-structure/latest-data

[4] Singapore was included in the list of 29 jurisdictions with Systemically Important Financial Sector by International Monetary Fund in 2013 under the Financial Sector Assessment Program (FSAP). See IMF: Mandatory Financial Stability Assessments under the FSAP

[5] Monetary Authority of Singapore – Asset Management Survey 2024

74. In recent decades, the relative importance of services to the Singapore economy has grown substantially. As at the end of 2024, the services industry contributed more than 73% of the GDP. Within the services industry, the Finance and Insurance sub-sector is the second largest sub-sector by GDP.

Financial sector, VASPs and DNFBPs

75. All FIs, VASPs and DNFBPs identified by the FATF Standards are covered by Singapore's AML/CFT/CPF framework.

76. The details and breakdown of FIs and VASPs are as follows:

Table 0.1. Overview of Financial Institutions (FIs) and VASPs in Singapore

Financial Institution Type	Number of Entities as at 31 Dec. 2024	Licensing / Registration Authority	AML/CFT/CPF Supervisory Authority	Size of Sector as at 31 December 2024
Banks	155	MAS	MAS	Total Assets: SGD 3 862.5 billion
EAMs	197	MAS	MAS	Total Assets under Management (AUM): SGD 123.2 billion
Fund Management Companies (excluding EAMs)	1 023	MAS	MAS	Total AUM: SGD 3 ,125.0 billion
Broker Dealers	180	MAS	MAS	Total Assets: SGD 100.8 billion
Corporate Finance Advisory Firms	27	MAS	MAS	Total Assets: SGD 0.1 billion
Approved Trustees	16	MAS	MAS	Total AUM: SGD 274.2 billion
The Central Depository	1	MAS	MAS	Total Assets Under Custody: SGD 891.7 billion
Insurance Brokers	105	MAS	MAS	Total Assets: SGD 5.3 billion
Financial Advisers	70	MAS	MAS	Total Assets: SGD 1.8 billion
DPTSPs (VASPs)	29	MAS	MAS	Total Transaction Value: SGD 157 billion
PSPs with Cross Border Money Transfer Services	199	MAS	MAS	Total Annual Transaction Value: SGD 515 billion
PSPs without CBMT Services	8	MAS	MAS	Total Annual Transaction Value: SGD 155.4 billion
Money Changers	246	MAS	MAS	Total Annual Transaction Value: SGD 66.2 billion
Non-Bank Credit Card Issuers	4	MAS	MAS	Total Annual Transaction Value: SGD 17.7 billion[6]
Finance Companies	3	MAS	MAS	Total Assets: SGD 19.7 billion
Direct Life and Composite Insurers	25	MAS	MAS	Total Assets: SGD 353.3 billion
Approved Exchanges	4	MAS	MAS	Total Annual Notional Trading Volume: SGD 13.9 trillion
Recognised Market Operators	76	MAS	MAS	Total Annual Notional Trading Volume: SGD 494 trillion
Moneylenders	154	MinLaw	MinLaw	Total Transaction Value: SGD 2.1 billion

[6] Credit and Charge Card Transaction Value

77. In terms of size/business turnover, the DNFBP sectors are relatively small in comparison to the financial sector.

Table 0.2. Overview of DNFBPs in Singapore

DNFBP Type	Number of Entities as at 31 December 2024	Licensing / Registration Authority	Supervisory Authority	Size of Sector
LTCs	65	MAS	MAS	Assets under Trusteeship (2024): SGD 699.8billion
CSPs	3 093	ACRA	ACRA	CSPs account for 75% of incorporation applications[7]
Accountants	4 612 (including 1 259 public accountants)	ACRA and ISCA	ACRA	Revenue (2023): SGD 0.17 billion[8]
PSMDs	2 024	MinLaw	MinLaw	Business turnover (2024): SGD185.5 billion[9]
Pawnbrokers	243	MinLaw	MinLaw	Value of outstanding loans (2024): SGD 1.5 billion
Lawyers	8 075	LawSoc	LawSoc	Percentage of law practice entities that handled at least one relevant matter (2021 – 2023)[10]: 49.1%
Law Practice Entities	1 174 law practice entities	MinLaw	MinLaw	
Casinos	2	GRA	GRA	Casino gaming revenue (2024): SGD 5.28 billion
Real Estate Agents and Salespersons	1 096	CEA	CEA	Value of private property transactions (2024): SGD 62.1 billion
Developers	210	URA	URA	

78. The Assessment Team placed the most weight on the banking sector, given its size, importance, global reach and complexity. It also placed significant weight on PSPs with cross border money transfer services sector, given the large amount of remittance activity, including with some high-risk jurisdictions, DPTSP sector, given the volume and growth of VA-related activities in Singapore, and EAMs, who act as intermediaries for high-net-worth customers and banks for wealth management. For DNFBPs, the Assessment Team placed the most weight on CSPs and LTCs given their important roles as gatekeepers to legal persons and arrangements structures, and PSMDs which are assessed as higher risk.

79. The Assessment Team placed lower weight on sectors covered for AML/CFT requirements that have a lower risk and/or materiality, including corporate finance advisory firms, non-bank credit card companies, approved trustees, insurance brokers, direct life and composite insurers, central depository, approved exchanges and moneylenders. For DNFBPs, the Assessment Team placed lower weight on sectors with lower risk and/or materiality, including pawnbrokers and public accountants (PAs).

Legal persons and arrangements

80. Singapore has an established reputation as a financial centre and trading hub. The country has a high degree of political stability, a pro-business environment and predictable legal system which makes it an attractive location to establish legal persons and arrangements.

7 52 186 companies were incorporated in 2024.

8 Revenue of Corporate Support Services by Accounting Entities in 2023

9 This includes the commodity trades on precious metals reported by PSMDs which accounted for approximately 64% of the 2024 business turnover. These transactions were mostly conducted outside of Singapore.

10 The data was collected by MinLaw in 2024 for the years 2021 to 2023. Relevant matters are defined in section 70A of the Legal Profession Act 1966 and include the situations listed in criterion 22.1(d), which set the threshold of CDD requirements under Recommendation 22. Please refer to https://sso.agc.gov.sg/Act/LPA1966 for the Legal Profession Act 1966.

Legal Persons

81. The table below summarises the legal persons that can be created in Singapore. This includes legal persons without a separate legal personality, aligned with FATF's definition of legal persons.

Table 0.3. Number of Registered Legal Persons in Singapore in 2024

Legal Person	Number of Entities as at 31 Dec 2024
Companies	443 329
Domestic Companies	441 438
Foreign Companies	1 891
Businesses	142 837
Sole Proprietorships	128 937
General Partnerships	13 900
Limited Liability Partnerships	16 709
Variable Capital Companies (VCCs)	1 170
Limited Partnerships	829
Others (comprises societies, cooperative societies and mutual benefit organisations)	8 676

82. Basic and BO information for all domestically created legal persons must be filed with Accounting and Corporate Regulatory Authority (ACRA) except for VCCs who do not have to file BO information. VCCs' BO information is instead available through FIs who may also act as their fund manager. Depending on the basic information required, it is available to the public for a fee, whilst law enforcement can directly access all information within the registry.

83. Foreign legal persons (Unregistered Foreign Companies) that are not regarded as carrying on business in Singapore if they only, inter alia, maintain any bank account or invest any of their funds or hold any property, do not need to be registered with ACRA.

Legal Arrangements

84. There are two types of legal arrangements (as defined by the FATF) which may be created in Singapore:

a) Express Trusts: There exists a variety of types of express trusts in Singapore. These include registered business trusts, collective investment schemes (including real estate investment trusts), the securities depository, and charitable purpose trusts. Further, there are other express trusts which would generally tend to be managed by non-professionals called the "residual trusts".

b) Wakafs: These are Muslim charitable purpose legal arrangements. Legal ownership of all wakaf assets automatically vests in Majlis Ugama Islam Singapore (MUIS) (i.e. the Islamic Religious Council of Singapore), a government statutory board in Singapore. MUIS is also statutorily required to administer all wakafs in Singapore; and is considered by the Courts to be the "trustee-equivalent" for wakafs.

Table 0.4. Number of Legal Arrangements in Singapore in 2024

Legal Arrangement	Number of Entities as at 31 Dec 2024
Express Trusts where the trustee is a Trust Company (established under Singapore law)	7 249
Express Trusts where the trustee is a Trust Company (established under foreign law)	2 985
Registered Business Trusts	15
Collective Investment Schemes (CIS), including Real Estate Investment Trusts (REITs)	1 378 CIS; and 39 REITs
Securities Depository	1

Legal Arrangement	Number of Entities as at 31 Dec 2024
Other express trusts ("residual trusts")	NA
Charitable Purpose Trusts	114[11]
Wakafs	92

85. Legal arrangements (trusts) do not have to file their basic or BO information with a registrar or equivalent: information is held by the trustee, and any reporting entity they have a relationship with and therefore CDD has been conducted. Most trusts are required to use LTC to establish the trust, with the LTC being supervised for AML/CFT compliance.

86. The Assessment Team places the most weight on companies, including foreign companies registered with ACRA and Unregistered Foreign Companies, and lesser weight on other legal persons. Companies present the highest ML/TF risk, are the most material and have had the highest involvement in ML typologies in Singapore. The Assessment Team also placed considerable weight on express trusts where the trustee is a trust company and residual trusts. Lesser weight was placed on wakafs and other types of express trusts due to their lower ML/TF risk and lower materiality.

Structural elements

87. The key structural elements for effective AML/CFT control appear to be present in Singapore. Political and institutional stability, accountability, rule of law and high-level political commitment are all present. Singapore's quality of governance has also been rated positively by the World Bank's Worldwide Governance Indicators[12] (2023):

- Control of Corruption (98.11 percentile rank);
- Rule of Law (98.11 percentile rank);
- Political Stability and Absence of Violence (97.16 percentile rank); and,
- Government Effectiveness (100 percentile rank)

88. Singapore's institutional structure provides it with the necessary framework to implement its AML/CFT regime. Singapore's AML/CFT/CPF efforts are led by a steering committee (the AML/CFT SC), which drives Singapore's policy objectives and directions for combating ML/TF/PF. The AML/CFT SC was formed in 1999 and comprises the Permanent Secretary (PS) of the Ministry of Home Affairs (MHA), PS of the Ministry of Finance (MOF), and Managing Director of the MAS. They are the most senior public servants from the respective agencies.

89. The AML/CFT SC's mandate includes responsibilities to direct the national effort to combat ML/TF/PF; determine Singapore's AML/CFT/CPF policy; oversee the effective co-operation and co-ordination between agencies on the development and implementation of policies and measures to combat ML/TF/PF; and ensure that various agencies have effective mechanisms in place to implement these policies, co-operate and co-ordinate with one another and strengthen Singapore's resilience against ML/TF/PF.

[11] As at end of 2023.

[12] https://www.worldbank.org/en/publication/worldwide-governance-indicators

Background and other contextual factors

90. Singapore approach to combat ML/TF/PF involves a whole-of-society approach, including:

- A mature and sophisticated AML/CFT/CPF regime comprised of mature and sophisticated organisations, including the criminal justice system, regulatory state and administrative regime;
- Established structures across government agencies that maintain close policy and operational co-ordination and co-operation; and,
- Close engagement, partnership and collaboration with private sector entities.

91. Singapore features a low level of corruption, low exposure to regional instability and limited exposure to violent domestic organised crime.

AML/CFT/CPF strategy

92. Singapore's whole-of-government approach to combat ML/TF/PF is led by the AML/CFT SC. The most recent AML strategy, published in 2024 sets out policy objectives to (i) maintain an effective, risk based and proportionate AML framework, so as to support Singapore's position as a trusted, attractive, open and dynamic financial centre and business hub, and (ii) protect Singapore's system from illegal activities and illicit fund flows. The strategy has three key pillars (Prevent, Detect and Enforce) supported by effective whole-of-society collaboration and co-ordination, a sound and comprehensive legal and regulatory framework, and close international co-operation with other jurisdictions.

93. Singapore has also published a law enforcement-specific Strategy to Combat ML, the National Strategy for Countering the Financing of Terrorism, the National Counter-Proliferation Financing Strategy and the National Asset Recovery Strategy that build on the above objectives.

Legal and institutional framework

94. The CDSA (primary AML legislation) and TSOFA (primary CFT legislation) serve as the legal foundation for Singapore's AML/CFT/CPF regime. AML/CFT/CPF efforts involve co-ordination between various government bodies and the private sector. The following key authorities are responsible for AML/CFT/CPF efforts in Singapore:

Ministries

- **The Ministry of Home Affairs (MHA)** is in charge of maintaining law and order as well as internal security in Singapore. MHA oversees the various LEAs, including the SPF, Commercial Affairs Department (CAD), which is a part of the SPF, and CNB. In respect of the AML/CFT policy/regime, the Ministry has responsibility for the relevant legislation, chiefly the CDSA (which gives LEAs the powers to deal with ML offences), as well as the TSOFA (which gives effect to Singapore's obligations under the International Convention for the Suppression of the Financing of Terrorism).
- **The Ministry of Finance (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. The main regulatory statutes under the MOF are the Companies Act 1967, Business Names Registration Act 2014, Corporate Service Providers Act 2024 and Accountants Act 2004.
- **The Ministry of Law's (MinLaw)** mission is to advance access to justice, the rule of law, the economy and society through policy, law and services. In the area of international co-operation to combat ML/TF, MinLaw is responsible for the Mutual Assistance in Criminal Matters Act 2000, the Extradition Act 1968 and the United Nations Act 2001.

- **The Attorney-General's Chambers (AGC)** is the principal legal adviser to the Government on all legal matters, whether relating to domestic or international law. The AGC is Singapore's Central Authority for MLA in criminal matters and is also in charge of processing extradition requests. On the domestic front, officers from the AGC advise the Government on the interpretation and application of domestic law, including by representing the Government in domestic litigation, and are also responsible for drafting Singapore's laws, including legislative amendments. The Attorney-General is also the Public Prosecutor of Singapore. The Constitution vests in the Public Prosecutor complete discretion to institute and conduct proceedings for any criminal offence, including those relating to ML/TF. In this capacity, Deputy Public Prosecutors from the AGC apply for and defend seizure of assets made pursuant to domestic investigations.

Criminal justice and operational agencies

- **The Singapore Police Force (SPF)** is one of three LEAs investigating ML for serious offences under its remit. As the lead ML enforcement agency, SPF also investigates into ML arising from foreign predicate, and ML arising from serious predicate offences enforced by other predicate agencies including tax ML, trade-based ML and illegal wildlife trafficking. Within SPF, complex ML is investigated by two specialist investigation departments – the CAD and the Criminal Investigation Department (CID). TF offences also come under SPF's purview and are investigated by CAD.
- **The Suspicious Transaction Reporting Office (STRO)** is Singapore's FIU and serves as Singapore's central agency for the receipt of STRs and other reports filed under the CDSA.
- **The Corrupt Practices Bureau (CPIB):** CPIB is Singapore's sole anti-corruption agency under the Prime Minister's Office that investigates bribery and bribery-related CDSA offences. The Investigation Department in CPIB is responsible for all incoming formal MLA requests routed to the Bureau by the AGC. The Investigation Department is supported by the International Affairs & Liaison Branch under CPIB's Operations Department. The IAL branch received and assesses all incoming informal agency-to-agency requests from foreign counterpart agencies and relevant authorities. The Operations Department also has an Intelligence Division which assesses referrals made by STRO.
- **The Central Narcotics Bureau of Singapore (CNB)** is the lead law enforcement agency that handles drug ML investigations as well as drug investigations and the concurrent financial investigation linked to drug offenders in Singapore.
- **Immigration and Checkpoints Authority (ICA)** is responsible for the security of Singapore's borders against the entry of undesirable persons and cargo through its land, air and sea checkpoints. As part of the border security functions, ICA acts on behalf of competent authorities to enforce their declaration regimes, such as the cross-border cash reporting regime, at the checkpoints. Apart from border security functions, ICA also performs immigration and registration functions such as the issuing of travel documents and identity cards to Singapore citizens.
- **The Internal Security Department (ISD)** is Singapore's domestic security and intelligence agency and Singapore's lead agency for investigating terrorism cases. All officers in ISD's Counter-Terrorism Division are also involved in TF-related work, which includes conducting TF probes, sharing and exchanging TF information with both its local and foreign counterparts to keep abreast of the evolving TF landscape and to enhance collaboration in detecting and investigating TF threats.

Supervisory authorities

- **The Monetary Authority of Singapore (MAS)** is Singapore's central bank and has a broad range of powers to supervise and monitor compliance of FIs, VASPs and LTCs with AML/CFT requirements, including powers of off-site surveillance, auditing and on-site visits and examinations. MAS is also empowered under the various regulatory statutes to issue directions to FIs, including the legal

obligations to take preventive measures to help mitigate the risk of Singapore's financial system being used for ML/TF.

- **Singapore's Ministry of Law (MinLaw)** supervises, monitors and ensures that moneylenders, PSMDs, pawnbrokers and law practice entities (LPEs) comply with AML/CFT requirements. MinLaw has the powers to perform off-site monitoring, on-site examinations and supervisory visits to examine their policies, procedures and controls, and to ensure compliance with requirements for the prevention of ML/TF.
- **The Gambling Regulatory Authority (GRA)** has a range of powers to perform supervision and monitoring of casinos to ensure compliance with AML/CFT requirements. GRA is also empowered under the Casino Control Act 2006 to issue direction to casinos to take preventive measures to mitigate ML/TF risks.
- **The Accounting and Corporate Regulatory Authority (ACRA)** is empowered to register, supervise, monitor and ensure that CSPs and accountants are in compliance with AML/CFT requirements.
- **The Council for Estate Agencies (CEA)** conducts examinations and investigations into real estate agents (EAs) /salespersons (RESs) to ensure compliance with the Estate Agents Act 2010 and its subsidiary legislations. This includes issuing directions to the industry such as how to implement preventive measures to mitigate ML/TF risks.
- **The Urban Redevelopment Authority (URA)** audits developers on their compliance with the AML/CFT requirements set out in the legislation, including performing CDD measures on purchasers, reporting suspicious transactions, implementing internal policies, procedures and controls to assess their ML/TF risks and put in place the appropriate measures to mitigate the ML/TF risks and record keeping.

Co-ordination and Co-operation Arrangements

- **AML/CFT Steering Committee (AML/CFT SC):** In 1999, Singapore established the AML/CFT SC, comprising the PS (Home Affairs), PS (MOF) and Managing Director of the MAS, to determine broad policy objectives for combating ML/TF. This Committee leads the national effort to develop and implement Singapore's AML/CFT regime.
- **Inter-Agency Committee (IAC):** The IAC supports the AML/CFT SC as the main operational body that co-ordinates the implementation of the national AML/CFT policy. The IAC comprises Singapore's key AML/CFT agencies who meet regularly to share information on ML/TF and proliferation financing threats and trends, as well as discuss cross-cutting policy issues.
- **Risk, Typologies Inter-Agency Group (RTIG):** RTIG was established in 2017 as the main working level body tasked with the identification, assessment and understanding of ML/TF/PF risks. Through the RTIG, agencies share information such as emerging ML/TF/PF threats and trends, FATF typologies, best practices and other developments.
- **AML Case Co-ordination and Collaboration Network (AC3N):** AC3N facilitates the development, prioritisation, and co-ordination of significant ML cases across agencies, including law enforcement and supervisory authorities.
- **Inter-Ministry Committee on Export Controls (IMC-EC):** The IMC-EC oversees Singapore's export controls framework, including relevant policy and operational issues relating to the proliferation of WMD and PF. In addition, the IMC-EC co-ordinates interagency follow-ups (including enforcement action by LEAs) when Singapore receives information or intelligence relating to the proliferation of WMD and PF. The AML Case Co-ordination and Collaboration Network (AC3N) deals with (non-export controls) PF cases surfaced by AC3N agencies and would consult and co-ordinate with the IMC-EC as necessary.

- **Inter-Ministry Committee on Counter Terrorism (IMC-CT):** The IMC-CT is mandated to comply with international requirements to combat terrorism and to strengthen its national capacity to implement measures to combat international terrorism, including terrorist financing.
- **Inter-Ministry Committee on Terrorist Designation (IMC-TD):** The IMC-TD is the competent authority for proposing terrorist designations pursuant to UNSCRs 1267/1989, UNSCR 1988, and UNSCR 1373. The IMC-TD ensures that information relating to terrorist designation is disseminated and the relevant CFT measures are enforced.
- **Inter-Ministry Committee on Scams (IMC-Scams)**: The IMC-Scams brings together a range of agencies covering law enforcement and supervisory agencies in relation to the financial and telecommunication sectors and to work with the private sector partners to co-ordinate efforts to combat CEF, including the threat of ML offences.

Preventive measures

95. Singapore extends preventive measures requirements to all sectors and activities covered under the FATF Standards. The Financial Services and Markets Act 2022 (FSM Act) is the enabling legislation for the sector-wide regulation of financial services and markets (except moneylending activities, which are governed under the Moneylenders Act 2008) and VASP activities. Each DNFBP sector is subjected to AML/CFT requirements through the respective sector-specific statute/regulations. The CDSA (primary AML legislation) and TSOFA (primary CFT legislation) apply to all financial institutions, VASPs and DNFBPs and cover obligations such as STR reporting and tipping-off. MAS' Financial Services and Markets Regulations (for FIs supervised by MAS), Variable Capital Companies (VCC) Regulations and the UN Regulations (for the general public, including DNFBPs and moneylenders) are the enabling legislation for provisions in relation to targeted financial sanctions pursuant to UNSCRs against the DPRK.

Supervisory arrangements

96. Singapore supervises all sectors and activities covered under the FATF Standards. MAS is an integrated regulator and supervisor of the financial sector that administers the various statutes pertaining to FIs (other than moneylenders, which are supervised by MinLaw), and VASPs. Each DNFBP sector is regulated for AML/CFT by its licensing/registration authority or self-regulatory body. Table 0.2 above shows the authorities responsible for AML/CFT supervision of the various DNFBPs.

97. Legal persons created in Singapore are required to register with ACRA. Foreign-created legal persons created in another jurisdiction that have sufficient links to Singapore are required to be registered with ACRA. Foreign-created legal persons are able to conduct certain activities (e.g., opening/holding a bank account, investing funds, holding property) in Singapore without meeting the criteria to be registered with ACRA.

98. There are two types of legal arrangements that can be formed under Singapore law; express trusts and wakafs. The various types of express trusts have their information held by the trustee, and any reporting entity they have a relationship with and therefore CDD has been conducted. Most trusts are required to use an LTC to establish the trust, with the LTC being supervised for AML/CFT compliance. All wakafs must be registered with MUIS, which maintains a register of wakafs. Further, MUIS being the administrator of all wakafs.

International co-operation

99. Singapore's Mutual Assistance in Criminal Matters Act 2000 (MACMA) permits the provision of a wide range of assistance, including several types of assistance without the need for an MLA treaty to be in force between the requesting country and Singapore so long as there is an undertaking of reciprocity. STRO

is a member of the Egmont Group, and uses the Egmont secure platform for information exchange, while LEAs leverage platforms like INTERPOL to apprehend criminals and repatriate assets.

100. Singapore plays an active role in regional co-operation initiatives, such as a multi-jurisdictional anti-fraud project with Indonesia and Malaysia under the ambit of the Financial Intelligence Consultative Group (FICG).[13] Singapore is also a member of the Association of Southeast Asian Nations (ASEAN). Singapore's key international partners are, within Asia, China (including Hong Kong, China), India, Indonesia and Malaysia, and outside Asia, the United Kingdom and the United States.

[13] The FICG is a regional body of FIUs from ASEAN 10, New Zealand and Australia.

1 Assessment of risks, co-ordination and policy setting

The relevant Immediate Outcome considered and assessed in this chapter is IO.1. The Recommendations relevant for the assessment of effectiveness under this chapter are R.1, 2, 33 and 34 and elements of R.15.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Singapore employs a dynamic approach to identifying and assessing ML and TF risks, which has led to a reasonably sound understanding of its ML and TF risks. However, there is no identification of the relative importance of ML/TF risks in Singapore's environment when particular risks are identified, assessed and mitigation plans put into place.

b) Singapore's ML and TF NRAs are a synthesis of the findings made through the dynamic approach but lack some nuance and detail in certain risk areas, such as cross border flows and TBML. They bring together the risk findings and various risk assessments from the 10-year period for the ML NRA and 4-year period for the TF NRA into one consolidated public document. The dynamic approach is an agile approach that allows Singapore to identify changes in risks but is an approach that identifies and assesses individual risks on a case-by-case basis without prioritisation. Singapore has not committed to updating the ML or TF NRAs in a particular time period and relies on discussions at the Risk, Typologies Inter-Agency Group (RTIG), Inter Agency Committee (IAC) and Steering Committee (SC) to ensure its risk understanding is up to date.

c) Singapore demonstrates strong political commitment and has established robust governance structures to address ML/TF risks. Its dynamic approach is centrally co-ordinated through whole-of-government mechanisms. However, there is a lack of systematic connection and prioritisation between risk identified in NRAs and the national AML/CFT strategies, which also did not include specific actions, deliverables and implementation timeline. Mitigation efforts are applied to individual risks as they arise without a comprehensive view of the overall risk landscape and the relative seriousness of the risk being addressed, though there is no indication of Singapore having an inadequate response to one of its highest ML/TF risk, cyber enabled fraud (CEF).

d) Enhanced measures are well-developed and effectively applied in higher-risk scenarios, including dealings with complex legal persons, DPTSPs, and high-risk jurisdictions.

Singapore's legal framework allows SDD and exemptions in lower risk areas, Singapore adopts a cautious approach to: (i) simplified measures, which is reasonable, and (ii) exemptions.. This reflects a broader weakness in Singapore's dynamic approach, which tends to prioritise higher risks flagged by authorities but lacks mechanisms to consistently identify and assess lower-risk scenarios for simplified measures/exemptions.

e) Singapore's competent authorities are actively engaged in the risk identification process with objectives generally aligned to identified risks, though there remain some inconsistencies in operational alignment and supervisory coverage. Agencies indicate that they are well-resourced, although there can be a better overarching mechanism to ensure consistency in supervision across sectors in practice. Singapore has taken a more intensive approach for some areas of lower risk in consideration of their broader regulatory objectives beyond AML/CFT concerns, which may not be in line with the relative ML/TF risk exposure.

f) Singapore's AML/CFT/CPF system is underpinned by extensive domestic co-ordination and co-operation through high-level and working-level committees that ensure cross-agency collaboration, policy alignment, and risk monitoring, supported by subject-specific interministerial committees (IMCs). The system reflects a well-integrated whole-of-government approach, with active engagement from supervisory authorities and industry associations.

g) Singapore has strong operational co-ordination and co-operation mechanisms, including AC3N and the AML/CFT Industry Partnership (ACIP), which facilitate inter-agency and public-private collaboration on AML/CFT efforts. Technical tools like National AML Verification Interface for Government Agencies' Threat Evaluation' (NAVIGATE) and Collaborative Sharing of ML/TF Information & Cases (COSMIC) enhance data sharing and tactical co-operation. These frameworks have led to effective case co-ordination and improved risk understanding, making policy co-operation a key strength of Singapore's AML/CFT regime.

Recommended Actions

Singapore should:

a) Ensure the NRA process, or other means of understanding of risk, provides a comprehensive and current understanding of the ML/TF risk landscape to better inform a risk-based approach to AML/CFT activities.

b) Implement a systematic and prioritised method of identifying and tracking risk-responsive mitigation measures with specific actions, deliverables and implementation timelines.

Overall Conclusions on IO.1

Singapore has a reasonably sound understanding of its ML/TF risks and demonstrates strong political commitment and co-ordination through a dynamic approach that enables agile responses to emerging threats. The 2024 NRAs aggregate the findings of the dynamic approach to arrive at a generally sound conclusion but lack some nuance and detail in certain risk areas, such as cross border flows and TBML. NRAs are not updated at regular intervals and Singapore relies on discussions at RTIG, guidance and ongoing engagements with the private sector to ensure an updated risk understanding. However, the dynamic approach is an approach that identifies and assesses individual risks on a case-by-case basis, and there can be better consideration of the relative importance of ML/TF risks in Singapore's environment when particular risks are identified, assessed and mitigation plans put into place. The mechanism to scan the risk horizon and anticipate new risks can however be improved. Connection and prioritisation between risk identified in NRAs and the national AML/CFT strategy documents which also did not include specific actions, deliverables and implementation timelines can also be improved.

Enhanced due diligence measures are applied in high-risk scenarios. Singapore adopts a cautious approach, which is reasonable, but the assessment team notes the lack of mechanisms to consistently identify and assess lower-risk scenarios for simplified measures/exemptions. Competent authorities are actively engaged, though there remain some inconsistencies in operational alignment and supervisory coverage. Agencies indicate that they are well-resourced, although there can be better overarching mechanism to ensure consistency across sectors in practice, and some supervisors had leveraged on their broader supervisory mandate to have more extensive supervisory coverage in the lower risk sectors. Singapore's AML/CFT regime benefits from extensive operational co-ordination and strong policy co-operation, supported a public-private partnership that enhances risk understanding, policy implementation case co-ordination.

Overall, the deficiencies identified in Singapore's system are limited in number and were considered to be of some importance to the effectiveness of Singapore's system. Moderate improvements in the few identified aspects are warranted.

Singapore is rated as having a Substantial level of effectiveness for IO.1.

Immediate Outcome 1

101. Since the 2016 MER, Singapore has established a number of co-ordination mechanisms to enhance its whole-of-government (WoG) approach in combatting ML, TF and PF risks. Singapore has retained the AML/CFT SC and IAC to steer the AML/CFT regime and supplemented these mechanisms with the RTIG in 2017. The RTIG is Singapore's key mechanism to identify, assess and understand ML/TF risks, discuss typologies and trends, and facilitate and support supervisory and enforcement policies and approaches in line with risk. Singapore established its public-private partnership, ACIP, in 2017 and the AC3N in 2024 (replacing the Inter-Agency Suspicious Transaction Report Analytics Taskforce (ISTRA) established in 2018) for inter-government case co-ordination.

102. Singapore published separate ML, TF and PF NRAs in 2024, following its last ML NRA in 2014[14]. Singapore uses a '*dynamic approach*' to risk assessment and understanding, and it has completed a number of thematic and sectoral risk assessments across the reporting period to identify ML/TF risks. The most significant shift in Singapore's risk and context since the 2016 MER has been the proliferation of fraud, particularly CEF, and the subsequent WoG efforts dedicated to combatting CEF. Singapore's other ML/TF risks and contextual factors remain largely the same as the 2016 MER.

1.1. Country's identification, assessment and understanding of its ML/TF risks

1.1.1. ML/TF risks

103. Singapore has a reasonably sound understanding of its ML and TF risks, as consolidated in the 2024 ML and TF NRAs and various risk products over the intervening period between the 2014 NRA and the 2024 updates.[15] Singapore was not able to provide a definition of the *dynamic approach* during the Assessment Team's onsite visit, but the approach is generally understood by the competent authorities as ongoing risk surveillance and monitoring, and deep dive reviews into specific risk areas and/or emerging risks as co-ordinated by RTIG. The Assessment Team understands the dynamic approach is an iterative, co-ordinated and agile method of identifying and assessing risks, thereby developing and updating the national ML/TF risk understanding. Risks are considered as competent authorities identify them to various inter-agency committees, notably RTIG, that ultimately report to the AML/CFT SC.

104. Under the dynamic approach, Singapore has various approaches/channels to assess risks, including (i) regular engagements of industry experts and practitioners (including through ACIP), (ii) data analysis on STRs and crime information from LEAs, (iii) monitoring international developments, trends and typologies through international and regional reports, and (iv) engagements and surveys of its key foreign law enforcement and FIU partners. Singapore provided a few examples where authorities (e.g. STRO) deployed the above approaches to assess risks associated with particular sectors (e.g. real estate sector) or typologies (e.g. misuse of legal persons), but mechanisms for horizon scanning, forward-looking modelling or scenario analysis for future risks can be improved. The dynamic approach allows Singapore to respond quickly to emerging new risks by convening the RTIG and discussing the relevant issue with all relevant parties, whether it is new threats, geopolitical shifts, or changes in macro customer behaviours. It is, however, an approach that identifies and assesses individual risks on a case-by-case basis as they arise in the environment. For instance, when the RTIG/IAC reviewed and rerated the ML risk of the real estate sector considering the rising threat in relation to real estate market and size of the sector, the assessment seemed to focus primarily on real estate agents and developers. While risks of the legal sector in relation to conveyancing services were considered, the rating was not amended as the sector was considered to have more mature AML/CFT regime and stronger risk awareness. As revealed from the 3B$ case, several LPEs were involved in and sanctioned for the purchase of real estate properties in question. The AT considers this was a missed opportunity to holistically consider the risk implications on different sectors when assessing the rising threat related to the real estate sector.

105. While RTIG/IAC has had discussions on sectoral risk ratings and key threats at different intervals during the assessment period, such discussions did not result in any regular and comprehensive update on overview of risks facing Singapore. Singapore brings to bear data and expertise available to assess risks, but there is scope to adopt a more systematic and better documented approach to risk reviews conducted by RTIG to ensure clear communication of a consistent risk overview to all relevant stakeholders. There is

[14] The 2014 NRA considered ML and TF risks together.

[15] This includes the thematic risk assessments developed by the RTIG, including: (i) Legal Persons (2019, refreshed in 2024); (ii) Virtual assets (2020, refreshed in 2024); (iii) Environmental Crime ML (2024); (iv) Legal Arrangements (2024); and TF NPO Risk Assessment (2019).

no identification of the relative importance of ML/TF risks in Singapore's environment when particular risks are identified, assessed and mitigation plans put into place. Singapore has not committed to updating the ML or TF NRAs in a particular time period and will rely on the discussions at RTIG to ensure its risk understanding is comprehensive and up to date.

106. The 2024 ML and TF NRAs are a synthesis of the findings made through the *dynamic approach*, bringing together the various risk assessments from the 10-year period for the ML NRA and 4-year period for the TF NRA into consolidated public documents. These documents synthesise the findings made through the *dynamic approach* and give relative criticality to the risks. Singapore identifies its ML and TF risks in its 2024 NRAs as follows:

Table 1.1. 2024 ML and TF NRA Findings

	ML NRA	TF NRA
Overall Finding	**Key ML Threats:** Fraud (particular CEF) Organised Crime (especially illegal gambling with foreign organised criminal groups) Corruption Tax Crimes TBML **Other Notable ML Threats:** Environmental crime Cyber-crime Drug-related offences	**Overall National TF Risk:** Medium-Low
Sector Risk Rating	**Sectors (ML)**	**Sectors (TF)**
High Risk	Banks	Money remittances, including: - Unlicensed money remittances - Cross-border online payments
Medium-High Risk	DPTSPs PSPs with CBMT Services EAMs LTCs CSPs EAs/RES/ Developers Casinos PSMDs	Banks, including: - New cross-border fast payment systems DPTSPs
Medium-Low Risk	Fund Management Companies (excluding EAMs) Money Changers PSPs without CBMT Services Broker Dealers and Corporate Finance Advisory Firms Moneylenders Lawyers Accountants	Non-profit organisations, including - Online fundraising Cross-border cash movement PSMDs
Low Risk	Non-Bank Credit Card Companies Approved Trustees Finance Companies Direct Life and Composite Insurers Securities Depository Financial Advisers (including insurance brokers) Pawnbrokers	Other AML/CFT regulated sectors not featured in the TF NRA report

107. Singapore's ML and TF NRAs assessed sectoral risks based on a function of threats (taking into account consequences and impact), vulnerabilities and controls. Singapore adopted a residual risk model across all sectors but decided to place greater emphasis on threats and vulnerabilities, while less emphasis is accorded to the mitigating effect of controls where they are assessed to be strong. Where controls are

assessed to be weak, the sector's residual vulnerability would be heightened due to the lack of effective risk mitigation. All sectors with AML/CFT obligations are assessed in the NRA, as are all serious crimes.

108. For the ML NRA, ML threats are assessed using five guiding parameters: domestic and foreign crime landscape, materialised ML activity, Singapore's inherent exposure to crime, propensity for laundering proceeds in Singapore, and perspectives from foreign partners. Indicators considered includes convictions of predicate offences, quantum of proceeds of crime involved, STRs tagged to predicate offences, as well as formal and informal international co-operation requests. While investigation and prosecution of predicate offences are taken into consideration, Singapore placed a higher focus on predicate convictions. Sectoral vulnerabilities are evaluated based on (i) exposure to identified threats, (ii) likelihood of threat materialisation, and (iii) the maturity of AML/CFT controls.

109. The TF NRA evaluates the likelihood of TF activities and Singapore's use as a transit point, based on indicators such as regional terrorism/TF activity, terrorism/TF requests for assistance, MLA requests, and TF investigations. Sectoral TF vulnerabilities are analysed through collaboration with regulators and supervisors, considering product and service risks, industry feedback, and Singapore's contextual factors such as its financial hub status, migrant population, and digital economy. Insights from FATF and international partners further enhance the understanding of TF typologies and risks.

110. Although Singapore draws on insights from FATF and international partners to strengthen its understanding of TF typologies and risks, these insights can be better contextualised within its own framework to integrate them into a dynamic and adaptive approach. In particular, organisational TF has not been adequately considered in the context of Singapore's role as a global financial centre.[16]

111. While authorities have taken steps to mitigate risks associated with the misuse of legal persons and have sought to gauge potential exploitation of their financial centre through global feedback, further measures are needed. Specifically, Singapore should investigate organised TF networks and concealed income, given its global significance as a hub for finance, trade, and company formation.

112. The Secretariat of the RTIG (comprising MAS and MHA), co-ordinates the review of risks and leads the drafting of the NRAs. Both NRAs have a generally justified scoring matrix and framework that sits beneath it, which is structured, data-driven and prioritised. The conclusions of the NRAs are clear and agreed across different competent authorities. The findings from the ML and TF NRAs and other risk assessments are communicated across government agencies and private entities through publication on websites and issuance of guidance. FIs/VASPs interviewed onsite generally showed reasonable knowledge of the NRAs, with an uneven understanding of ML/TF and PF risks in some DNFBP sectors. This WoG approach is a key strength of Singapore's ML and TF NRA processes.

113. The 2024 ML and TF NRAs reach appropriate conclusions in most cases. However, some methodological adjustments could be made for sharper assessment of risks. For example, while Singapore's understanding of geographic risk in relation to ML/TF is reasonable, it could be enhanced by more granular analysis of geographic risks mapped against predicate crime types and contextualised for Singapore. In particular, the private sector reported that they use their own geographic lists that are more detailed and extensive than the advice provided by the Singaporean authorities.

114. For example, it is well acknowledged from Singaporean authorities that most illicit funds are foreign-sourced, but the NRA lacks detailed mapping of high-risk jurisdictions and transaction patterns specific to cross border flow of funds. There is scope for Singapore to enhance its understanding of risks from cross border transactions, especially in relation to cash transactions by money mules. TBML is acknowledged as a key ML threat, but there is limited empirical data on its scale and typologies in

[16] FATF – Comprehensive Update on Terrorist Financing Risks, see Sections 7 and 8 (hyperlinked from the contents), particularly paragraphs 237 and 396.

Singapore's massive trade ecosystem. There is also no detailed mapping of high-risk trade routes, commodity vulnerabilities, or financial instruments used in TBML schemes.

115. Singapore indicated that quantitative data and qualitative indicators are accorded equal weights in risk assessments, though there does not appear to be a systematic and clearly communicated mechanism on how these different sources are weighed or reconciled. In practice, it appears that qualitative indicators may sometimes take precedence over quantitative and operational information, and result in a higher threat rating even if the number of cases may not be significant. Singapore has made good efforts to address previously identified gaps, particularly by incorporating more international typologies and foreign requests for assistance. However, this may have come at the cost of a lesser focus on understanding of domestic risks, for example the risk posed by complex legal arrangement/person structures, and risks within the legal sector.

116. While Singapore takes into consideration quantitative, operational data in its formulation of NRA findings, the TF NRA is heavily reliant on international and regional typologies and their applicability to Singapore's risk and context. Singapore has made concerted efforts to consider the risks associated with "unknown unknowns", such as external organisational terrorist financing, through its 2024 TF Risk Perception Survey conducted with 41 FATF members, regional, and high TF risk jurisdictions. The overall TF risk ratings are justified.

117. While Singaporean agencies and private sector representatives demonstrated a reasonably sound risk understanding that aligned with, and in some cases, went beyond, the findings of the ML and TF NRAs, there remained some inadequacies in comprehensiveness and granularity as well as consolidated documentation for communication of a common understanding in Singapore's dynamic approach to risk understanding.

1.2. National policies and activities to address identified ML/TF risks

1.2.1. Policies and activities to address ML/TF risks

118. Singapore demonstrates strong political commitment, as well as strong co-ordination and governance mechanisms to co-ordinate policy and activities to address what it identifies as the highest ML/TF risks, found through its dynamic approach. These policies and mechanisms are overseen by the AML/CFT SC, which is chaired by PS of the MHA, PS of the MOF and Managing Director of the MAS.

119. In 2024, Singapore released national-level AML/CFT strategy documents (the Strategies) together with the respective NRAs. As the NRAs are aggregations of the risks assessed through the dynamic approach, the Strategies set out the key high-level prongs of the mitigation measures that have been implemented. Singapore tracks progress against the mitigation measures (including those highlighted in the Strategies) through the RTIG and AML/CFT SC/IAC mechanism. The National AML Strategy highlights a three pillar, three building block approach to prevent, detect and enforce ML (see Box 1.1).

Box 1.1. Singapore's National AML Strategy

Singapore published the National AML Strategy on 30 October 2024 to set out its ongoing approach to addressing ML risks. Singapore's National AML Strategy, which expands upon Singapore's 2016 National Policy Statement on ML/TF, comprises three key pillars:

- **Prevent** – to deter proceeds of crime from entering Singapore's system and prevent the misuse of Singapore's system by criminals;
- **Detect** – to identify illicit flows and activities and ensure timely and effective mitigation, disruption and enforcement actions; and
- **Enforce** – to take firm and dissuasive actions against persons who abuse Singapore's system for ML.

These three pillars are in turn supported by three inter-dependent building blocks of (i) Whole-of-Society Co-ordination and Collaboration; (ii) Legal and Regulatory Framework; and (iii) International Co-operation, which form the foundation of Singapore's AML framework.

120. The National AML Strategy sets out non-specific actions for Singapore that were in train or have been implemented to address risks that were identified in the dynamic approach. More than half of the actions begin with the term 'continue' and are non-specific, i.e., "continue to leverage on international co-operation and provide timely and quality assistance to actively tackle ML activities" or "continue to enhance effectiveness of risk-based supervision", and do not draw specific linkages to the risk findings in the NRA.

121. The National CFT Strategy also highlights a three pillar, five prong approach, as summarised in Box 1.2:

Box 1.2. Singapore's National Strategy for CFT

Singapore refreshed its National Strategy for CFT, alongside a refresh of Singapore's TF NRA on 1 July 2024, to underpin Singapore's national approach towards addressing its TF risks. Like the National AML Strategy, the National Strategy for CFT comprises three thrusts:

- **Prevent**: Proactively deter prospective terrorists, terrorist organisations, and sympathisers from exploiting Singapore's open economy for TF activities;
- **Detect**: Promptly identify and trace TF activities through robust monitoring and tracking of red flag indicators, especially in high-risk sectors, and emerging TF typologies of concern; and
- **Disrupt**: Take strong and resolute actions against terrorists, terrorist organisations, and sympathisers seeking to raise, move and use funds for terrorism activities, both locally and abroad.

Singapore achieves these objectives through its five-pronged National Strategy for CFT:

- Co-ordinated and Comprehensive Risk Identification;
- Strong Legal and Sanctions Framework;
- Robust Regulatory Regime and Risk Targeted Supervisory Framework;
- Decisive Law Enforcement Actions; and
- International Partnerships and Co-operation.

122. As with the National AML Strategy, the National CTF Strategy demonstrates a general strategy already in action through initiatives that were undertaken since the last publication of the National CFT Strategy in 2022. It also sets out forward looking non-specific actions for Singapore that, largely, they were already undertaking prior to the development of the strategy.

123. The Strategies do not illustrate any direct connection between the mitigation measures that are put into place and the relative level of risks in Singapore. The dynamic approach considers mitigation measures when individual risks arise, and there can be better consideration of the entire risk landscape or environment in Singapore. The holistic risk picture and landscape and/or future risks may not be adequately identified or mitigated, unless raised by a relevant agency. Singapore applies a very high level of resources, expertise and mitigation measures against fraud (particularly CEF), as compared to other higher threats (e.g. corruption, tax ML, etc.). Singapore explained the differences was due to the pervasive and fast-evolving nature of fraud and exponentially growing cases, whereas other threats, though considered high risk, have more stable typologies and are addressed through targeted measures.

124. There is no consolidated document that maps out the measures for different threats under the prevent, detect and enforce pillars to set out the timelines, agency responsibilities, specific deliverables. Singapore relies on regular discussions at RTIG, IAC and SC for deciding actions for responsible agencies and/or specific deliverables to mitigate the ML/TF risks identified. Based on the high-level principles in the Strategies, individual agencies develop risk mitigation measures and action plans which are discussed and approved by RTIG, IAC and SC. Agencies report to the RTIG, IAC and SC on progress of actions they are taking to address risk, but there is no centralised reporting timescale.

125. Although national policies and activities in Singapore are not systematically driven by identified ML/TF risks at all times, there is no indication of Singapore having an inadequate response to one of its highest ML/TF risks, CEF. Competent authorities demonstrated strong alignment and commitment to achieving collective AML/CFT objectives and Singapore has implemented very strong national policies and activities. To mitigate the very high level of risk of ML from CEF, Singapore is taking an innovative, WoG approach (see Box 1.3).

Box 1.3. Singapore's monitoring and mitigation of risks related to CEF

In response to the surge in CEF cases, Singapore set up the IMC-Scams in April 2020. Chaired by the Minister for Digital Development and Information and the Minister of State for Home Affairs, the IMC-Scams comprises a range of agencies including MHA, SPF, and regulatory agencies of the financial and the telecommunication sectors. The IMC-Scams meets regularly to discuss the latest scam trends and typologies, as well as strategies to combat CEF and associated ML activities. Through this channel, Singapore released its anti-scams strategy, which aims to: (i) prevent and block syndicates from abusing its telecommunications infrastructure, financial systems and online spaces to target scam victims; (ii) facilitate the reporting and detection of scams; (iii) take enforcement action against scammers and ML enablers; and (iv) recover scam proceeds.

Singapore combats online scams through strong legislation, industry collaboration, and real-time enforcement. The 2023 Online Criminal Harms Act empowers authorities to block criminal content and requires scam mitigation measures, such as user verification. MAS and IMDA work with banks and telecommunication companies to deploy tools like "Kill Switch", which allows banking customers to suspend their accounts quickly if compromised, "Money Lock", which allows bank customers to set aside an amount in their bank accounts which cannot be transferred out digitally, and scam call blocking. The 2025 Protection from Scams Act further empowers LEAs by allowing them to issue Restriction Orders (i.e. limiting legitimate use of a person's bank account when he/she is suspected of being a scam victim).

Reporting has improved through ScamShield mobile application, which allows the public to report suspected scam calls and messages, and a 24/7 anti-scam hotline. Agencies also consolidated advisories on the latest scam trends, steps to take if someone has been scammed, and preventive measures to avoid being scammed into a ScamShield website. Enhanced fraud detection systems help reporting entities identify suspicious transactions using insights from SPF. Amendments to CDSA and the Computer Misuse Act 1993 in 2023 expanded authorities' toolkit for dealing with ML suspects who wilfully claim ignorance and to criminalise actions of scammers who abuse SingPass to perpetrate scams and other crimes introduced offences against those aiding ML and recommended stiffer sentences. In August 2024, the Sentencing Advisory Panel also recommended harsher imprisonment sentences for those who hand over control of their payment accounts or SingPass credentials to scammers to facilitate ML from scams.

To recover stolen funds, SPF's Anti-Scam Centre and Project Frontier swiftly freeze compromised accounts. In the first half of 2024, over 10 300 bank accounts and mobile lines were blocked, recovering SGD 54 million (USD 39.9 million).

126. The focus on ML from fraud, particularly CEF (see IO.7) is partly aligned with Singapore's context and risk environment and shows the strength of the dynamic approach. CEF is a fast-moving crime where methods and money movements are changing week-to-week. The iterative nature of the dynamic approach has led to a full suite of policies, legislative amendments and activities (as outlined in Box 1.3 above) to combat CEF that were built over time as the risk was changing and becoming more prominent. However, while significant focus is given to CEF, these policies and activities have not yet shown full effectiveness, with scam losses from CEF in Singapore rising dramatically over the reporting period. The measures Singapore has implemented will logically mitigate fraud, particularly CEF and ML risks. As reported at the onsite visit, the 2025 scam loss figures appear to have stabilised from 2024 for the first time in the reporting period after an exponential rise. It is expected that efficacy of these measures will increase with time.

127. Singapore has an established, comprehensive framework for the implementation of AML/CFT policies and activities administered through the AML/CFT SC that is supported by a clear commitment from all levels of government. This framework uses the dynamic approach to risk understanding and mitigation. This dynamic approach is strong in that it can very quickly react to emerging and/or changing risks, but policies and activities appeared to be implemented on a risk-specific basis without a systematic and regularly updated overview of risk landscape or future forward planning. Connection between the high risk areas identified through the NRAs and the strategy documents can be improved.

1.3. Exemptions, enhanced and simplified ML/TF measures

1.3.1. Simplified Measures and Exemptions

128. Singapore adopts a very cautious approach to simplified measures and exemptions.

129. FIs, VASPs and DNFBPs do not have to perform certain BO checks in specific lower risk scenarios. Examples of such customers include Singapore and foreign government entities, and an entity listed on the Singapore Exchange. FIs can apply the exemption unless there are doubts over the veracity of the CDD information or if the FI has ML or TF suspicions.

130. Singapore has also put in place provisions for simplified CDD measures that may be applied in relation to a customer, any natural person appointed to act on behalf of the customer and any BO of the customer if it is satisfied that the risks of ML/TF are low and when the assessment is supported by adequate information. The simplified CDD measures must continue to be commensurate with the level of risk, based on the risk factors identified by the FI/VASPs/DNFBPs. Simplified CDD measures are prohibited in higher risk scenarios, including where there is a suspicion of ML/TF.

131. Singapore has a very limited number of exemptions in place. Singapore considers exemptions when raised by the private sector through the RTIG. The following entities were exempted from AML/CFT requirements following RTIG discussions.

- PSPs if they only offer products that meet certain low risk criteria for ML/TF[17], and
- trustee-managers of business trusts.

132. The exemption applies in relation to CDD, foreign currency exchange transactions, issuance of bearer negotiable instruments and cash payouts, agency arrangements, and wire transfers. Singapore identified these scenarios following an RTIG risk discussion and a ML/TF Risk Assessment. These exemptions are not in line with the findings of the ML NRA in relation to cross border money transfers as higher risks for Singapore, but notes that such exemptions are only allowed in very limited circumstances.

133. MAS has also encouraged FIs to conduct SDD when appropriate, for instance through issuance of circular on SDD measures for remittance services to foreign workers under isolation during Covid-19 period. However, there is no systematic mechanism to proactively and consistently monitor and identify scenarios for possible exemptions or simplified measures. Singapore indicated that the private sector may and has in fact raised the issue of exemptions, which was subject to rigorous discussion at the RTIG and approval by the AML/CFT SC. Singapore has focused its attentions on higher risk areas but could have better utilised its dynamic approach to more systematically consider and justify exemptions and simplified measures. In view of the process barriers and the low number of exemptions/simplified measures

[17] MAS defined low risk activities. These relate to account issuance services, domestic money transfer services, and CBMT services that meet certain low risk criteria, such as payment that is strictly only for goods or services and that payment is funded from an identifiable source (i.e. from a FI that is subject to and supervised for AML/CFT requirements).

implemented, which is reasonable. Singapore does not effectively use its understanding of ML/TF risk to systematically justify exemptions and simplified measures.

1.3.2. Enhanced measures

134. Singapore has effective enhanced measures provisions in law and has applied them in practice in line with risks. Singapore requires EDD for FIs dealing with higher risk legal persons, with specific indicators that may indicate higher risks, including where the FI is not able to establish if the legal person has (a) any ongoing/apparent business activities, (b) economic or business purposes for its corporate structure, or (c) substantive financial activity.

135. Singapore has also applied enhanced measures to DPTSPs, including requiring CDD for all customers (a) that the DPTSP establishes business relations with, or (b) for whom the DPTSP undertakes or intends to undertake any transaction without an account being opened. FIs are also required to perform enhanced risk ongoing monitoring measures where a transaction involves a transfer of a digital token to, or receipt of a digital token, from an entity other than a MAS-regulated FI (or FIs subject to AML/CFT requirements consistent with FATF standards, where the FI is incorporated or established outside of Singapore).

136. Singapore also requires EDD for FIs engaging in transactions with higher risk countries or jurisdictions, including those identified by the FATF. MAS engages with FIs to ensure that they remain alert to risks resulting from geopolitical developments, including sanctions evasion risks. Relevant private sector institutions also noted they had their own geographic considerations and took enhanced measures as a result of risk advisory guidance. Singaporean authorities also demonstrated a more nuanced understanding of geographic risks and maintain their own lists of higher risk countries. This understanding of geographic risk could be better communicated to the private sector and used to inform the application of enhanced measures.

137. Overall, the results of Singapore's assessments of ML/TF risks informs and supports the application of enhanced measures for higher risk scenarios.

1.4. Objectives and activities of competent authorities and SRBs

138. Singapore's competent authorities are part of the dynamic approach and were closely involved in the NRA development process. Objectives and activities are generally in line with the findings of the risk assessment processes and aligned with the Strategies. All relevant agencies reported prioritisation of CEF, in line with the NRA findings. However, not all key high ML/TF risks are given comparable priority (see section 2.2.2). The lack of specific actions and deliverables against the Strategies has some impact on the objectives and activities of competent authorities.

139. From a resourcing perspective, agencies are allocated dedicated resources through a central mechanism and individual agencies can each identify needs for additional resources, based on guidance provided at the SC and IAC. This resource application is submitted at the agency level and considered on a case-by-case basis. At isolated junctures, the SC/IAC have also reviewed the resource of AML/CFT agencies and guided agencies to consider if more sources across the government are needed for AML/CFT work. The SC and IAC would benefit from having a more regular full overview of the number of AML/CFT resources across the system, although no competent authorities in Singapore reported resourcing issues.

140. The lack of regular overview has led to resource allocation differences in practice. Resource allocation across different supervisors covering DNFBP sectors does not appear proportionate to the sectoral risks identified, with high intensity controls applied to relatively lower risk sectors or products (for example, pawnbrokers, accountants or wakafs). Singapore attributed this to the fact that their supervisors

are able to include AML/CFT examinations as part of their broader regulatory oversight beyond AML/CFT concerns (e.g. for social and prudential reasons), but there appears no overarching mechanism to ensure consistency and proportionality of supervisory efforts across different sectors on a regular basis.

141. In addition, STRO is well resourced while relying on automation and technology to prioritise, analyse and disseminate STRs. Financial intelligence produced and disseminated by STRO aligns with the country's risk profile to a good extent, as discussed further in section 6.2. Financial intelligence from STRO is being used to initiate and support investigations to some extent: 26% of financial intelligence packages and 17% of Fin-IRs disseminated by STRO are used to initiate investigations, while 14% of packages and Fin-IRs supported investigations (see Section 6.4).

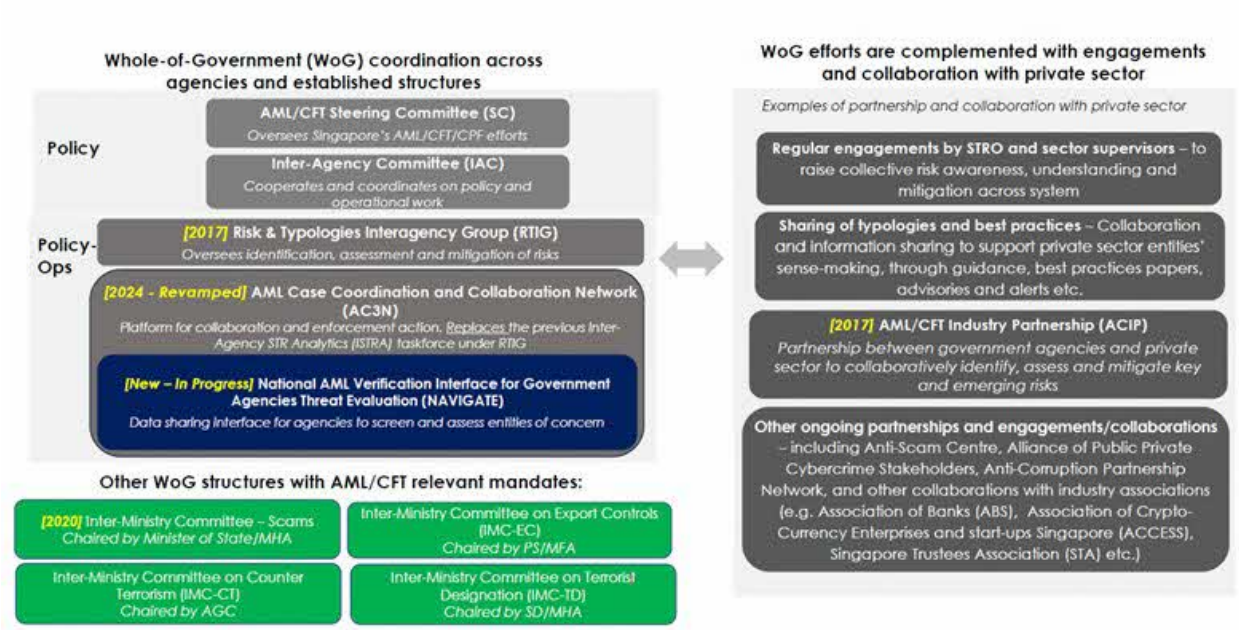
142. LEAs demonstrated a risk understanding that is aligned with the findings of the NRAs and was more nuanced in some areas with a reasonably sound understanding of the data that underpinned the analysis. As part of the RTIG mechanism, competent authorities were alive to existing risks and trends and authorities reported that the dynamic approach to risk monitoring was very effective. In particular, authorities saw it as a positive that Singapore could remain agile and not be bound by bound by a fixed NRA cycle. In practice, 93% of Singapore's ML investigations involve domestic predicate offences, which only partly aligns with Singapore's risk and context.

143. Singapore has focused attention on its highest risk (i.e. fraud), as compared to the other key high ML/TF risks and has generally not taken decisions to de-prioritise lower risk areas. There are fewer investigations into other higher-risk areas (i.e., tax crimes, corruption and TBML). The focus on ML from CEF overweighs Singapore's investigative resources into one high risk offence at the expense of others, with the majority of the CEF cases being relatively low value CEF, initiated by Singaporean victim complaints. Competent authority actions often fall short in addressing the risk of foreign actors using Singapore's economy to channel CEF proceeds. Singapore's dynamic approach is a strong approach to risk monitoring and assessment in theory, but the lack of an updated and comprehensive overview has resulted in some mismatch in operational alignment and supervisory coverage.

1.5. National co-ordination and co-operation to develop and implement policy

144. The strength of Singapore's AML/CFT/CPF system lies in its robust domestic co-ordination and co-operation on AML/CFT issues at the policy level. Singapore has strong and clear national co-ordination and co-operation mechanisms to develop and implement policies, through the AML/CFT SC, the IAC and RTIG mechanisms, supported by subject matter-specific Inter-Ministry Committees (see Figure 2.1 below). These co-ordination and co-operation mechanisms include representation from all relevant ministries and agencies in Singapore.

Figure 1.1. Singapore's WoG co-ordination structures and collaboration mechanisms within government and with the private sector



145. The AML/CFT SC develops and co-ordinates the implementation of Singapore's AML/CFT/CPF policies. The AML/CFT SC is comprised of the most senior public servants from the MHA (PS), MOF (PS) and the MAS (Managing Director).

146. The IAC is one level below the AML/CFT SC and is co-chaired by the Deputy Secretary of MHA and the Deputy Managing Director of MAS. The IAC's membership comprises all relevant competent authorities for AML/CFT purposes. The IAC provides a forum for agencies to share information such as emerging threats and trends, FATF typologies, best practices and other developments, and makes recommendations to the AML/CFT SC on policy initiatives.

147. Singapore's RTIG is co-chaired by the Senior Director of MHA and the Executive Director of MAS and is the main working-level body tasked with identifying, assessing and understanding ML/TF risks at the WoG level. RTIG is responsible for the development of Singapore's NRAs. RTIG meets quarterly, reporting into the AML/CFT SC as needed.

148. In addition to the AML/CFT SC, IAC and RTIG, Singapore has a number of subject matter-specific interministerial committees (IMC). The IAC and RTIG works closely with these committees to ensure a consistent and coherent approach in policy making. Some examples include:

- The IMC-TD is the mechanism responsible for proposing terrorist designations under UNSCR 1267/1989, UNSCR 1988, and UNSCR 1373 (see IO.9/10).
- The IMC-EC oversees Singapore's export controls framework, including relevant policy and operational issues relating to the proliferation of WMD and UNSC sanctions (see IO.11).
- The IMC-Scams brings together a range of agencies covering law enforcement and regulatory agencies in relation to the financial and telecommunication sectors to work with the private sector partners to co-ordinate efforts to combat CEF, including the threat of ML offences (see IO.7).

149. Agencies interviewed during the onsite were very aware of the various co-ordination mechanisms and actively use them to resolve issues or highlight emerging threats. Agencies reported a collaborative and a 'One Singapore' approach in these committees, noting that they can normally resolve policy issues at the working level and only need to deconflict or set out major policy initiatives at the most senior level.

There is a regular and clear framework for policy co-ordination and co-operation amongst government departments. This is reflective of Singapore's WoG approach in AML/CFT and is one of Singapore's key strengths.

150. Co-operation between MAS, other supervisory authorities, SRBs, and industry associations is key to developing and implementing AML/CFT policies for FIs, VASPs and DNFBPs. MAS, SRBs and industry associations have held multiple engagements to discuss risks, policy impacts, and implementation issues. These include sharing common gaps, best practices, and enforcement actions. Topics such as risks, STR expectations, and TFS implementation are regularly addressed. SRBs and industry associations play a key role in raising awareness of identified risks and mitigation measures among their members.

1.6. National co-ordination and co-operation for operational purposes

151. Singapore has established strong co-ordination and co-operation mechanisms for operational purposes. Singapore's primary operational co-operation mechanism is the AC3N, formerly known as the ISTRA. Formed in 2018 under RTIG, the ISTRA was made up of representation from all relevant competent authorities in Singapore's AML/CFT regime. The ISTRA reviews and prioritises STRs and conducts network analysis for the identification of significant ML activity for possible regulatory and/or enforcement actions. Since its establishment, ISTRA was used to escalate 34 cases for inter-agency co-ordination, which resulted in supervisory follow-ups by sector supervisors and/or investigations by LEAs. ISTRA was reformed into AC3N in September 2024, with a broadened membership and a direct reporting line to the AML/CFT SC with a view to enabling more comprehensive and timelier co-ordination. In addition to these formal collaboration channels, working level collaboration is also enhanced by measures such as secondment of staff.

152. Singapore also has a public private partnership, the ACIP, which brings together nine materially significant banks with all relevant competent authorities in Singapore. This venue facilitates open discussion on actual cases and trends (see IO.3 and IO.6 for more on ACIP). ACIP also creates ACIP Case-Specific Information (ACIP CSI) taskforces to detect and develop priority cases. Through these taskforces, tactical information is shared with members through a hub-and-spoke model, which conduct further analytics on their information holdings to surface new leads. Such sharing has resulted in positive outcomes, as well as enhancements in the relevant FIs' risk understanding which in turn leads to better risk mitigation and AML/CFT controls. These taskforces are also used to co-ordinate actions during major investigations. These ACIP-CSI taskforces go beyond the membership of the nine permanent FI members to other FIs, VASPs and DNFBPs, as needed. There was positive feedback from ACIP members and government authorities indicating that the ACIP was leading to real world results.

Box 1.4. Collaboration between private sector and authorities to take action in relation to Trade-Based ML

Given Singapore's position as an international trade hub, Singapore is susceptible to the threat of trade-based ML. Through ACIP, an industry best practices paper was published in 2018 highlighting common trade-based ML red flags, typologies and best practices for identification and mitigation of trade-based ML risks. On an ongoing basis, ACIP monitors the trade-based ML risks and typologies, and banks regularly share their observations and measures adopted to mitigate risks.

These efforts have produced tangible and significant results. In 2019, an ACIP bank alerted CAD to Company A's under-invoicing, phantom shipments and suspected use of shell companies. CAD worked with banks to share information and intelligence through the ACIP case information sharing mechanism, and banks filed STRs relating to Company A. STRO subsequently analysed the STRs and disseminated relevant information to CAD, allowing CAD to take swift and effective enforcement action.

With the financial information and multiple reports lodged by banks and finance companies who had extended credit facilities to Company A for the purposes of trade financing, CAD commenced investigations into the former Chief Financial Officer of Company A in January 2020, was convicted of 11 counts of cheating under Section 420 of the Penal Code 1871 (Penal Code) and one count of falsification of accounts under Section 477A of the Penal Code in January 2023. She was sentenced to imprisonment of 20 years for deceiving 16 FIs of more than USD 469 million.

153. Singapore has developed a number of technical solutions to assist in its co-ordination and co-operation efforts. Competent authorities have developed the NAVIGATE platform in 2024 for WoG data sharing, to enable agencies to screen against one another's databases and expeditiously assess persons and entities of concern. In addition, in 2024, Singapore launched COSMIC, a centralised platform enabling tactical private-to-private information sharing amongst six major commercial banks in Singapore.

154. During the assessment process, Singapore presented a number of case studies demonstrating effective collaboration between STRO and LEAs in combating ML, TF, and predicate offences. Interviews with authorities reaffirmed that both LEAs and the FIU exhibit strong commitment to inter-agency co-operation, demonstrating a clear understanding of their collective critical role in financial crime enforcement.

2 International co-operation

The relevant Immediate Outcome considered and assessed in this chapter is IO.2. The Recommendations relevant for the assessment of effectiveness under this chapter are R.36-40 and elements of R.9, 15, 24, 25 and 32.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Singapore has a sound legal and operational framework to provide and seek a broad range of assistance. This is supported by bilateral and multilateral treaties, SOPs, recent legislative amendments and a simplified extradition mechanism with Malaysia and Brunei.

b) Singapore's Central Authority takes a collaborative approach, applies a prioritisation system for international co-operation and provides timely and constructive international co-operation to a reasonable extent, having executed a majority of MLA it receives. However, one third of MLA requests remain pending/partly executed. The scope of information Singapore can provide is generally broad. There are some limitations with respect to BO information and Unregistered Foreign Companies (see IO.5).

c) Singapore's MACMA sets a high legal bar to providing formal co-operation, whereby requests must be of 'substantial value' to be executed, which can hamper timeliness. Feedback from the Global Network indicates that Singapore generally provides timely and effective co-operation, though sometimes with delays during clarificatory processes to meet legal thresholds.

d) Outgoing extradition requests significantly outnumber incoming ones, and both are largely handled through a simplified process with Brunei and Malaysia, where no formal extradition request is required. co-operation under this framework is generally effective and timely. There have been no extradition requests related to CEF and ML-related to CEF, which are high-risk areas.

e) Singapore seeks international co-operation in more modest ways and makes four times fewer MLA requests than it receives despite acknowledging that its primary risks lie abroad. Authorities seek modest formal co-operation for ML when considering the significant number of ML investigations. Formal co-operation aligns with risks to some extent.

f) Singapore has shown some success using international co-operation for asset recovery purposes. It is responsive to requests and enforces a small number of confiscation orders, which leads to repatriation of assets in a limited number of cases. The need to verify legal requirements under MACMA increases the risk of asset dissipation to some extent, although LEAs can use CPC powers simultaneously to seize/freeze assets. Despite being highly exposed to foreign predicate offences, Singapore has sent a very modest number of MLAs to recover assets, aligning with risks to some extent, and has secured the return of approximately SGD 52 million (USD 39 million).

g) Singapore is active engaging in other forms of co-operation. Competent authorities actively engage in a broad range of bilateral and multilateral channels to pursue criminals and criminal property. This co-operation is generally timely, effective, and aligns with risks to some extent. Feedback from the Global Network is generally positive.

Recommended Actions (RAs)

Singapore should:

a) Ensure that constructive and timely assistance is provided by streamlining the evidentiary requirement in MACMA's Section 22(4)(b)(i) to define and simplify the term 'substantial value'. To facilitate requests, this should include how this threshold is reached, for example in public SOPs.

b) Make active use of formal international co-operation channels consistent with its risk profile, and in priority for all appropriate cases with a cross-border nexus, for asset recovery and other high-risk offences (including CEF).

c) Review pending/partially executed MLA requests and take steps to execute that assistance in order to provide more complete and timely assistance to jurisdictions.

Overall Conclusions on IO.2

As an IFI with significant cross-border risks, international co-operation is essential for Singapore, who has a sound legal and operational framework to provide a broad range of assistance. Feedback from the Global Network indicates that Singapore generally engages in timely and effective international co-operation in spite of a high legal bar to prove that requests are of 'substantial value' to the requesting state. This can result in a clarificatory process that affects Singapore's response, including the timeliness of co-operation. One third of incoming requests remain pending where some assistance is provided. Singapore can exchange a broad range of information (with some limitations noted on BO) and provides timely and effective co-operation to a reasonable extent.

Singapore seeks international co-operation in more modest ways and received almost four times as many MLA requests as it sends despite its predominant risks lying outside the country. International co-operation sought through both formal and informal channels aligns with Singapore's highest risks to some extent, mainly driven by fraud cases. There is

scope to improve co-operation in respect of ML as less than one percent of ML investigations resulted in an MLA request, as well as tax crime, corruption and TBML. Competent authorities use international co-operation for asset recovery purposes with some success and have secured the return of approximately SGD 52 million (USD 39 million); however, there is scope to make better use of international co-operation in this area.

Competent authorities actively engage in other forms of co-operation, including with respect to asset recovery. This co-operation is generally timely and effective, although not sufficiently risk aligned.

Singapore is rated as having a Substantial level of effectiveness for IO.2.

Immediate Outcome 2

155. As an IFC and trade hub with significant cross-border ML/TF risks, international co-operation is essential for Singapore to act against criminals and their property. Singapore has a sound legal framework for MLA and extradition under MACMA (updated in 2024 to broaden the type of assistance that can be provided), the Extradition Act, supported by SOPs and operational frameworks (numerous bilateral and multilateral agreements) to prioritise and pursue international co-operation.

156. The AGC's International Legal Co-operation Team (ILCT), together with the Central Authority Registry, constitutes the Central Authority (CA) for processing MLA and extradition requests (see R.37-39). With a team of 10 trained staff, CA takes a collaborative approach, managing requests efficiently, including urgent requests outside office hours. In 2020, AGC introduced 'Intelligent Workspace' (IW), an online Case Management System to streamline requests, track timelines and deliverables, manage court filings, and maintain records. SOPs set a two-week response time if no deadline is provided, though prioritisation is based on court deadlines, involvement of PEPs, or risk of asset dissipation. CA also provides online guidance to help foreign authorities submit requests, including urgent ones.

2.1. Providing constructive, timely and quality mutual legal assistance and extradition

157. Singapore has a sound system in place to provide constructive and timely MLA and extradition requests, including for asset recovery purposes. MACMA allows Singapore to provide a wide range of assistance on the basis of reciprocity, although the high legal requirement to execute some requests may affect the timeliness of assistance provided.

2.1.1. Providing evidence and locating criminals

158. To a reasonable extent, Singapore provides constructive, timely and quality MLA in response to requests on ML, associated predicate offences and TF. Singapore received 988 MLA requests. As the breakdown in Table 2.1 shows:

a) Thirty-nine per cent of MLA requests were executed in a timely manner.
b) Thirty-four per cent of MLA requests remain pending and are at different stages of execution. Singapore considers an MLA request, which may encompass multiple requests for assistance, as pending if (1) at least one category of requested assistance remains outstanding, or (2) Singapore

is clarifying and/or substantiating the request with the requestor. 28% of the pending MLA requests are partially executed, where some assistance has been provided, whereas assistance is still pending in 72% of those requests, including where Singapore is actively engaging with the requesting jurisdiction.

c) Twenty-six per cent of MLA requests received during the time period were closed due to inactivity or withdrawals. The requests were closed either after six months of inactivity where the requesting jurisdiction no longer responds to Singapore's follow-up or by withdrawal by the requesting state. This six-month timeframe is short, considering that requesting states may need time to follow-up on requests, but Singapore can re-open the request at any time if the requesting jurisdiction responds to a request past the deadline.

d) One per cent of MLA requests were formally declined by Singapore, typically due to unmet requirements under MACMA (including dual criminality, or where there are ongoing domestic investigations or court proceedings).

Table 2.1. – Incoming MLA requests (per type of predicate offence and status)

	2020	2021	2022	2023	2024	Total (%)
Total Requests	189	219	183	170	227	988 (100)
ML	75	86	67	58	72	358
TF	1	1	2	0	2	6
PF	0	1	1	1	0	3
Corruption and bribery	5	6	11	7	9	38
Counterfeiting	1	0	1	3	1	6
Environmental crime	2	1	0	1	0	4
Extortion	4	6	3	4	6	23
Forgery	6	11	5	8	10	40
Fraud	65	83	69	64	86	367
Illicit trafficking in drugs	6	5	3	5	2	21
Insider trading and manipulation	1	0	0	1	1	3
Kidnapping	3	0	1	1	2	7
Murder, grievous bodily injury	4	9	2	3	8	26
Organised criminal group/racketeering	2	2	0	1	4	9
Robbery or theft	14	18	9	12	7	60
Sexual exploitation	8	2	9	12	16	47
Smuggling	4	8	4	1	7	24
Tax crimes	19	12	15	7	17	70
Terrorism	1	2	2	3	4	12
Status						
Number of requests executed	112	105	63	54	47	381 (39)
Number of requests declined	3	3	6	1	0	13 (1)
Number of requests closed due to inactivity or withdrawals	61	84	46	37	25	253 (26)
Number of requests pending/partially executed	13	27	68	78	155	341 (34)

Note: a single MLA request may involve multiple types of assistance therefore the total number of requests per predicate offence does not match the number of requests received

159. Most formal assistance is provided through exercising powers under MACMA. A much more limited amount was provided through exercising CPC powers or even on a voluntary basis. The nature of requests varies and concerns both simple and more complex requests, such as enforcing confiscation orders. A majority are for coercive measures, particularly production orders (e.g. records from FIs and the restraining of financial assets) which require court orders under S22(3-4) MACMA). Seeking information/evidence that requires coercive measures partly explains delays in executing requests as

competent authorities may need to seek a court order to execute the request. Singapore does not maintain statistics on BO information sought by requesting parties (Table 2.2).

Table 2.2. Type of request received[18]

	Legal provision	# requests	% total
Witness statement & taking of evidence (video-link)	Non-MACMA	299	19
Government records	Non-MACMA	245	15
Taking of evidence for criminal proceedings	MACMA (S21)	63	4
Records from FI or other natural/legal persons	MACMA (S21)/others	773	49
Restrain/enforcement of confiscation order	MACMA (S29-30) and CPC	73	5
Search and seizure	MACMA (S33)	15	1
Location/Identifying persons	MACMA (S 37)	16	1
Service of process	MACMA (S38)	65	4
Others	Non-MACMA	41	3
Total		1 590	100

160. Case studies, statistics and discussions with the authorities demonstrate that Singapore generally provides timely assistance. Complex MLA requests are executed within an average of ten weeks, and simpler ones, such as providing video-link evidence, can be completed in as little as three days. Case studies and feedback provided by the Global Network generally indicates that assistance provided by Singapore is comprehensive.

161. Applications for production orders under Section 22 of the MACMA (to share documentation, records and 'other things') and search warrants under Section 34 (for requests to obtain things by search and seizure) can be granted upon several conditions being met. Authorities must be satisfied that there are reasonable grounds to suspect that a specified person has carried on or benefited from a foreign offence. There must be reasonable grounds to believe that the documents or records sought through production orders are likely to be of 'substantial value' to the criminal matter, are not legally privileged and the provision of documents is not contrary to public interest. This is a much higher bar than is required by domestic authorities. It may be very difficult for a foreign investigator to know in advance whether information sought will provide value, much less substantial value, to their investigation. The term 'substantial value' is undefined in the legislation or in SOPs[19]. Singapore have indicated that they interpret 'substantial value' to mean 'relevant'. The Assessment Team assesses that these are very different thresholds. As a result, there remains some ambiguity in operationalising this threshold. The qualifier 'substantial' adds to the requirement to be of value, which may hamper timeliness.

162. In practice, upon receiving a request, the CA will check that these requirements are met by seeking clarifications from requesting jurisdictions (where necessary). This clarificatory process typically involves verifying property or account details, the nexus between the offence and underlying investigation in the requesting jurisdiction and the property or records of interest in Singapore, assessing whether the conduct constitutes an offence under Singaporean law and establishing the value of the requested information for the criminal matter in the requesting jurisdiction. This can be time-consuming, especially in complex cases involving multiple accounts and/or legal persons/arrangements. Moreover, some feedback from the Global Network highlighted concerns that excessive requests for clarifications by Singapore may result in delays due to procedural complexities. 108 MLA requests (31.6% of the pending MLA requests) have been pending for over two years because of these requests for clarifications. Singapore has made efforts to reduce the need for clarifications by making available on the CA's publicly accessible website detailed templates for

[18] Some assistance is provided through MACMA powers, non-MACMA (e.g. CPC), or both MACMA/CPC.

[19] Assistance may be provided on the basis of reciprocity in the absence of an MLA Treaty (MLAT). See c 37.1

common types of assistance and maintaining close relationships with foreign counterparts to assist when they make requests.

163. Requests are generally in line with risks and relate overwhelmingly to ML and fraud (Table 7.1). The nature of these requests aligns with known typologies (e.g. TBML, misuse of legal persons and arrangements, etc.). Most requests emanate from regional partners (Vietnam, Thailand, Malaysia), as well as other materially relevant jurisdictions (USA, India, Australia etc.). Some other jurisdictions (e.g. China, Hong Kong China, Cambodia etc.) make fewer requests to Singapore despite trading links and cross-border ML/TF risk.

2.1.2. Extradition

164. Singapore has an appropriate operational and legislative framework in place to provide extradition, including simplified extradition, and to act on urgent cases. Under the Extradition Act, urgent applications for provisional arrest can be made by the requesting country, pending the receipt of the formal extradition request. Singapore also has bilateral extradition requests with key partners and a special arrangement with Malaysia and Brunei simplifying the process to extradite each other's fugitives without a formal extradition request. Where either of these countries requires the arrest of persons in Singapore, they make a request to Singaporean LEA directly, who will apply to the courts for endorsement of the warrant in Singapore before executing the warrant.

165. Singapore generally provides good and timely assistance in response to the limited number of extradition requests received (21). These primarily relate to predicate offences and originate from important partners like the United States, European and Asian Countries, which aligns with risks reasonably well. Of these, 43% were executed, while 19% were declined, 14% were closed due to inactivity by the requesting state, and 24% remain pending. Five cases are pending subject to clarifications concerning dual criminality and other legal checks including the involvement of the individual in domestic criminal proceedings or where the individual contests extradition. The declined cases largely involve situations where the fugitive was not located in Singapore or was only transiting through, leaving insufficient time for Singapore's competent authorities to act.

166. Although simplified extradition procedures exist, Singapore typically executes requests within an average of three months, which is appropriate given the legal complexities involved. This timeframe includes cases where the defendant appeals the extradition (in one instance, extradition was granted nearly two years after the initial request). During the reporting period, Singapore received 14 expedited extradition requests from Brunei/Malaysia, and executed all of these, unless withdrawn by the countries or warrants for execution were not submitted to Singapore.

2.1.3. Facilitate asset recovery

167. Singapore is equipped to assist requesting jurisdictions in asset recovery by enforcing freezing, seizure, and confiscation orders across a wide range of assets. Its legal framework allows for co-operation in civil confiscation proceedings and enables enforcement even without a foreign confiscation order. MACMA amendments in 2024 further strengthened this framework by allowing LEAs to physically transfer confiscated items, rather than only returning realised assets. These changes permit Singapore to enforce foreign confiscation orders issued by competent authorities beyond the courts, enhancing its flexibility and responsiveness in cross-border asset recovery efforts (see R. 38).

168. As indicated in Table 2.3, the authorities received 73 MLA requests on asset recovery, which includes a mix of request to freeze, seize and confiscate assets, including enforcement of foreign confiscation orders. These requests are risk-aligned and mainly relate to ML and fraud, totalling at least SGD 1.14 billion (USD 844 million) in assets, such as bank accounts and real estate. LEAs may use such

MLA requests to open a domestic investigation (for example, 27 ML investigations were started during the reporting period using CPC powers to freeze/seize assets).

169. Singapore executed 36 MLA requests (49% of total), recovering SGD 778 million (USD 576 million) and other assets for foreign jurisdictions. Singapore considers that MLAs are executed even where no assets are ultimately identified, This can include situations such as where bank accounts that were the subject of the foreign request were closed, the assets had been dissipated by the time Singapore received the request, the assets that were the subject of the foreign request did not exist, where other forms of assistance were provided instead, or the assets (such as virtual assets) were not located within Singapore. Of the 37 remaining requests to facilitate asset recovery (51% of total), 14 are still pending (19%), six were declined (8%) and 17 requests (23%) were closed due to inactivity or withdrawal by the requesting jurisdiction.

170. As discussed above, the thresholds under MACMA may cause variable processes for execution resulting in delays with executing requests or potentially non-responses for requesting jurisdictions. In every MLA request that seek asset recovery assistance, Singapore also considers if informal assistance outside the MACMA framework, such as under CPC powers, can be provided to prevent asset dissipation. Exercising such powers outside the MACMA framework requires a suspicion that under Singapore law, an offence has occurred. In the case of MLA requests that seek asset recovery assistance, this would typically be an ML offence. Obtaining the facts from the requesting jurisdiction to determine if such a suspicion can be formed may take time and may also create a risk of asset dissipation, especially liquid assets such as bank accounts, which account for a significant number of requests. Upon receiving an MLA request, the relevant LEA conducts informal checks to verify whether the bank account is still active, whether it holds funds, and whether there is suspicion of a domestic ML offence. If all conditions are met, the LEA may use its powers under the CPC to seize the funds without requiring a court order under MACMA. This process may affect the timeliness of co-operation that Singapore provides.

171. 26 of the 73 asset recovery-related MLA requests concern enforcing a foreign judgement[20] (Table 2.3). These requests are not executed by Singapore in only a few instances. Three requests were declined: (i) two because the foreign court order did not satisfy the relevant MACMA requirements; and (ii) one request was declined so as not to prejudice ongoing domestic investigations / court proceedings. Three requests are pending execution as the requesting jurisdiction failed to provide all relevant documentation for the Court to approve the requests. Singapore executed five MLA requests to enforce a foreign judgement leading to the repatriation of SGD 13.5 million (USD 10 million) (see IO.8). Nine cases are ongoing with no assets yet repatriated, either because Singapore is addressing procedural and legal requirements under the MACMA, because notices of registration must be served in third jurisdictions, or where responses or additional documentation from those jurisdictions are pending. There are a small number of cases where the clarificatory process to ensure that MACMA conditions are met led to delays of more than 2 years. In one instance, despite frequent communication between Singapore and a foreign jurisdiction, assets were repatriated to the requesting jurisdiction four and half year after Singapore received the request. This exceptional situation related to the unknown situation of the accused's whereabouts, and time was needed to effect substituted service in the jurisdiction where the accused's last known address was, in compliance with the domestic laws of the requesting jurisdiction.

[20] This figure excludes 12 requests Singapore received for both freezing/seizing and enforcement of foreign confiscation orders. Although a detailed breakdown is unavailable, figures for the enforcement of foreign confiscation orders are likely higher.

Table 2.3. MLA (asset recovery and enforcement of foreign confiscation orders)

	2020	2021	2022	2023	2024	Total (%)
1. Total MLA requests	14	23	11	13	12	73 (100)
ML	11	12	6	8	8	45 (62)
Corruption and bribery	0	2	1	1	0	4 (5)
Extortion	1	0	0	0	0	1 (1)
Forgery	0	0	0	1	0	1 (1)
Fraud	1	7	4	3	3	18 (25)
Illicit trafficking in narcotic drugs	0	0	0	1	0	1 (1)
Robbery and theft	0	2	0	0	1	3 (4)
Tax crimes	1	0	0	0	0	1 (1)
2. Status of requests						
Executed (amounts frozen, seized, confiscated and repatriated where applicable)	9 SGD 30.4m	10 SGD 732.9m + others	3 SGD 0.7m	6 SGD 0.5m + others	8 SGD 14.4m	36
Closed due to inactivity/withdrawal by requesting State	4	7	4	2	0	17
Declined	1	4	0	0	1	6
Pending	0	2	4	5	3	14
3. Enforcement of Foreign Confiscation Orders (FCO)						
Received[21]	6	8	4	2	6	26
Assets repatriated	4	1	0	0	0	5
Assets frozen but not repatriated	0	0	3	2	2	7
FCO registered but assets not repatriated	1	0	0	0	1	2
Requests closed due to inactivity/ withdrawal	0	2	1	0	0	3
Request not executed	0	2	0	0	1	3
Requests declined under MACMA conditions	1	1	0	0	0	2
Request declined (ongoing domestic investigation)	0	1	0	0	0	1
Requests pending	0	1	0	0	2	3

[21] A request for the enforcement of foreign confiscation orders may include requests to freeze/seize assets as well.

Box 2.1. Provision of International Co-operation

MLA request to share bank records, restrain and repatriate funds

Singapore received various requests from two foreign counterparts to restraint bank accounts belonging to a former government official from a Southeast Asian State who was accused of receiving bribes in exchange for awarding government contracts (equivalent to approximately USD 1.8 million). LEAs commenced domestic investigations and froze bank accounts in line with CPC powers to prevent the dissipation of assets. LEAs subsequently obtained restraint orders in respect of the bank accounts and production orders under MACMA to share bank account information. One foreign counterpart sent an MLA request in June 2021, seeking the restraint of one bank account on the basis that civil forfeiture proceedings had been instituted in that counterpart's country. In August 2021, Singapore obtained MACMA restraint orders for that bank account.

Enforcement of a foreign confiscation order

In January 2020, Singapore received a request from an East Asian State to register and enforce a confiscation order for over USD 500 000 in corrupt proceeds laundered through a Singapore FI. The CA obtained a High Court order to register and enforce the foreign confiscation order in October 2020. Under MACMA, notice of registration of a foreign confiscation order must be served on the accused. As the accused's whereabouts were unknown, substituted service was effected in February 2022 which required the approval of the requesting state's courts. Singapore applied to realise the assets in April 2023, with service in the requesting Sate confirmed in January 2024. A High Court order was granted in February 2024, and the proceeds were repatriated in July 2024.

2.2. Seeking appropriate and timely mutual legal assistance and extradition

172. Singapore seeks international co-operation in a timely manner as well as to facilitate asset recovery. Authorities understand the value of international co-operation and proactively seek MLA to pursue ML and associated predicate offences with transnational elements.

2.2.1. Seeking evidence and locating criminals

173. Singapore uses MLA to some extent, having issued 234 MLA requests during the reporting period, averaging approximately 46 requests per year (Table 2.4). There was a notable increase in 2024 followed the implementation of SOPs that clarified when LEAs should initiate MLA requests. The overall number of requests remains modest when considered against the country's risk and context and the high number of ML investigations (11 000), an even higher figure when accounting for all predicate offences. This is notable given Singapore's cross-border risk exposure. While use of formal co-operation through MLA must be considered alongside the use of informal co-operation channels, Singapore could have made better use of MLA requests over the assessment period.

174. Requests are initiated by a range of competent authorities and are managed by the CA. The SPF-CAD accounts for 71% of requests. MLA requests are primarily directed to key international partners, including Hong Kong, China, UAE, US, UK, and neighbouring countries. Fewer requests are sent to jurisdictions such as Cambodia, despite typologies and case studies indicating a clear fraud/ML nexus. Most MLA requests concern relatively straightforward matters, such as obtaining government records (39%) or

the taking of witness statements or evidence (83%). MLA has been used for asset recovery purposes with 47% of requests relating to the restraint or enforcement of a confiscation order.

175. Of the total MLA requests, 47% have been executed by the requested states, while 42% remain pending and 12% have been withdrawn by Singapore. Notably, no requests have been refused. 67% of the pending requests were issued in 2023 and 2024 (see Table 2.4), suggesting a potential time lag in execution. Onsite interviews and statistics show that Singapore proactively follows up on outstanding requests, typically every two months, and provides clarifications to facilitate execution. This proactive approach reflects the generally high quality of Singapore's MLA requests, a view supported by feedback from the Global Network.

Table 2.4. Outgoing MLA requests by Singapore (per type of offence and status)

	2020	2021	2022	2023	2024	Total (%)
Requests per predicate offence	50	53	32	32	67	234
ML	8	7	7	3	7	32 (14)
TF	0	0	0	0	0	0 (0)
PF	0	0	0	1	0	1 (0)
Corruption and bribery	1	4	0	1	2	8 (3)
Counterfeiting	0	0	0	0	0	0 (0)
Environmental crime	0	0	0	1	0	1 (0)
Extortion	0	0	0	0	0	0 (0)
Forgery	3	8	2	3	5	21 (9)
Fraud	26	24	19	28	45	142 (61)
Illicit trafficking in drugs	2	1	1	3	2	9 (4)
Insider trading and manipulation	2	1	1	0	0	4 (2)
Kidnapping	0	0	0	0	0	0 (0)
Murder, grievous bodily injury	1	2	0	1	1	5 (2)
Organised criminal group/racketeering	0	1	0	0	0	1 (0
Robbery or theft	2	1	0	0	1	4 (2)
Sexual exploitation	6	5	3	2	2	18 (8)
Smuggling	0	1	0	0	1	2 (1)
Tax crimes	1	0	0	0	2	3 (1)
Status of requests						
Number of requests executed	32	33	17	13	13	108 (46)
Number of requests declined	0	0	0	0	0	0 (0)
Number of requests withdrawn by Singapore	5	10	6	2	5	28 (12)
Number of requests pending	13	10	9	17	49	98 (42)

Note: a single MLA request may involve multiple types of assistance, which explains that the total of request per predicate offence does not match the number of requests received

176. Requests are aligned with risks to some extent and some higher risk areas are insufficiently pursued. Most formal requests are directed toward combating CEF, which represents 61% of total requests and has shown steady annual growth demonstrating Singapore's focus on its highest risk predicate crime. Only 14% of formal requests relate to ML, despite Singapore's significant international risk profile. When considering the overall number of ML investigations, fewer than 1% result in authorities sending MLA requests. MLAs are used less frequently in other areas identified by Singapore as being of higher risk, including drug trafficking, corruption, organized criminal groups, and tax crimes. No request was made concerning TF, which is considered appropriate given Singapore's risk and context. While Singapore indicates this can be attributed to LEAs primarily relying on informal co-operation (exemplified in Box 2.4), quantitative information does not fully support this, and there is scope for to improve alignment of both formal and informal channels with risks.

2.2.2. Extradition

177. Almost all extradition requests (103) sent by Singapore use the simplified process with Malaysia and Brunei (Table 2.5). As for incoming extradition requests from these countries, this expedited process is done between LEAs without involvement of the CA. Separate from this, Singapore only sent six extradition requests. One example was provided of Singapore working with the requested state to execute an urgent request in the absence of an extradition treaty, which suggests that co-operation in this area can be timely and appropriate, even in the absence of an extradition treaty (see R.37). Where required, Singapore also uses other informal mechanisms (e.g. INTERPOL's red and blue notices) to support its extradition requests.

178. No extradition requests were made for CEF or ML related to CEF. As discussed in IO.7, there are some legal challenges to doing so, but this is a missed opportunity given the volume of cases, foreign perpetrators and the dissuasive effect of targeting Singaporeans that would be brought by doing so.

179. A relatively high number of extradition requests (including 'expedited' requests to Malaysia/Brunei) are declined, withdrawn or pending, with some pending requests dating as far back to 2022. Singapore notes that requests were declined by jurisdictions due to reasons such as offences being time-barred in local laws, fugitives having left the jurisdiction, or insufficient information provided in the request. For expedited requests to Malaysia/Brunei, cancellations were mainly due to arrests in Singapore, the subject's death, or the case no longer being pursued. Pending requests remain due to subjects being untraceable, having left the jurisdiction, or being imprisoned. Where cases are pending, Singapore continues to engage with the relevant jurisdictions to secure arrests and extraditions. These reasons are considered reasonable.

Table 2.5. Outgoing extradition requests

	2020	2021	2022	2023	2024	Total (%)
No of requests sent (excluding Brunei/Malysia)	**2**	**0**	**2**	**1**	**1**	**6 (100)**
Executed	0	0	1	0	0	1 (17)
Declined	1	0	1	0	1	3 (50)
Pending	1	0	0	1	0	2 (33)
Withdrawn by Singapore	0	0	0	0	0	0
Requests to Brunei/Malaysia	**4**	**14**	**28**	**23**	**34**	**103 (100)**
Executed	4	13	19	10	20	66 (65)
Pending or withdrawn	0	1	9	13	14	37 (35)

2.2.3. Seeking to facilitate asset recovery

180. While SOPs and NARS encourage LEAs to pursue international co-operation for asset recovery in serious cases through both formal and informal channels, more could be done to utilise formal international co-operation to secure better outcomes.

181. As a standard practice, all MLA requests include basic and BO information, which facilitates asset tracing. Forty-seven per cent of all outgoing MLA requests (110) concern the restraint of assets, enforcement of foreign confiscation orders, or request for assistance to seize any proceeds traced to the fraudulent transaction for the purpose of returning the sums to the victim. Singapore pursued the seizure, restraint and/or confiscation of SGD 144 million (USD 107 million) (including 3 properties) and secured the return of SGD 52 million (USD 38.5 million). Close to 60% of MLAs were executed by the requested country, but most (51%) were executed without any assets found for seizure/confiscation and repatriation (e.g. in situations where assets dissipated in the foreign country). Thirty-seven per cent of cases remain pending, including from the early 2020's, which shows limitations in securing international co-operation (See

Table 2.6). As stated in IO.8, Singapore does not seek to enforce its foreign confiscation orders abroad, which hampers final confiscation/repatriation of assets to Singapore.

Table 2.6. MLA requests (asset recovery[22])

	2020	2021	2022	2023	2024	Total (%)
# MLAs	24	18	17	12	39	110
Assets sought for recovery (millions)	SGD 10.7m + 2 properties	SGD 23.2m + 1 property	SGD 32.8m	SGD 89.3m	--	SGD 144.5m + 3 properties
Total Executed	17	12	12	7	17	65 (60%)
# Executed & assets (1)	1 (2 properties)	1 (1 property)	1 ($0.3m)	0	5 (SGD 51.3m)	8(7%) (SGD 51.6m + 3 properties)
Executed without assets recovered	16	11	11	7	12	57(51%)
Withdrawn by Singapore	1	1	1	0	1	4
Declined	0	0	0	0	0	0
Pending execution by requested jurisdiction	6	5	4	5	21	41 (37%)

Note: (1) this includes amounts that are frozen, seized, confiscated and repatriated where applicable.

182. Eighty-nine per cent of these outgoing MLA requests relate to fraud, while 11% concern ML. This distribution is in line with Singapore's risk and context to some extent and reflects its focus on addressing the growing threat of CEF. It is a missed opportunity not to have sought MLA for recovering assets related to any offence outside of fraud and ML, including the numerous offences designated as higher risk by Singapore.

[22] See Table 8.6, IO.8

Box 2.2. Seeking International Co-operation

Request for assistance to restrain a real estate property acquired using proceeds of crime

Between 2014 and 2018, employees of a Singaporean oil refinery, including the accused, misappropriated gasoil via unauthorised transfers to complicit vessels. The accused was convicted on 40 charges (under different provisions) and was sentenced on 2 August 2024, with over USD 800 000 in assets forfeited and funds returned to the refinery owner. Investigations revealed the accused had purchased a property (registered to him and his wife) in a Pacific State using the criminal proceeds.

To prevent asset dissipation, Singapore obtained a restraint order under S16, CDSA and sent an MLA requests in August 2021 to have the order registered (acted upon by the Pacific State in December 2021). In January 2025, following a plea bargain, the restraint order in Singapore was lifted to allow the property's sale, with proceeds returned to the victim. Singapore also asked the Pacific State to lift the restraint order accordingly.

Extradition on basis of reciprocity

A remisier at a FI in Singapore misappropriated over SGD 13 million (USD 9.6 million) from 15 victims over two years, using forged trading records and false entries to deceive them. The funds were used for personal expenses. The fugitive fled Singapore in January 2022 before police reports were filed. A warrant of arrest and INTERPOL Red Notice were issued, and with the help of multiple jurisdictions, she was located and arrested in a European State. Despite no formal extradition treaty, the European State accepted Singapore's assurance that it will use its best efforts to comply with a future request by the European State for the return of a suspect involving a similar criminal offence and circumstances, subject to the laws of Singapore. The fugitive initially expressed intent to surrender but later sought asylum, which was denied. The person was extradited in July 2023 and the prosecution is ongoing.

2.3. Seeking and providing other forms of international co-operation for AML/CFT purposes, including asset recovery

183. Competent authorities actively use informal channels as a means to an end and to support formal co-operation mechanisms, although greater alignment with risk could be achieved. This is appropriate and a positive feature of Singapore's approach to international co-operation, but as noted above, it cannot replace formal co-operation channels when needed. Singapore leverages on various mechanisms such as multi-lateral networks, bilateral and diagonal co-operation, and joint analysis and investigations to provide a wide range of information, such as criminal records and intelligence, information on the identity of a suspect, financial information and intelligence. There are limitations to the provision of basic and BO information, which has a minor impact on this type of co-operation.

184. Despite guidelines and SOPs highlighting the importance for LEAs to seek international co-operation, informal co-operation aligns with risks to some extent. The number of requests made by some competent authorities (e.g. STRO, IRAS, CPIB) in respect of several high-risk offences (such as corruption and tax crimes) is much lower in comparison to those made in respect of fraud. This is similar to trends identified in respect of formal co-operation request (MLA issued by Singapore – see Table 7.4), indicating that informal co-operation in this area is ineffective and not sufficiently supportive of formal co-operation channels.

2.3.1. FIU

185. STRO is used in an appropriate and timely manner to seek and provide information to foreign counterparts, either to support its own purposes or those of other competent authorities.

186. STRO plays a central role in international co-operation, using Egmont Secure Web and other secure channels to exchange information with foreign FIUs, including non-Egmont members, on a reciprocal basis. It sent 1 465 RFAs (predominantly on SPF's behalf), receiving responses to 86%. Most (73.5%) were submitted on behalf of LEAs, predominantly SPF, and according to authorities, these generally support investigations, asset tracing and provisional measures, highlighting STRO's role in asset recovery (see Box 2.3). RFAs broadly align with risks, focusing on fraud/CEF (46%) and ML (37%). However, fewer requests target tax crimes (4%), T/TF (3%), and corruption (2%), suggesting underuse of international co-operation to pursue some higher-risk areas.

187. STRO provides appropriate and prompt assistance where requested, having received 1 744 RFAs and responded to 97%. In line with Egmont Standards, STRO responds to urgent requests within 7 days (per SOPs) and over 98% of non-urgent requests within 60 days. This timing is due to the need for STRO to verify the nature of the offence, and whether assistance can be provided under Singapore's legislation. Around 30% of RFAs involved financial institution data, which should be quicker to obtain and share. Although STRO does not keep detailed statistics on assistance provided, RFAs typically involve (i) information from STRO's databases, (ii) other information (e.g. bank or transaction records) obtained from REs (used in approximately 23% of requests) (iii) BO information and (iv) STRO's own analysis. STRO may also consult other competent authorities – e.g. ACRA on BO information – when responding to RFAs. STRO also shares information spontaneously, sending 834 Spontaneous Exchange of Information (SEI), (mainly to USA, UK, Australia) on corruption and bribery, fraud, and ML, which generally aligns with risks.

188. Statistics on requests to freeze or recover funds are limited (but Singapore indicates STRO receives these). STRO cannot directly suspend transactions (this power lies with LEAs following the initiation of a domestic investigation, which can increase the risk of asset dissipation (see R.38). Case studies, however, show that STRO and LEAs generally act quickly when such requests arise (Box 2.3).

189. While feedback from the Global Network indicates that STRO's assistance is generally satisfactory, some jurisdictions noted gaps in transaction details and limited information on financial flows, and a few delegations highlighted that responses could be timelier.

Box 2.3. International co-operation by STRO

Use of RFA in domestic investigations

STRO received an RFA from a North American counterpart in November 2023 regarding a person who was suspected of a fraud offence and transferring fraudulent funds to a Singaporean investment account. In response, STRO conducted further inquiries (including checks with the financial institution) and shared information to the foreign counterpart within three weeks, indicating the possible presence of proceeds of crime. STRO received consent from the counterpart to share this information with SPF, which promptly seized SGD 1 million (USD 740 000) on the accounts. The case – including efforts to repatriate the assets – is ongoing.

Application of provisional measures (suspension of transactions) and timely assistance provided

In 2022, STRO received a RFA from a foreign FIU via the Egmont Group's BEC Rapid Response channel regarding a BEC scam involving approximately USD 7.5 million transferred to Singapore. Leveraging on the ACIP mechanism, STRO immediately alerted the receiving bank and CAD through established ACIP channels. The receiving bank temporarily held the funds to allow CAD to investigate. Close co-ordination allowed the full amount to be recovered and returned to the victim within the same week.

2.3.2. Law enforcement agencies (LEAs)

190. LEAs regularly use international co-operation to detect offences, advance investigations, and to trace and recover assets, providing timely assistance overall (Box 2.4).

191. Singapore has robust operational systems, supported by SOPs and MOUs, ensuring confidentiality and timely responses: LEAs should generally respond within three working days for interim acknowledgment, seven working days for simpler cases, and one month in more complex ones. Dedicated units manage cross-border engagement, such as the International Co-operation Department (SPF-ICD) for INTERPOL-related matters (e.g. screening against Red Notices and INTERPOL's databases). The dedicated units handling international co-operation within the respective LEAs are the International Co-operation Branch for SPF-CAD, the International Operations Desk and Investigation Division for CNB, and the International Affairs & Liaison Branch and Intelligence Division for CPIB. Also, within SPF, the ASC and CID's Cyber Crime Command play key roles in facilitating co-operation, particularly in CEF cases. ASC operates a 24/7 service to enable rapid seizure of suspected criminal proceeds and direct engagement with foreign counterparts.

192. LEAs generally share a wide range of information, apart from BO information concerning Unregistered Foreign Companies. Even in the absence of domestic investigations, LEAs may share property valuations and land titles. Information typically sought by LEAs includes witness statements, criminal records, involvement in foreign investigations, and BO or company data, all of which support effective cross-border enforcement. Where coercive powers are required, foreign authorities must submit formal MLA requests.

193. Operational liaison channels – such as attachés in China and Indonesia, accredited officers in Singapore, and seconded officers at INTERPOL – enhance co-operation. Singapore engages bilaterally under MoUs or reciprocity and multilaterally through INTERPOL, ARIN-AP, WCO, IACCC, and the GLOBE Network, complemented by joint investigations (which has led to successful repatriation of funds), regular visits and training to strengthen relationships.

194. Singapore demonstrates active international engagement. LEAs received 3 741 INTERPOL requests, mainly on fraud (36%), ML (8%), cybercrime (7%), and corruption (1%), executing 84% (based on 2023–2024 data), and rejecting only 2% (usually where no offence was apparent or coercive powers – requiring an MLA – are required). SPF also plays a significant role seeking co-operation, sending approximately 11 975 requests to 152 jurisdictions, mainly targeting regional and material counterparts (such as Malaysia, China, Hong Kong China, Philippines, Thailand, UK and USA). These requests focus on fraud, ML, and cybercrime, reflecting Singapore's risk exposure to a good extent. While comprehensive statistics are not available for the entire period (nor on the status of the requests), the volume and thematic focus of requests suggest a good alignment with risk and operational priorities.

195. Singapore does not maintain statistics on TF for confidential reasons, but case studies (see IO.9) and onsite discussions show that ISD and SPF both use informal channels as required. As noted in IO.9, it is a point of strength that Singapore shares pertinent information on TF investigations with international counterparts, through formal and informal channels.

196. Singapore also does not maintain statistics on whether each outgoing MLA request follows informal co-operation. Interviews with the authorities and some case studies suggest LEAs routinely rely on informal channels to obtain preliminary information. These channels are sometimes used to trace assets, including BO and bank account information, which can subsequently support formal actions such as asset seizure and confiscation. Most asset recovery requests target regional and materially significant partners and focus on fraud and ML offences. SPF plays a central role in asset recovery, successfully recovering over SGD 102 million (USD 75 million) through these channels. Where credible and actionable information exists that property in Singapore is linked to criminality, Singapore is able to assist foreign authorities in seizing property without delay with assistance having been provided in some cases within a day of receiving a request.

197. As identified in IO.5, the basic and BO information of Unregistered Foreign Companies is held only by the reporting entity. Unregistered foreign companies are those that are not regarded as carrying on business in Singapore and which only carry on activities in Singapore such as maintaining any bank account, investing any of their funds, or holding any property in Singapore. Given that LEAs require reason to suspect the commission of an arrestable offence to open an investigation and seek basic and BO information in relation to such companies, there may be delays or an inability in providing assistance where a threshold to open an investigation cannot be met. However, where LEAs detect information in STRO's database that is relevant to the foreign LEA's investigations, they will alert STRO, which may then send a spontaneous exchange of information (SEI) to the relevant foreign FIU, with explicit consent to share the information with the relevant foreign LEA.

Box 2.4. International co-operation by LEAs

3B$ case

SPF actively engaged with foreign authorities, sending 33 requests to 10 jurisdictions for information to, among others, trace assets and the whereabouts of suspects placed on INTERPOL notices (27 accused were investigated). In parallel, SPF received 63 requests from 18 jurisdictions. STRO also collaborated with at least 10 foreign FIUs to exchange financial intelligence supporting foreign investigations. LEAs shared detailed case findings, forensic data, and/or banking information with some jurisdictions. SPF worked closely with counterparts in two jurisdictions to facilitate their submission of MLAs seeking financial and court records.

Provision of timely assistance to foreign jurisdictions (Anti Scam Centre)

Upon the receipt of a police report lodged by a European conglomerate alleging embezzlement by its staff, CAD took immediate steps to work with the Anti-Scam Centre and various banks to expeditiously seize these accounts by the following day. About USD 70 million was recovered in Singapore across 15 bank accounts held by 12 shell companies and one individual.

CAD also actively pursued the funds after dissipation from the Singapore bank accounts. CAD reached out to 26 jurisdictions through INTERPOL and FIU counterparts to share relevant information and trace the funds. This resulted in an additional USD156 000 being returned to Singapore, which was subsequently seized and returned to the victim, along with the rest of the seized funds.

2.3.3. Supervisors of FIs, VASPs and DNFBPs

198. MAS regularly co-operates with foreign counterparts, either on a bilateral basis, during forums and conferences (Table 2.7). MAS can share information both upon request and spontaneously. Limited statistics show that MAS co-operates mainly with regional counterparts, other international financial centres and established partners (USA, Australia, Hong Kong, etc.).

199. Most of the information MAS seeks from counterparts concerns fit and proper checks, licensing and regulatory information, which help it conduct its supervisory functions (Box 2.5). There are limited instances of MAS seeking inspection reports. Where requested, MAS provides timely information to counterparts when all the confidentiality requirements are met. These requests overwhelmingly concern fit and proper information where feedback from the Global Network is generally positive). MAS granted 20 AML/CFT examinations on FIs in Singapore by foreign counterparts, out of which one was a joint inspection in 2023 and spontaneously shared six inspection reports to foreign counterparts.

Table 2.7. International co-operation by MAS

	2020	2021	2022	2023	2024	Total (%)
Outgoing requests by MAS	790	849	659	692	721	3 711
Fit and proper checks	310	314	305	278	295	1 502 (40)
Regulatory information	229	252	163	171	168	983 (26)
Exchange of inspection reports	0	1	0	0	1	2 (0)
Licensing information	229	251	163	168	168	979 (26)
IOSCO	22	31	28	75	89	245 (7)
Incoming requests by MAS	102	88	111	134	133	568
Fit and proper checks	88	77	79	90	104	438 (77)
Regulatory information	3	6	13	21	15	58 (10)
Exchange of inspection reports	4	1	2	0	0	7 (1)
Joint examinations	0	0	0	1	0	1 (0)
Licensing information	3	3	11	18	13	48 (8)
IOSCO	0	0	1	0	1	2 (0)
Others (on-site examination/supervisory visit)	4	1	5	4	0	14 (2)
Information requests executed by MAS	100	83	92	102	111	488

200. DNFBP supervisors appear to engage with foreign counterparts to exchange supervisory and regulatory information to a reasonable extent and for various purposes, although there is no detailed information. For example, ACRA has shared information with audit regulators from two neighbouring countries pertaining to registration of Singapore's PAs and public accounting entities (PAEs) (collectively referred to as accountants) in those States, including the dates and results of audit examinations and information on any disciplinary proceedings. Between 2020 and 2024, GRA also exchanged information in over 180 outgoing and 40 incoming requests pertaining to the suitability of applicants with its nine MOU partners. Such requests are generally sent for higher-risk applicants to gather information on suitability, including their compliance records and any licence rejections by the foreign gambling regulators.

Box 2.5. International co-operation for supervisory purposes

Sharing Fit and proper information

In 2021, MAS received requests from a foreign supervisor for fit and proper information concerning an entity incorporated in Singapore. This was triggered further to inquiries conducted by the foreign Supervisor into a parent company of the entity in Singapore. MAS provided information concerning both the entity in Singapore and relevant information concerning its parent company. The foreign counterpart ordered the entity to cease operations due to its inability to meet pre-licensing conditions. MAS also used this information when deciding not to renew the entity's Singaporean license.

2.3.4. Customs and tax authorities

201. Singapore demonstrates a proactive approach to international co-operation for customs and tax purposes, which is appropriate considering Singapore's risk and context as an IFC.

202. With respect to customs, SC leverages SOPs when requesting information from foreign LEAs to investigate customs offences, detailing the case background, verification steps, and specific information sought, which may be linked to asset recovery. SC has received 109 spontaneous alerts from foreign administrations and acts on them where relevant and made 179 exchanges of information (EOI) requests to foreign counterparts in the assessed period. SC also provides assistance to counterparts in response to 551 EOI requests received (none were refused), for example to provide information on goods transhipping through Singapore which are suspected to be intended to be smuggled to foreign jurisdictions. This assistance is generally provided within one month, or quicker if the request is urgent. Based on its surveillance and operational activities, SC sent 182 spontaneous disseminations about suspicious activity with counterparts, either bilaterally or through the World Customs Organisations, which has helped in their enforcement activities.

203. With respect of tax, IRAS leverages a broad network of EOI arrangements with 156 jurisdictions to support enforcement, including in tax evasion cases. Requests are managed by a dedicated EOI team within IRAS's International Tax and Relations Division, ensuring compliance with international standards and domestic legal requirements. All outbound requests are tracked, with follow-ups initiated if responses are delayed beyond 90 days (which is the international standard), and complex cases are escalated through direct engagement. Between 2020 and 2024, IRAS sent 90 tax-related requests in relation to suspected tax evasion cases and sent a total of 4 375 spontaneous EOIs to foreign partners. IRAS received 1 800 information requests from foreign partners and executed 98.2% of these (the remainder were withdrawn, with only a fraction declined by Singapore where they do not meet the EOIR standards).

3 Financial sector and virtual asset supervision and preventive measures

The relevant Immediate Outcomes considered and assessed in this chapter is IO.3. The Recommendations relevant for the assessment of effectiveness under this chapter are R.9-21, 26, 27, 34 and 35 and elements of R.1, 29 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Singapore has a robust licensing framework in place to ensure that criminals and their associates are not beneficial owners or holders of controlling interests in FIs and VASPs. All supervisors focus on identifying unlicensed FI/VASP activity, generally relating to the provision of remittance services and VASP-related services. SPF investigates unlicensed activities on the basis of referrals from supervisors but the penalties for conducting unlicensed activities are not effective, proportionate and dissuasive.

b) MAS has a robust understanding of country-level and sector-level ML/TF risks from its involvement in the NRA process and the dynamic approach. Institutional-level risk understanding for the financial and DPTSP sectors is varied and was established through three separate components and the day-to-day consultation and co-ordination between MAS' AML specialist department and prudential supervisory departments. This process is not thoroughly systematised and documented and does not result in a residual risk rating on an institutional level to inform supervisory planning. MinLaw has a reasonable understanding of ML/TF risks affecting the country and a less in-depth understanding of ML/TF risk on an individual moneylender basis.

c) MAS' work to ensure that FIs and VASPs understand ML/TF risks and AML/CFT obligations is a strength of Singapore's system. FIs and VASPs have a solid understanding of ML/TF risks. MinLaw has taken a less developed range of measures to promote industry awareness, and moneylenders have an adequate understanding of the ML/TF risks facing their business.

d) FIs and VASPs generally demonstrated a comprehensive understanding of AML/CFT obligations and risk control measures, recognising the need to implement

enhanced due diligence and other risk mitigation measures when dealing with high-risk scenarios such as PEPs or clients from high-risk jurisdictions. However, number of STRs submitted by in some higher risk sectors (e.g. DPTSP) or for some ML typologies that Singapore is highly exposed to (e.g. TBML) appears not proportional to the risk identified.

e) MAS' supervision of FIs/VASPs consists of supervisory activities driven by three components: FIRA (i.e. inherent risk assessment) and risk surveillance by AMLD, as well as day-to-day controls-based supervisory activities conducted by the nine prudential supervisory departments and AMLD. These three components allow MAS to respond to risks in an agile manner. However, supervisory activities are not planned in accordance with institutional level residual risks, nor in a documented and systematised risk-based supervisory process across MAS. There is limited coverage of the supervised population for the FIRA and risk surveillance based supervisory activities. Singapore does not track complete statistics on the scope and/or findings of controls-based supervisory activities, which account for almost all of MAS' supervisory activities, to develop an understanding of the effect that supervisors are having on their supervised population. The broad coverage of controls-based supervisory activities can, based on case studies provided to demonstrate their rigour, to a reasonable degree, be considered effective in supervising FIs/VASPs.. The intensity of supervisory activities for some sectors lacks depth as they rarely find breaches. For moneylenders, entities assessed to pose higher risk are generally inspected more frequently than lower risk entities, but overall, there is room to align supervision more proportionately with the lower ML/TF risks posed by the sector.

f) MAS adopts a range of remedial and sanctions depending on the severity of breaches. MAS has increased its sanctions since the last MER, particularly against individuals and such actions are generally published for deterrent effect. The number of remedial actions and sanctions remains relatively low. The level of financial sanctions remains not proportionate when considering the size of relevant FIs/VASPs, the serious nature of breaches, as well as Singapore's risk and context. Singapore's remedial actions and sanctions are complemented by close monitoring, strong industry engagement and public-private partnership, which has fostered a stronger compliance culture amongst FIs/VASPs and drive improvements in AML/CFT controls amongst FIs/VASPs.

Recommended Actions (RAs)

Singapore should:

a) Have MAS systematise its model of identifying and assessing residual risks at institutional level to ensure and deliver a clear consolidated view of ML/TF risk across the AMLD and nine supervisory departments.
b) Have MAS implement an updated sanctions framework that imposes more dissuasive and proportionate financial sanctions for FIs/VASPs found with breaches of AML/CFT obligations.
c) Take measures to impose more dissuasive and proportionate sanctions for individuals and entities found to be providing unlicensed financial and VASP-related services.

d) Have MAS conduct further outreach to enhance reporting entities' understanding of suspicious transactions, particularly in some higher risk sectors reporting lower number of STRs and on ML typologies where there is limited reporting, such as TBML.

e) Have MAS expand the use of COSMIC to other FIs beyond the limited set of commercial banks, and to cover financial crime risks beyond the three currently covered.

Overall Conclusions on IO.3

Singapore has a comprehensive licensing framework to ensure criminals, and their associates, are not beneficial owners or holders of controlling interests in FIs or VASPs. Unlicensed activity is effectively addressed through criminal investigations, but penalties could be more commensurate to the gravity of offences committed.

MAS has a robust understanding of country-level and sector-level ML/TF risks, but varying understanding of residual risk at institutional level. The process to identify, assess and document institutional residual risks between MAS' AMLD and the nine prudential supervisory departments can be better systematised.

Singapore invests significant resources into ensuring that FIs and VASPs understand their ML/TF risks and AML/CFT obligations. As a result, generally, FIs and VASPs understand their ML/TF risks and AML/CFT obligations and apply appropriate mitigating measures well. STR reporting is relatively low for some higher-risk sectors (e.g. DPTSPs) and major ML typologies (e.g. TBML) in Singapore.

The three components of MAS' supervisory activities allow MAS to address potential vulnerabilities and respond to emerging threats in an agile manner. There is broad coverage of supervisory activities, but these activities are primarily controls-based activities where there is no complete statistics on the scope and/or findings. Accordingly, the broad coverage of controls-based supervisory activities can, to a reasonable degree, be considered effective in supervising FIs/VASPs.

Singapore has stepped up sanctions and held individuals to account for their lapses in recent cases, however, the number of remedial actions and sanctions remains low and there is need to improve the dissuasiveness and proportionality of sanctions. Singapore complements these remedial actions and sanctions with close monitoring, strong industry engagement and public-private partnership, which is observed to have fostered a stronger compliance culture amongst FIs/VASPs and drive improvements in AML/CFT controls amongst FIs/VASPs.

Singapore is rated as having a Substantial level of effectiveness for IO.3.

Immediate Outcome 3

204. There are two AML/CFT supervisors for FIs and VASPs in Singapore: MAS and MinLaw. MAS supervises banks, external asset managers (EAMs), fund management companies, broker dealers, corporate finance advisory firms, approved trustees, the central depository, insurance brokers, financial advisors, DPTSPs, payment service providers (PSPs), money changers, non-bank credit card issuers, finance companies, direct life and composite insurers, approved exchanges and recognised market operators, while MinLaw supervises moneylenders.

205. In assessing the effectiveness of Singapore's supervision of FIs and VASPs, the Assessment Team placed the most weight on the banking sector, given its size, importance, global reach and complexity. It also placed significant weight on PSPs with cross border money transfer services (CBMT) sector, given the large amount of remittance activity, including with some high-risk jurisdictions, the DPTSP sector, given the volume and growth of VA-related activities in Singapore, and EAMs, who act as intermediaries for high-net-worth customer between customers and banks for wealth management. The Assessment Team placed lower weight on sectors covered for AML/CFT requirements that have a lower risk and/or materiality, including corporate finance advisory firms, non-bank credit card companies, approved trustees, insurance brokers, direct life and composite insurers, central depository, approved exchanges, recognised market operators, and moneylenders.

206. Singapore takes a tech-agnostic view and considers digital capital markets product (dCMP) tokens part of capital market products under other FI sectors and are not considered separately as a sector either in Singapore or for this report. Singapore instituted a licensing regime for Digital Token Services Providers (DTSPs) offering virtual assets services exclusively to overseas customers one day prior to the beginning of the AT's visit to Singapore with the expressed policy goal of approving zero applications for the regime given the risk associated with the business. No applications to become a DTSP had been received at the time of onsite visit and, consequently, no assessment can be made on this sector. The term VASP in this report refers only to the DPTSP sector.

207. In 2016, MAS set up a dedicated AML Department (AMLD), which consolidated the responsibilities previously carried out by different departments. There are over 40 staff members in AMLD, with good knowledge and experience on AML/CFT, allocated into three units separately responsible for overseeing (i) policy formulation, (ii) compliance of higher risk banks and non-bank institutions and (iii) risk surveillance. In addition, across the Financial Supervision Group in MAS, nine prudential supervisory departments with over 400 staff cover AML/CFT issues as part of their prudential supervision of FIs and VASPs.

3.1. Licensing, registration and controls for FIs and VASPs preventing criminals and associates from entering the market

3.1.1. Market entry controls

208. Singapore has a robust process for licensing and approval of FIs and VASPs. MAS is responsible for licensing and approval for FIs and VASPs except for moneylenders[23], which are under the purview of MinLaw. All FIs and VASPs, including foreign legal persons, must be licensed before they can carry on activities in Singapore, in addition to being registered with ACRA as a legal person (see IO.5).

209. MAS undertakes rigorous licensing assessments for FIs and VASPs through open sources, applicant submissions including AML/CFT policies and procedures and, where relevant, strength of home country supervision. MAS may reject the application or require additional mitigation actions within an agreed timeframe. Examples of such mitigation actions include independent audits, directives to bolster the AML/CFT compliance function and the appointment of independent directors to enhance the governance framework. Applicants may choose to withdraw their application if they anticipate rejection or considered the additional mitigation measures too stringent for their business. The withdrawal/rejection rate vary significantly by sector, largely based on the maturity of the sector, with banks seeing very few and the DPTSP sector witnessing an 80% withdrawal/rejection rate over the evaluation period.

[23] The Central Depository Limited (CDP) is subject to a designation regime (akin to licensing) in line with the Securities and Futures Act 2001.

Box 3.1. Risk Surveillance leads to Voluntary Withdrawal of License Application

In October 2022, MAS reviewed nine STRs filed by a DPTSP licence applicant (DPTSP A) on its customers. MAS noted these customers had no clear nexus to Singapore (foreign companies with foreign authorised signatories/BOs/directors), a majority were only incorporated recently and were not in VA-related business. Most of their suspicious transactions occurred shortly after onboarding/change of BO, and large and/or pass-through transactions were not detected in a timely manner.

MAS assessed that there were weaknesses in DPTSP A's onboarding processes, risk assessment, ongoing account and transaction monitoring, and STR filing controls. Despite repeated queries, DPTSP A maintained that postmortem reviews on its processes were not required as it had performed thorough investigations prior to the filing of each STR and the relevant accounts had been closed. Given MAS' feedback that DPTSP A was unable to demonstrate the ability to meet the AML/CFT requirements and other licensing criteria, DPTSP A subsequently withdrew its application in September 2023 and ceased regulated business activities in Singapore. As per MAS' process, DPTSP A was required to provide a comprehensive wind-down plan upon withdrawal, that was subject to monthly monitoring by MAS to ensure implementation. This includes clear communications to clients and stakeholders on its cessation in Singapore, taking down of its Singapore website and return of client assets and monies.

210. MAS conducts high quality fit and proper checks for required personnel, including controllers, substantial shareholders (20%+ in direct or indirect ownership), directors, and senior management at the licensing step and upon any changes. The Guideline on Fit and Proper Criteria is published on MAS website and updated regularly. Fit and proper checks take into account criminal records checks, screening with STRO/LEAs, screening on STRs, sanctions screening and open-source news checks, background checks with foreign supervisors, amongst other sources. MAS may still approve individuals if their past convictions are evaluated to not have impact on their fitness and/or propriety on a person-by-person evaluation basis (e.g. unrelated offence, significant amount of time elapsed).

211. MAS rejects applicants or informs applicants to withdraw their applications when they believe relevant individuals are not suitable for the position. During the assessment period (2020-2024), 84 and 24 applications were rejected and withdrawn respectively, due to concerns over AML/CFT related factors.[24] Noting risks associated with VASPs as an emerging sector, MAS applied more stringent measures on fit and proper for relevant individuals and these more stringent measures resulted in a higher rejection/withdrawn rate.

212. FIs and VASPs are required to inform MAS of any matter that would affect the fitness and/or propriety of the required personnel. If they are found to no longer be fit and proper, they will have to dispose of shares or relinquish their position. MAS also conducts checks on required personnel where there is adverse news or STRs that implicate an individual, or where there are changes for business reasons such as through takeovers or other changes to ownership structures.

213. Singapore put in place a moratorium on new moneylender licenses in 2012. Since the six new licenses granted in 2018-19 for testing new business models, there were no license applications during the review period. Moneylenders are required to seek approval from Insolvency and Public Trustee's Office under MinLaw to (i) employ or engage any person to assist in the moneylending business; (ii) appoint a director / a person taking part in the management of the business; or (iii) make changes concerning substantial shareholders. These individuals are screened at the time of any change and at least annually

[24] Singapore indicated that it did not capture rejection/withdrawal statistics for some sectors, hence the numbers quoted here are based on Singapore's record collected on a best effort basis and not exhaustive.

against police records, sanctions lists and open-source information. If individuals are found to no longer be fit and proper, then they will be disqualified from involvement in the moneylending business and in the case of substantial shareholders, be required to reduce their substantial shareholding to a level required by the Registrar.

214. Overall, the licensing framework in Singapore, including market entry and ongoing monitoring, is effective at preventing criminals and their associates from owning controlling or holding key management positions in FIs and VASPs to a very large extent.

3.1.2. Detecting and addressing breaches

215. Unlicensed activities most often occur for businesses illegally conducting virtual asset services provision and effecting remittance, i.e., individuals/entities that would fit in the DPTSP and PSP with CBMT sectors, if licensed. MAS uses multiple tools to detect and address unlicensed operators in these sectors as a priority, and in other sectors under its purview more generally. This includes analysing STRs, querying corporate registry information, whistleblowing channels, the use of blockchain analytics providers and other open-source information. Upon detection, MAS alerts the public of individuals/entities that may be conducting regulated activities without licences on their Investor Alert List, where there were 78 new entries during the review period, many of which were providing DPTSP-type services. MAS ensures that the public is warned of potential unlicensed operators and there is appropriate enforcement against unlicensed activities. MinLaw relies on complaints from the public to commence actions into potential unlicensed moneylenders.

216. Where there are breaches of licensing requirements, MAS and MinLaw refer the cases to the SPF for enforcement. The SPF pursues cases when referred and cases are brought to conviction in a good number of instances. From 2020-24, SPF opened 4 695 investigations into individuals and entities suspected of conducting unlicensed moneylending, and payment services such as remittance and DPTSP services. 292 persons were convicted for unlicensed moneylending and payment services in the same period. The sentences meted out were up to 78 months' imprisonment, fines up to SGD 700 000 (USD 542 000) for those convicted for unlicensed moneylending, and up to 12 months' imprisonment and fines of up to SGD 100 000 (USD 74 000) for unlicensed payment services. While Singapore has recently stepped-up sanctions meted out for persons conducting unlicensed payment services, the sanctions given remain not proportionate or dissuasive to the crimes committed, for example in the case of Zin Nwe Nyunt who was sentenced to 18 months' imprisonment in July 2025 for conducting over SGD 640 million (USD 454 million) in unlicensed remittances.

3.2. Supervisors identifying understanding and promoting FI and VASP understanding of ML/TF risks

3.2.1. Identifying and maintaining an understanding of the ML/TF risks in the different sectors and types of FIs and VASPs and of individual FIs and VASPs over time

217. MAS has a reasonably sound understanding of country-level and sector-level ML/TF risks as informed by the RTIG process (see IO.1) but their way of identifying, assessing and understanding of the residual ML/TF risk facing individual FIs and VASPs can be improved.

218. MAS' country-level understanding has been developed through the dynamic approach of identifying risks using an iterative process as a major contributor to Singapore's RTIG and various risk assessments. While MAS published a range of guidance, standalone sector risk assessment documents are

not produced outside of the NRA. Based on the outcome of ML NRA, MAS categorised regulated financial sectors into four tiers in accordance with risks associated with each sector (See Table 5.3). MAS would also consider the TF and PF NRA's findings and risk ratings to further calibrate its supervisory approach for the respective sectors. For example, as PSPs with CBMT were assessed to be of highest TF risk, MAS had subjected higher risk entities in this sector to a shorter supervisory baseline compared to other Tier 2 entities and had focused on more PSPs with CBMT as part of its TF thematic review.

219. MAS adopts a multi-layered and dynamic approach to identify and assess the ML/TF risk facing individual FIs and VASPs in Singapore, specifically through three components: (i) inherent risks assessment (FIRA), (ii) controls information, and (iii) risk surveillance insights. Their understanding of residual risks at institutional level is established through daily co-ordination between the AMLD and the nine prudential supervisory departments, with AMLD primarily accountable for inherent risk assessment (i.e. FIRA) and risk surveillance insights, and the nine supervisory departments and AMLD responsible for controls information. The process to bring this information together to drive work planning twice yearly is not thoroughly systematised and documented.

220. FIRA is a tool that measures inherent ML/TF risk through information provided by FIs/VASPs to AMLD through periodic questionnaires and other materials. FIRA focuses on six risk areas: (i) business risk, (ii) cross-border risk, (iii) tax risks, (iv) corruption risk, (v) TBML risk, (vi) TF/PF risk. These factors cover most but not all major risks identified in NRAs. While risks on fraud and organised crime are the most prominent threats identified in Singapore, they have not been assigned as any dedicated contributing factor in FIRA but are accounted for indirectly via indicators for other existing risk areas. FIRA's methodology is periodically reviewed and updated, with the last major review having been completed in 2020.

221. The periodicity of FIRA questionnaires is driven by the sector risk rating from the NRA, with the highest risk sector (banks) being required to submit information annually while the lowest risk sectors being required to update information every four years. FIRA contributes to understand ML/TF risks of individual FIs and VASPs over time but only considers inherent risk. The FIRA process rates each FI and VASP as being a high risk, medium-high risk, medium-low risk or low risk.

Table 3.1. Breakdown of FIs and VASPs under MAS supervision by Inherent ML/TF Risk Rating

Sector NRA Risk Rating	Sector	High	Medium-High	Medium-Low	Low
Tier 1	Banks	19 (12%)	18 (11.4%)	32 (20.3%)	89 (56.3%)
Tier 2	DPTSPs	7 (24%)	7 (24%)	15 (52%)	0
	PSPs with CBMT services	13 (7%)	55(28%)	97 (48%)	34(17%)
	EAMs	6 (3.6%)	13 (7.7%)	33(19.6%)	116 (69%)
Tier 3	Fund management companies (excluding EAMs)	1 (0%)	3 (0%)	188 (20%)	752 (80%)
	Money changers	0	0	0	246 (100%)
	PSPs without CBMT services	0	0	1 (12.5%)	7 (87.5%)
	Broker dealers	4 (3%)	7 (5%)	47 (33%)	85 (59%)
	Corporate finance advisers	1 (1%)	1 (1%)	36 (28%)	91 (70%)
Tier 4	Approved Trustees	1 (6%)	0 (0%)	3 (18%)	13 (76%)
	Direct life insurance companies	1 (4%)	1 (4%)	7 (27%)	17 (65%)
	Securities depository	0	0	0	1 (100%)
	Financial advisers	1 (1%)	1 (1%)	28 (20%)	111 (78%)
	Finance companies	0	0	0	3 (100%)

222. The FIRA results are, in most cases, aligned with NRA sector risk ratings. There is a misalignment of the FIRA results with the NRA sector ratings with regard to the DPTSP sector. MAS has decided to identify a higher proportion of high-risk entities in DPTSP sector and apply closer oversight for this sector, a medium-high risk sector, than it does for its high-risk sector (banks) as it considered DPTSPs to be less familiar with AML/CFT requirements and less risk-aware than more mature sectors (see also Table 3.2). MAS did not reflect this view in their risk assessment for the sector accordingly or update FIRA. This yields a logical result but demonstrates that MAS' risk understanding for the sector is not consistent with its own FIRA risk model or with the actual changes in the risk environment, even when acknowledged by MAS.

223. Completely separately from the FIRA assessment, MAS, employs its second component whereby its nine prudential supervisory departments and AMLD carry out day-to-day controls-based supervision with a view to assessing the robustness of AML/CFT controls at the institutional level. MAS reported that AMLD, as the 'control tower' on AML/CFT matters, coordinates with the nine supervisory departments on day-to-day manner to assess, understand the residual risk at institutional level. However, this process for assessing residual institutional level risk is not thoroughly conducted in a systematised and documented manner(i.e., there is no residual risk scoring per institution).

224. MAS had been focusing more of its recent efforts on its risk surveillance programme, its third component, which identifies and monitors ML/TF/PF risks in MAS' regulated sectors using data analytics and information/intelligence from both domestic and foreign sources. The data is analysed to identify networks of suspicious activity through network analysis as well as broader emerging risk themes and concerns identified through RTIG. Higher risk networks are identified, from which specific institutional risks or accounts are sifted out for further supervisory follow-up. Thematic risks identified are consolidated into reports which are disseminated to relevant supervisory departments within MAS helping them improve understanding of key risks and planning of supervisory activities. Higher risk thematic areas covered recently based on risk surveillance includes, for example, wealth management, SFOs, DPTSPs and VCC sectors.

225. MAS is also continually enhancing its surveillance capabilities. As an example, Singapore launched COSMIC (see Box 3.3) in 2024 with six participating FIs and the insights/data gained through COSMIC contributes to MAS' risk surveillance capabilities. COSMIC identifies material networks of high-risk actors for further analysis and follow-up. The risk surveillance programme complements the FIRA and controls-based assessments, and MAS has a process to override the FIRA inherent risk ratings where these do not align with supervisors' risk understanding from risk surveillance. However, this overriding process is implemented on an individual case-by-case basis and operated as a separate line of work. Further, risk information gained through risk surveillance does not join up with the controls information in a systematic manner.

226. Overall, MAS has a reasonably sound understanding of country-level and sector-level ML/TF risks. Their understanding of residual ML/TF risk facing individual FIs and VASPs is varied due to the lack of a systematised mechanism for consolidating risk information across its three risk assessment components. MAS already has all the appropriate risk assessment components but has not yet brought all of these together in a systematic manner to form a net residual risk understanding for individual FIs and VASPs. FIRA considers only inherent risks despite MAS having substantial information on controls implemented by FIs and VASPs. Insights from risk surveillance are not built into a residual risk calculation. These components can be combined in a more systematised manner to enhance MAS' understanding of risk at institution-level. Further, there is a lack of proper documentation of the net residual risks on an institutional level, it is merely a perceived understanding across MAS from daily interaction. It is crucial for MAS to develop, agree and maintain a shared risk understanding which could be accessed, understood, and utilised to guide the planning of AML/CFT supervisory activities across AMLD and the nine supervisory departments.

227. MinLaw has a reasonable understanding of ML/TF risks affecting the country and relies on the NRA for their country-level and sector-level understanding. MinLaw develops an understanding of the risks facing moneylenders during examinations, surveys, quarterly returns, feedback from the Credit Association of Singapore and the moneylenders themselves. This risk assessment process is less developed than MAS' efforts to understand the risk facing their covered entities and has led to consequently, a less in-depth understanding of ML/TF risk on an individual moneylender basis.

3.2.2. Promoting FI and VASP understanding of ML/TF risks and AML/CFT obligations

228. MAS' work to ensure that FIs and VASPs understand their ML/TF risks and AML/CFT obligations is a strength of Singapore's system. MAS conducts four lines of activity to ensure that FIs and VASPs are informed: supervisory uplift, guidance papers to set supervisory expectations, partnerships with industry and industry engagement.

229. Supervisory Uplift: In 2022, MAS launched the supervisory uplift programme which comprises intensive bilateral engagement with Singapore's domestic systematically important banks (DSIBs) and digital banks, making up 90% of market share of retail and small and medium enterprise banking in Singapore. The banks are required to develop multi-year roadmaps with measurable action plans for each bank to elevate its AML/CFT controls, to address the following key focus areas: governance, risk surveillance and execution of AML/CFT requirements. This programme has generated outcomes, including a significantly increased number of STRs and exited customers following the use of data analytics (270 STRs and 318 exits in Q2 2022, compared to 2 694 STRs and 2 676 exits in Q2 2024), and the detection of a customer potentially facilitating sanctions evasion.

230. Guidance Papers: MAS regularly issues guidance papers to raise risk awareness and assist FIs and VASPs in complying with their AML/CFT obligations. During the past five years, MAS has issued 58 guidance papers, nearly one per month. Case studies and best practices are often included in guidance papers, which serve as practical guidance for AML/CFT practitioners within the industry. Reporting entities are expected to benchmark themselves against the recommended practices and supervisory expectations set out in the guidance and conduct a gap analysis against their own controls, which MAS also reviews during interventions on the FIs. Reporting entities met while onsite appreciated the frequency and depth of guidance issued by MAS.

231. Partnerships: One of ACIP's main tasks is to co-develop and promote a mutual understanding of risks and AML/CFT obligations between Singapore's competent authorities and Singapore's private sector. This includes the development of best practices and information papers to recommend measures that FIs can take to identify, prevent and disrupt money laundering in priority areas, such as the misuse of legal persons for corruption/tax-ML and trade-based ML. ACIP Advisories were introduced in April 2019 to enable quick dissemination of risk information on significant cases and typologies observed by MAS, CAD, other government agencies or ACIP members to the industry. The advisories alert industry to new and/or emerging risks, including those relating to legal persons and complex structures, tax fraud, etc., so that industry (not only ACIP members) can take swift measures to mitigate these risk concerns (including the filing of more pertinent STRs to enrich our intelligence database). ACIP has issued four best practice papers and five advisories since 2020.

Box 3.2. Singapore's AML/CFT Industry Partnership (ACIP)

ACIP, Singapore's public-private partnership, was initially set up in 2017, is co-chaired by SPF/CAD and MAS and supported by a Steering Group comprising nine banks and the Association of Banks in Singapore. ACIP brings together stakeholders from industry and government to collectively identify, assess and mitigate key and emerging ML/TF risks facing Singapore, and promulgate best practices to strengthen industry AML/CFT controls. Through ACIP, Singapore's competent authorities have been working with the private sector to raise industry ML/TF risk awareness and mitigate those risks.

232. Industry Engagements: During the last five years, MAS has held or participated in 73 industry engagements, including general engagements and industry-wide townhalls to reach out to obliged entities on their ML/TF risks and AML/CFT obligations. These engagement sessions have been positively received by the industry.

233. MinLaw has taken some measures to promote industry awareness, but these are less developed than the measures undertaken by MAS. These include an information guide, newsletters and quizzes to raise awareness of their ML/TF/PF risks, and dissemination of updates to FATF black/grey lists. Over the past five years, MinLaw has conducted ten outreach events to moneylenders, including industry engagement webinars, and has issued 21 guidance papers and eight circulars/documents, primarily concerning the outcomes of various national and thematic risk assessments, and guidance on source of wealth/source of funds checks, ongoing monitoring and STR filing.

3.3. FI and VASP understanding of existing and evolving ML/TF risks

234. FIs and VASPs met onsite have a solid understanding of ML/TF risks and have developed AML/CFT programmes that are appropriately designed to mitigate ML/TF risks to ensure that the financial system is not misused to facilitate financial crime.

235. FIs and VASPs in Singapore are required to assess and understand their ML/TF risks through conducting an Enterprise-Wide Risk Assessment (EWRA) to identify and understand ML/TF risks associated with their business lines, customer base, operating jurisdictions, products, and other factors on an annual basis. The EWRA must be reassessed when significant changes occur in risks or the operating environment, when new products/services are introduced, or when triggering events arise (e.g., the issuance of new guidelines). MAS verifies the integrity of the EWRA process through their supervisory activities and examinations, and where they find weakness in properly conducting EWRA they impose remedial measures, including sanctions. Good practices and common weaknesses observed during MAS' supervisory activities of FIs/VASPs are communicated to the industry through guidance papers and through industry engagement sessions. These measures have collectively improved financial institutions' understanding of ML/TF risks and application of mitigation measures. As an example, the number of STRs filed by major banks arising from detection of front/shell companies using data analytics has increased significantly from 236 in 2020 to 2086 in 2024.

236. Six major FIs in Singapore have been engaged in COSMIC to share information on existing and evolving ML/TF risks. This is a positive development to allow the private sector to share information and should be expanded to other reporting entities, and across more risk areas.

Box 3.3. Collaborative Sharing of ML/TF Information & Cases (COSMIC)

COSMIC was co-developed by MAS and six major commercial banks in Singapore - DBS, OCBC, UOB, Citibank, HSBC and Standard Chartered Bank. COSMIC allows FIs in Singapore to securely share information with one another on customers who exhibit multiple "red flags" that may indicate potential financial crime concerns, if stipulated thresholds are met. This makes it easier for FIs to detect and thereby deter criminal activity. Information sharing is currently voluntary and focused on three key financial crime risks in commercial banking, namely: (i) misuse of legal persons; (ii) misuse of trade finance for illicit purposes; and (iii) proliferation financing.

COSMIC has significantly improved the participant banks' ability to detect bad actors. In the first year since its launch, COSMIC resulted in an additional 461 STRs filed with total value exceeding SGD 1.6 billion (USD 1.18 billion) and 1 152 suspicious customer accounts closed. Two suspicious networks were also detected as a direct result of COSMIC sharing, and several more through additional checks by MAS and the participant banks. MAS will consider expanding COSMIC to more FIs and risk areas in subsequent phases.

237. Moneylenders have an adequate understanding of the ML/TF risks facing their business, which is established by MinLaw during its examinations of moneylenders. Other than CDD, record keeping and STR filing requirements, MinLaw also requires moneylenders to establish internal policies, procedures, and controls to enable their AML/CFT requirements. This demonstrates awareness of ML/TF risks by compliance staff.

3.4. FI and VASP understanding and compliance with AML/CFT obligations and mitigating measures

238. Interviewed FIs and VASPs generally demonstrated a comprehensive understanding of AML/CFT obligations and risk control measures, recognising the need to implement enhanced due diligence and other risk mitigation measures when dealing with high-risk scenarios such as PEPs or clients from high-risk jurisdictions. However, the number of STRs reported in some higher risk sectors (e.g. DPTSPs) and for some ML methodologies that Singapore is highly exposed to (e.g. TBML) are not proportional to the risks identified.

239. Singapore distinguishes between deficiencies and breaches, where deficiency refers to weaknesses in the FI's or VASP's AML/CFT controls (which does not amount to a breach of AML/CFT requirements set out in legislation); and breach refers to a breach of AML/CFT requirements set out in legislation. Moreover, supervisors report deficiencies/breaches based on the number of regulatory requirements/areas affected, rather than the actual number of individual instances (e.g. an entity found to have failed to perform enhanced customer due diligence (EDD) measures for five customer accounts in one inspection is counted as one deficiency/breach instead of five). Taking these into account, the number of deficiencies/breaches reported by Singapore is understated.

3.4.1. CDD, record-keeping, BO information, ongoing monitoring

240. FIs and VASPs generally understand their CDD obligations and record keeping requirements and have implemented appropriate measures to successfully undertake these obligations and requirements. Singapore's FI and VASP ecosystem is concentrated in a number of globally operating, sophisticated FIs and VASPs and systematically important local banks that have significant resources dedicated to AML/CFT,

including employing globally consistent policies and procedures, the use advanced systems and third-party service providers. MAS does occasionally find errors in CDD and record keeping. Supervisory activities conducted by MAS between 2020 and 2024 identified 25 deficiencies and 103 CDD breaches generally involving the relevance and timeliness of CDD documentation. These failures are instance-specific and isolated and rarely related to systematic issues.

241. FIs and VASPs have effective processes in place for on-boarding customers and carrying out CDD, including through online channels. For individuals, Singapore's national identity card (NRIC) system includes a population register available to government with key elements of personal identity, such as biometric identification data, date of birth, gender and photo biometric data. The NRIC is complemented by SINGPASS, Singapore's digital identity available to all citizens and permanent residents above the age of 15. These provide a strong element of customer verification during CDD processes. Non-residents in Singapore may open a bank account. FIs and VASPs generally require passport verification to open an account for non-residents.

242. For legal persons, Singapore's FIs and VASPs rely on basic information in ACRA's database or commercial sources, such as shareholder list and article of incorporation, to verify their beneficial owners. Singapore's BO registry is only available to competent authorities. Foreign-created legal persons can hold accounts in Singapore and FIs and VASPs generally rely on commercial providers or publicly available BO information in their home jurisdiction to verify information. For legal arrangements, including foreign legal arrangements, FIs and VASPs also use commercial software to track chains of ownership, but these might not always provide adequate information. The larger FIs met during the onsite demonstrated their effectiveness in identifying beneficial owners including for foreign legal and arrangements persons by using commercial databases to track all beneficial owners, while some smaller FIs reported that it was, in some instances too costly or there was a lack of reliable information to track beneficial owners. When beneficial owners cannot be confirmed or is too costly to maintain, FIs and VASPs in Singapore do not proceed with opening an account. MAS identified 1 deficiency and 13 breaches in relation to BO between 2020 and 2024.

243. FIs and VASPs give risk ratings to their customers based on the factors such as their individual characteristics, the products and services that they use and geographic exposure, amongst other characteristics. The frequency of review of customer profile corresponds to the risk ratings. Typically, high risk customers are subject to annual review, medium risk customers every two to three years and low risk customers every three to five years. Customer activity is monitored and examined when there is a trigger to do so. Where information is requested by FIs and VASPs as part of ongoing CDD, FIs and VASPs place limitations on customers' accounts, until the information is received. MAS has identified 25 deficiencies and 36 breaches related to ongoing monitoring between 2020 and 2024. These deficiencies are in relation to lapses in ongoing monitoring of business relations, including ensuring that CDD data, documents and information are relevant and kept up-to-date, and monitoring and detecting suspicious, complex, unusually large or unusual patterns of transactions.

244. There is limited reliance on third parties to conduct CDD in Singapore. FIs and VASPs with international operations leverage their group to gather CDD or BO information for foreign customers but still conduct CDD processes by themselves.

3.4.2. Enhanced or specific measures

245. PEPs - Singapore has a broad definition of a politically exposed person, their family and their associates, including both domestic and foreign PEPs. FIs and VASPs identify foreign and domestic PEPs, including their family members and close associates, through self-declaration by the customers and checks against commercial databases. PEPs self-identify when entering into a business relationship and FIs/VASPs scan open source information to identify clients who are PEPs. FIs and VASPs apply EDD measures for PEPs and track their source of funds/wealth. Once an individual is considered a PEP, they would typically be

always considered a PEP by the FI and VASP in Singapore. Overall, FIs and VASPs in Singapore apply strong measures for PEPs.

246. Correspondent Banking - Banks are required to develop a comprehensive understanding of the respondent bank and generally use questionnaires to conduct due diligence on respondent banks. Banks in Singapore have a good understanding of the risks and mitigating measures related to correspondent banking relationships. These relationships are subject to senior management approval and subject to periodic reviews. MAS has not observed any compliance deficiencies in correspondent banking.

247. New Technologies – MAS actively encourages FIs' and VASPs' use of new technologies. FIs and VASPs are required to identify and assess the ML/TF risks arising from new products, practices and technologies in advance of their implementation. Some FIs in Singapore do not take on business related to new technologies when they are perceived to be of high risk, such as virtual assets. Where FIs and VASPs do conduct business involving VAs, they conduct a risk assessment in advance of listing or doing business involving a particular VA.

248. Wire and Virtual Asset Transfer Rules – Relevant FIs comply with MAS' requirements for identification, submission and recording of information of both incoming and outgoing wire transfers. Wire transfers with incomplete information are scrutinised and rejected if the originator is unable to provide complete information. STRs would also be filed in appropriate cases. From 2020 to 2024, MAS had observed zero deficiency and six breaches in relation to wire transfer requirements. MAS had also taken supervisory/enforcement actions against 6 FIs for non-compliance with the wire transfer requirements. When sending or receiving virtual assets, FIs and VASPs are required to abide by the 'travel rule' to collect, securely transmits and documents the requisite originator and beneficiary information. Limited interoperability between solutions has led to challenges in implementing the 'travel rule' in Singapore and globally. In such cases, VASPs have implemented additional risk mitigating measures for transfers that were not compliant with the 'travel rule', such as restricting transfers to only first party transfers or ceasing to facilitate such transfers entirely. These mitigation measures are not consistently applied. Overall, FIs and VASPs generally apply wire and virtual asset transfer rules effectively and are aware of their obligations in this area, with some difficulty observed in implementing the 'travel rule' and mitigating risk of incomplete virtual asset transfer information.

249. High-risk Countries Identified by the FATF - FIs and VASPs have generally put in place clear policies for dealing with customers from FATF high risk jurisdictions, including the application of EDD. FIs and VASPs, met during the onsite were able to explain enhanced processes, which included requiring senior management approval to enter into commercial relationships with high-risk customers. FIs and VASPs generally showed a much more nuanced understanding of geographic risk beyond high-risk countries identified by the FATF and measures were more specific and far reaching than limiting geographic risk to consideration of jurisdictions identified by the FATF.

3.4.3. AML/CFT reporting obligations, tipping off

250. Overall, FIs and VASPs adequately understood their reporting obligations (see IO.6 for the breakdown of STRs per sector). The trend in reporting is positive with a doubling in annual STR submission over the course of the assessment period. More than 90% of the STRs have been filed by banks and PSPs with 10 banks representing over half of all STRs filed in Singapore. This is generally consistent with the fact that these two sectors are material and identified to have high and medium-high ML risk respectively. In addition, the number of STRs reported by some higher risk financial sectors (e.g. DPTSPs) does not seem proportional to the identified risk. Some lower risk sectors including direct life and composite insurers, broker dealer, finance advisory firms and money changers, rated as medium-low or low risks, reported a relatively large number of STRs every year. This could possibly be the result of defensive reporting or an incorrect understanding of risks against these sectors in NRA. A number of sectors have reported a low

number of STRs, including moneylenders. There are also limited STRs reported on key ML methodologies that Singapore is exposed to, such as TBML. More needs to be done by the authorities to ensure the suspicious transaction reporting of the financial sector is contributing to intelligence and supporting LEA objectives in these areas. MAS identified only single digit deficiencies and breaches related to STR filing across all sectors between 2020 and 2024.

251. FIs and VASPs generally leverage automated systems to monitor suspicious transactions and activities. VASPs generally subscribe to blockchain analytic tools for on-chain transaction monitoring as well as screening. Most FIs indicated that their primary trigger for submitting an STR is through adverse news reports and/or outreach from competent authorities in Singapore, though some FIs have started leveraging data analytics and network analytical tools to improve their detection of suspicious activities, entities and networks. There is still room for improvement in FIs and VASPs proactively detecting suspicious transactions rather than reactive and retrospective reporting following adverse news.

252. MAS and STRO supports the private sector quality and quantity of reporting through the publication of sector-specific red flag indicators and providing feedback on STR trends and STRs submitted to major reporters. From 2020 to 2024, MAS had observed one deficiency and seven breaches in relation to STR filing. MAS had taken supervisory/enforcement actions against eight FIs for failure to promptly submit STRs to STRO.

253. FIs and VASPs understand their obligations regarding tipping off and can explain processes to prevent this happening in practice. This understanding is consistent with supervisory findings.

3.4.4. Internal controls, procedures and audit to ensure compliance

254. FIs and VASPs in Singapore generally have internal controls and procedures in place to ensure compliance with their AML/CFT requirements. These controls and procedures include management oversight, dedicated, well-resourced compliance functions, staff training, and independent audit functions to check regularly for the effectiveness of the FI/VASP's AML/CFT measures. FIs' AML/CFT policies and procedures are reviewed and approved by senior management and communicated to staff via regular training by the FI. FIs/VASPs are subject to annual audit which covers AML/CFT requirements. However, MAS has observed 37 deficiencies and 29 breaches from 2020 to 2024, which resulted in remedial actions/sanctions against 20 FIs.

255. AML/CFT compliance is generally prioritised at an appropriate level in Singapore. Regular reports on key AML compliance matters are presented to the Board and Senior Management. FIs generally have put in place and maintained an appropriate audit function by establishing an internal audit function or outsourcing the audit function to suitable external service providers. MAS requires that all FIs submit an annual external audit report. The audits are focused on assessing the effectiveness of measures that the FI has taken to prevent ML/TF, including determining the adequacy of the FI's AML/CFT policies, procedures and controls and the extent of staff's compliance with established AML/CFT policies and procedures.

3.4.5. Legal or regulatory impediments to implementing AML/CFT obligations and mitigating measures

256. The Assessment Team did not identify any legal or regulatory requirements impeding implementation of AML/CFT obligations and mitigating measures in Singapore.

3.5. Supervisors risk-based monitoring or supervising compliance by FIs and VASPs

257. MAS implements an AML/CFT supervisory approach which selects and scopes supervisory activities based on three components (i) FIRA (i.e. inherent risk assessment) and (ii) risk surveillance managed by the AMLD, and (iii) AML/CFT controls managed by the nine supervisory departments and AMLD as part of their daily prudential supervision. These three components each have positive characteristics that contribute to conducting supervision on a risk-basis, but risk insights from these three components are not systematically consolidated into an integrated risk assessment on individual entities (see Section 3.2), which limits Singapore's ability to implement a risk-based approach to supervision.

258. Under the FIRA component (see Section 3.2 above), AMLD buckets each sector into one of four risk tiers in line with the ML/TF risk that sector was deemed to pose by the NRA (see Table 3.2 below). Within each sector, each individual FI or VASP is placed on an inherent risk spectrum from 'high' to 'medium-high' to 'medium-low' to 'low' risk based on their responses to the FIRA questionnaire and MAS' internal information. FIRA has some weaknesses if used as a stand-alone risk assessment tool, as it only focuses on inherent risks. Based on their placement in the inherent risk spectrum, institutions receive a full scope supervisory activity on a cycle intended to be commensurate with their inherent ML/TF risk. FIs under Tier 3 and Tier 4 sectors are not subject to cycle-based supervisory activities.

Table 3.2. FIRA-driven Supervisory Approach

Risk Tier	Sector	Supervisory Approach
Tier 1 – High Risk	Banks	High risk institutions examined every 3-4 years and medium-high institutions every 5-6 years Other institutions subject to controls-based supervisory engagements and risk surveillance-based examinations.
Tier 2 – Medium-High Risk	DPTSPs	High and medium-high risk DPTSPs and PSPs examined every 1-5 years High-risk EAMs examined every 4-6 years and medium-high every 6-8 years Other institutions subject to controls-based supervisory engagements and risk surveillance-based examinations.
	PSPs with CBMT services	
	EAMs	
Tier 3 – Medium-Low Risk	Fund management companies (excluding EAMs)	All institutions subject to controls-based supervisory engagements and risk surveillance-based examinations.
	Money changers	
	PSPs without CBMT services	
	Broker dealers	
Tier 4 – Low Risk	Corporate finance advisers	All institutions subject to controls-based supervisory engagements and risk surveillance-based examinations.
	Approved Trustees	
	Direct life insurance companies	
	Securities depository	
	Financial advisers	
	Finance companies	

259. The FIRA component of MAS' supervisory approach is inconsistent with the risks identified. For instance, the DPTSPs and PSPs with CBMT sectors, which are both Tier 2 sectors, are identified to be examined more frequently than banks, the only Tier 1 risk sector. MAS explained the increased frequency for the two sectors were due to (i) recency and unfamiliarity of regulatory scheme; (ii) variety in business model across the sector; and (iii) high TF risk posed by PSPs with CBMT services. While these explanations are logical, this highlights a flaw in the baseline risk model, where the basis for cycle-based supervisory activities is overridden for other factors rather than building those factors into a holistic risk understanding which underpins the coverage, selection and scoping of supervisory activities.

260. The number of FIRA-driven supervisory activities conducted by AMLD is very limited (73 across all sectors in 2020-24, see Table 3.3 below). This number of supervisory activities is also not in line with FIRA's recommended supervisory cycle. The FIRA process indicates that high-risk banks are subject to 3-4-year examination cycle, while high and medium-high risk DPTSPs and PSPs with CBMT services should be examined every 1-5 years. In reality, the number of FIRA-driven examinations conducted by MAS is much lower. For instance, for the five-year period from 2020-2024, MAS conducted 17 FIRA-driven examinations on the 19 high-risk banks identified, two FIRA-driven examinations on the seven high-risk DPTSPs and eight FIRA-driven examinations on the 13 high-risk PSPs with CBMT services. The FIRA-driven supervisory cycles are not met in practice. MAS indicated that the supervisory coverage has been complemented by other supervisory activities driven by the other two components, which is factual, but those activities are triggered by specific control issues or risk surveillance findings and are of narrower scope and vary in scope and intensity.

Table 3.3. Number of Supervisory Activities Driven by (i) FIRA and (ii) Risk Surveillance by Year

Sector		2020		2021		2022		2023		2024		Total	
		(i)	(ii)	(i)	(ii)	(i)	(ii)	(i)	(ii)	(i)	(ii)	(i)	(ii)
Banks (155)	Onsite	3	4	3	7	4	0	11	20	7	0	28	31
	Offsite	0	0	0	0	0	0	0	0	0	0	0	0
DPTSPs (29)	Onsite	0	0	0	0	1	0	2	2	0	0	3	2
	Offsite	0	0	0	0	0	0	0	0	0	0	0	0
PSPs with CBMT services (199)	Onsite	2	0	0	0	0	0	21	3	18	3	41	6
	Offsite	0	0	0	0	0	0	0	0	0	0	0	0
EAMs (197)	Onsite	0	0	0	0	0	0	0	2	0	2	0	4
	Offsite	0	0	0	0	0	0	0	0	0	1	0	1
Fund management companies (excluding EAMs) (1023)	Onsite	0	1	0	0	0	0	0	1	0	0	0	2
	Offsite	0	0	0	0	0	0	0	0	0	0	0	0
Money changers (291)	Onsite	0	0	0	0	0	0	0	0	0	0	0	0
	Offsite	0	0	0	0	0	0	0	0	0	0	0	0
PSPs without CBMT services (8)	Onsite	0	0	0	0	0	0	0	0	0	0	0	0
	Offsite	0	0	0	0	0	0	0	0	0	0	0	0
Broker dealers (180)	Onsite	0	0	0	0	0	0	0	1	0	1	0	2
	Offsite	0	0	0	0	0	0	0	0	0	0	0	0
Corporate finance advisers (27)	Onsite	0	0	0	0	0	0	0	0	0	0	0	0
	Offsite	0	0	0	0	0	0	0	0	0	0	0	0
Approved Trustees (16)	Onsite	0	0	0	0	0	0	0	0	0	0	0	0
	Offsite	0	0	0	0	0	0	0	0	0	0	0	0
Direct life insurance companies (25)	Onsite	1	1	0	0	0	0	0	1	0	0	1	2
	Offsite	0	0	0	0	0	0	0	0	0	0	0	0
Securities depository (1)	Onsite	0	0	0	0	0	0	0	0	0	0	0	0
	Offsite	0	0	0	0	0	0	0	0	0	0	0	0
Financial advisers (70)	Onsite	0	0	0	0	0	0	0	0	0	0	0	0
	Offsite	0	0	0	0	0	0	0	0	0	0	0	0
Finance companies (3)	Onsite	0	1	0	0	0	0	0	0	0	0	0	1
	Offsite	0	0	0	0	0	0	0	0	0	0	0	0

261. The second component driving MAS' supervisory activities is risk surveillance. AMLD selects and scopes supervisory activities from MAS' periodic and trigger-based meta-analysis of information including STRs filed by FIs/VASPs, intelligence from domestic and foreign counterparts, whistleblowers and adverse media reports, to detect evolving/emerging risk trends and typologies for targeted supervisory activities. This method is in part reactive, where MAS conducts 'for cause' supervisory examinations when they are already aware of a compliance issue from the information they have received, or in response to adverse media reports or supervisory/law enforcement actions taken by foreign counterparts. The approach is also partly proactive, where MAS follows up with supervised FIs/VASPs that exhibit a theme, trend or typology

that has been observed in the environment, or control issues which are identified through MAS' analysis. Over the five-year period from 2020-24, AMLD conducted 51 risk surveillance-driven supervisory activities across all sectors (see Table 3.3 above), again a small number, with the majority focusing on banks and covering some sectors that would otherwise not be subjected to supervisory activities under the FIRA approach. This supervisory approach intends to respond to the emerging or key risks as they develop.

Box 3.4. MAS' Risk Surveillance - DPTSP sector

In parallel with the introduction of AML/CFT requirements to DPTSPs in 2020, MAS focused significant surveillance resources on the DPTSP sector. MAS utilised a range of information sources, such as STRs, blockchain analysis tools, commissioning proprietary research and confidential intelligence to derive surveillance insights that have complemented and enhanced DPTSP supervision by (i) detecting unlicensed DPTSPs; and (ii) identifying DPTSPs with potential control weaknesses for earlier supervisory scrutiny. On (i), MAS identified 32 entities to be assessed for listing on the Investor Alert List, with seven referred to law enforcement. On (ii), MAS referred nine licensed DPTSPs for closer scrutiny due to control weaknesses, leading to examinations, supervisory warnings, and mandated remediation. MAS also conducted deeper reviews on 22 notified entities, resulting in actions on 19 entities, including one DPTSP that withdrew its application after failing to meet AML/CFT standards. For example, in April 2023, MAS' surveillance uncovered that a licensed DPTSP had onboarded three customers despite inconsistent information provided during onboarding and being unable to verify the legitimacy of the customer's business. In addition, large value and pass-through transactions that occurred in 2020 were only detected by that DPTSP in 2023. These observations helped inform MAS' inspection of this DPTSP, where the examiners found that the DPTSP's customer risk assessment framework and ongoing monitoring controls were inadequate. Following the inspection, MAS issued a supervisory warning to the DPTSP; and required it to put in place a remediation plan and appoint an independent auditor to validate the effectiveness of its remediation.

Apart from directly sharing probative findings with supervisors and LEAs (law enforcement agencies), MAS also consolidated its insights into a series of thematic surveillance reports issued from 2023 to 2025.

262. Risk surveillance is a good development in MAS' supervisory programme as it allows MAS to be dynamic and adapt to the risk environment, but MAS could further benefit from the approach if the risk factors considered could be systematically integrated into the other methods to arrive at a comprehensive risk understanding on institutional level to select and scope supervisory activities.

263. Finally, controls-based supervisory activities are conducted by MAS' nine supervisory departments and AMLD as part of their daily prudential supervision, and account for the vast majority (92%) of MAS' supervisory activities (see Table 3.4 below). For some of these activities, MAS' supervisory departments place a great reliance on the review of annual independent external audit and biannual internal audit reports. MAS reviews of external and internal audit reports are conducted for all institutions in all sectors under MAS' supervision as the baseline to identify any AML/CFT controls deficiencies for follow-up to ensure that any systemic deficiencies are appropriately addressed. MAS conducts controls-based supervisory activities of varying intensity including (i) reviews of findings of external or internal audit reports that had led to supervisory or remedial actions with the institution (offsite); (ii) follow-up with FIs/VASPs to assess AML/CFT/CPF breaches noted from review of STRs and voluntary disclosure by FIs/VASPs (offsite); (iii) physical or virtual meetings with FIs/VASPs on AML/CFT matters (onsite); and (iv) supervisory activities arising from offsite control factor assessments conducted on specific sectors (e.g. LTC and EAM sectors in 2020) and onsite supervisory activities to ascertain the state of controls and raise industry analysis/awareness.

Table 3.4. Number of Controls-based Supervisory Activities by Year

Sector		2020	2021	2022	2023	2024	Total
Banks (155)	Onsite	56	115	77	63	63	374
	Offsite	135	352	393	1 068	785	2 733
DPTSPs (29)	Onsite	0	6	8	18	18	50
	Offsite	5	3	3	0	6	17
PSPs with CBMT services (199)	Onsite	18	32	18	39	57	164
	Offsite	5	0	4	3	1	13
EAMs (197)	Onsite	3	0	3	1	1	8
	Offsite	59	2	5	5	10	81
Fund management companies (excluding EAMs) (1023)	Onsite	0	3	2	1	0	6
	Offsite	1	16	1	6	6	30
Money changers (291)	Onsite	0	0	0	0	0	0
	Offsite	7	2	1	3	2	15
PSPs without CBMT (8)	Onsite	13	26	11	11	9	70
	Offsite	0	0	0	0	0	0
Broker dealers (180)	Onsite	1	2	0	0	4	7
	Offsite	36	16	3	10	11	76
Corporate finance advisers (27)	Onsite	1	0	1	0	0	2
	Offsite	0	0	0	0	0	0
Approved Trustees (16)	Onsite	0	0	0	0	0	0
	Offsite	0	0	0	0	0	0
Direct life insurance companies (25)	Onsite	1	3	5	7	10	26
	Offsite	20	14	65	37	104	240
Securities depository (1)	Onsite	0	0	0	0	0	0
	Offsite	0	0	0	0	0	0
Financial advisers (70)	Onsite	0	2	0	0	0	2
	Offsite	2	0	0	3	4	9
Finance companies (3)	Onsite	0	1	0	0	0	1
	Offsite	1	1	2	2	3	9

264. These controls-based supervisory activities account for almost all of MAS' supervisory activities. There is a good level of coverage of regulated institutions in terms of frequency. However, they vary in scope and intensity significantly. Some examples of controls-based supervisory activities provided by Singapore were in reference to documentation related to a single account, while others were considering much more full scope compliance obligations and analogous to a classical compliance examination. Controls-based supervisory activities are also focused on controlling and remedying known or suspected deficiencies but not planned with reference to institutional residual ML/TF risks. Singapore provided examples where controls deficiencies were successfully remedied through these controls-based supervisory activities. In addition, examples were also provided where these supervisory activities resulted in remedial measures and sanctions. While Singapore does not track complete statistics of what these activities scoped in or found, Singapore demonstrated the rigour of these activities through case studies. Accordingly, the Assessment Team attributes them some weight given their broad coverage and demonstration of remediations.

265. These three components are brought together through MAS' annual work planning process. At the end of each year, MAS establishes the annual supervisory workplan for the coming year, guided by baseline cycle examinations informed by inherent risk from the FIRA model and foreseen risk surveillance-driven supervisory activities to address key emerging risks. Controls-based supervisory activities are triggered by and conducted through daily supervision of the nine supervisory departments, and hence there is no planning of such activities. The annual workplan is reviewed and updated on a half-yearly basis

to identify FIs/VASPs warranting additional supervisory activities through additional risk surveillance insights and/or escalating compliance issues. The baseline cycle supervisory activities are not met for a number of sectors. MAS is prioritising controls/surveillance-driven activities over FIRA-driven supervisory activities, though MAS indicates that it is well-resourced to implement their annual supervisory plan, both with internal resources and contracted external providers.

Table 3.5. Breaches Identified for High and Medium-High Risk Sectors by Year

Sector	Breach	2020	2021	2022	2023	2024
Banks	CDD	18	5	5	4	7
	BO	4	2	0	0	0
	EDD	6	7	3	2	4
	Sanctions	6	4	2	3	4
	Policy/Training	0	0	0	0	1
	Record Keeping	0	0	1	1	0
	EWRA	1	0	0	0	1
	STR	1	1	0	0	0
DPTSPs	CDD	0	0	0	2	0
	BO	0	0	0	0	0
	EDD	0	0	1	1	0
	Sanctions	0	0	0	1	0
	Policy/Training	0	0	2	1	0
	Record Keeping	0	0	0	0	0
	EWRA	0	0	0	1	0
	STR	0	0	0	0	0
PSPs with CBMT	CDD	0	0	0	0	0
	BO	0	0	0	0	0
	EDD	0	0	0	0	0
	Sanctions	0	0	0	0	0
	Policy/Training	0	0	0	0	0
	Record Keeping	0	0	0	0	0
	EWRA	0	0	0	0	0
	STR	0	0	0	0	0
EAMs	CDD	2	1	2	1	1
	BO	1	1	0	0	0
	EDD	5	1	0	2	1
	Sanctions	1	0	0	3	0
	Policy/Training	1	1	0	3	0
	Record Keeping	0	0	1	1	0
	EWRA	2	0	0	1	1
	STR	1	1	0	0	1

Note: This chart identifies the number of requirements that were breached, not the instances of the breach, so the numbers are understated.

266. Overall, MAS undertakes a range of supervisory activities of varying intensity and scope across its three components. The number of FIRA-based supervisory activities, as the most intensive and widest scoped supervisory activities, is limited, and the planned cycles are not met. Risk surveillance allows MAS to be dynamic and adapt to emerging threats, but the number of these targeted scope supervisory activities is equally limited. The controls-based component compensates for the frequency of supervisory activities and is targeted at improving AML/CFT controls where there are known deficiencies but such focus on treating observed deficiencies is not risk-based. While there is limited statistics on the scope and results of the controls-based activities, Singapore has demonstrated the rigour of such activities through case

studies. The intensity of supervisory activities overall for particular sectors seems to lack depth as they rarely find breaches (e.g. zero deficiency identified in PSPs with CBMT services during the 224 supervisory activities in 2020-24; but 20 breaches in 1H 2025). Overall, Singapore has the components of an effective programme to mitigate ML/TF risk through supervision; however, these components can be better combined in a more systematised manner to mitigate institutional ML/TF residual risks.

267. Moneylenders assessed to pose higher risk are inspected more frequently than the lower risk entities. During the assessment period, MinLaw carried out 80 examinations on annual basis by checking records on implementation of CDD requirement, sanction screening, risk assessment, training, etc. There was near 100% coverage of annual examinations for high risk and medium-high risk moneylenders, and around 50% coverage for medium and low risk moneylenders. The significant coverage appeared out of proportion to the risk identified in the sector, yet MinLaw advised that the AML/CFT supervisory examinations are conducted as part of its examinations for other prudential requirements for efficient use of supervisory resources. Overall, there is room to align supervision more proportionately with the lower ML/TF risks posed by the sector.

Table 3.6. Moneylender Onsite Supervisory Activities by Institutional Risk Level by Year

	2020	2021	2022	2023	2024
High (22)	45	8	11	19	22
Medium-High (11)	6	9	12	11	11
Medium (65)	11	31	29	25	26
Low (56)	18	32	28	25	21

3.6. Impact of monitoring, supervision, outreach, remedial actions and effective, proportionate and dissuasive sanctions on FI and VASP compliance

268. MAS can impose several types of remedial actions and sanctions depending on a number of factors including the nature/seriousness of the misconduct (e.g. the extent of weaknesses in an FI's/VASP's AML/CFT controls) and the severity of the breaches. In less severe cases, remedial actions such as supervisory reminders or sanctions such as private reprimands and supervisory warnings may be issued to the FIs/VASPs and/or the individuals concerned. MAS has the power to impose more serious sanctions, including financial sanctions (maximum SGD 1 million or USD 740 000 per offence), prohibition orders (POs), curtailment of business, as well as revocation or suspension of licence. In 2024, MAS expanded the scope of its POs to allow MAS to ban persons who are responsible for AML/CFT non-compliance from the financial sector.

269. MAS tracks the rectification of breaches identified. MAS requires FIs to submit regular updates (e.g. monthly or quarterly) on the progress of remediation (refer to "reports requiring remediation" as set out in Table 3.7) and monitor FIs and VASPs' progress until all issues are satisfactorily addressed. Where required follow-up actions are incomplete or late, a deeper supervisory action is conducted. MAS may also take other measures, such as appointing independent auditors to monitor completion of remediation actions, which MAS has done in 19 instances over the last five years. When a supervisory activity finds systemic AML/CFT failings, it makes a recommendation to MAS' Enforcement Department to determine the appropriate actions to be taken. Most proposals made to the Enforcement Department result in the imposition of an enforcement action.

Table 3.7. Remedial Actions and Sanctions applied by MAS across all FIs/VASPs (Except Moneylenders) Combined

Remedial Actions/Sanctions	2020	2021	2022	2023	2024
Reports requiring remediation	133	40	20	90	67
Supervisory reminders	3	5	3	4	4
Supervisory warnings	14	12	10	7	9
Private reprimands	3	4	0	0	3
Financial sanctions in lieu of prosecution	5 (SGD 2.3mm)	2 (SGD 2.1mm)	2 (SGD 3.3mm)	4 (SGD 3.8mm)	2 (SGD 4.4mm)
Others (e.g., curtailment of business, license revocation)	2	0	2	1	0

Note: Figure on reports requiring remediation includes instances of all other remedial actions and sanctions imposed.

270. MAS' Penalty Framework has a gradated consideration for remedial measures and sanctions. The maximum prescribed fine is SGD 1 million or USD 740 000 per offence. MAS also applies a composition framework where financial sanctions statutorily capped at 50% of the maximum offence amount can be paid in lieu of prosecution. From that much lower statutory cap, MAS, in consultation with the AGC, would compound some of the breaches which are of a similar nature or which arose from similar circumstances or were part of the same transaction or incident. Collectively, the much lower statutory cap for composition and the decisions to compound breaches resulted in significantly lower numbers and amounts of financial sanctions in practice. Apart from financial sanctions, MAS applies other serious sanctions against severe breaches, including revocation of licence of one fund management company in 2020.

271. MAS has used financial sanctions (15 financial sanctions from 2020 to 2024), and other serious penalties on FIs including curtailment of business or revocation of licenses (five from 2020 to 2024), etc. Since its last mutual evaluation, the average number of sanctions applied annually have significantly increased (16.4 vs 24.4), but the absolute number remains low. In 2025, MAS has further stepped up its sanction efforts, with a total of 33 sanctions taken as of July 2025, comprising 15 financial sanctions and 18 supervisory reminders/warnings and private reprimands. On 4 July 2025 (during onsite visit), sanctions amounting to SGD 27.45 million (USD 20.3 million) were imposed against nine FIs in relation to the 3B$ case; in addition, POs were issued against four individuals for failing to raise red flags when they were aware of information that should raise suspicion and failure to perform EDD for multiple persons of interests related to the case, and reprimands were issued against 14 individuals for failure to conduct or ensure proper due diligence of persons of interest related to the case. This progress is encouraging but the value of financial sanctions remains not commensurate with the nature of the breaches, the size/scale of FIs/VASPs in Singapore or Singapore's risk and context.

Table 3.8. Actions by MAS against Individuals

Action	2020	2021	2022	2023	2024
Letter of Advice	2	2	0	0	0
Supervisory Warning	0	0	0	0	0
Reprimand	2	0	0	0	3
Prohibition Order	1	0	1	1	0
Financial Sanctions	0	0	0	0	0
Others (e.g., individual's investigation findings recorded in MAS' internal licensing database)	1	0	0	0	0

272. Apart from institutions, MAS also holds senior managers and employees accountable for their part in the FI's/VASPs' failings. MAS has taken a range of actions against individuals proportionate to their misconduct, including reprimands and prohibition orders (upwards of a lifetime ban). Between 2020 and 2024, MAS took actions against 13 individuals including three prohibition orders, with 21 additional actions taken in the first seven months of 2025 (including four prohibition orders and two financial sanctions). This is a key area that MAS had stepped up since its last mutual evaluation. MAS' sanctions against FIs and individuals are also published to achieve deterrent effect.

273. MAS' sanctions are complemented by pro-active and close follow-up with FIs and VASPs to ensure implementation of remedial actions, including monitoring internal and external audit reports, examinations, or appointing independent auditors, etc. For example, FIs/VASPs would be required to put together a comprehensive plan to address MAS' concerns, including commitments to increase ML/TF headcount and technology investment, re-organisation of institutional set-ups, conduct wider remedial measures, etc. Following these actions, MAS observed that FIs/VASPs had increased AML/CFT related resources and committed significant technology investments to enhance controls, as well as strengthened front office accountability and elevated the level of management oversight.

274. MAS' supervisory initiatives also serve to strengthen the overall compliance culture. For instance, under MAS' intensive Supervisory Uplift programme, MAS requires FIs to develop effectiveness indicators (e.g. number of STRs filed, customers exited in relation to key risks identified) and monitors these indicators to ensure effectiveness of FIs' controls on a sustained basis. The financial industry was proactive in improving sector-level AML/CFT resilience, including industry-led best practice papers, sharing of experiences at industry-led workshops, and proactive sharing of risk information through COSMIC. Specifically, even though sharing on COSMIC has yet to become mandatory, participating banks have filed an additional 461 STRs involving a total of SGD1.6 billion (USD 1.2 billion) and 1 152 suspicious customer accounts were closed in the first year of COSMIC operations. An additional 91 customers were subjected to enhanced monitoring by the banks as their profile or behaviour did not yet warrant the filing of an STR.

275. MinLaw will require the moneylenders to rectify the deficiencies within a required timeline where AML/CFT deficiencies are identified during on-site examinations. MinLaw's Insolvency and Public Trustee's Office is empowered to impose administrative penalties (e.g., license revocation/suspension or forfeiture of security deposits) or criminal enforcement actions (e.g., warnings, composition penalties, and prosecution) on moneylenders non-compliant with AML/CFT/CPF rules. During the assessment period, MinLaw has issued one warning to a moneylender. No other remedial measures or sanctions have been applied.

276. Overall, Singapore needs to strike a better balance between supporting reporting entities and preventing non-compliance. MAS has made progress in the application of sanctions although the number of remedial actions and sanctions remains relatively low and the level of financial sanctions remains not proportionate or dissuasive when considering the size of FIs/VASPs, the serious nature of breaches as well as Singapore's risk and context. Singapore has stepped up sanctions and held individuals to account for their lapses in recent cases, and such actions are generally published for deterrent effect. That said, sanctions are complemented by Singapore's extensive remedial measures and close monitoring, strong industry engagement and public-private partnership, which is observed to have fostered a stronger compliance culture amongst FIs/VASPs and drive improvements in AML/CFT controls amongst FIs/ VASPs.

4 Non-financial sector supervision and preventive measures

The relevant Immediate Outcomes considered and assessed in this chapter is IO.4.[25] The Recommendations relevant for the assessment of effectiveness under this chapter are R.22, 23, 28, 34 and 35 and elements of R.1, 29 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Singapore has implemented robust market entry controls and fit and proper tests to prevent criminals and their associates from being the beneficial owner or holding a controller position in DNFBPs. DNFBP supervisors actively detect and investigate unlicensed activities under their respective regulatory remit, and SPF investigates into unlicensed activities, such as illegal gambling.

b) Singapore's DNFBP supervisors demonstrate varying yet improving understanding of ML/TF risks they face at the country- and sector-level, with some DNFBP supervisors such as MAS, ACRA, GRA, and MinLaw (for PSMDs) demonstrating reasonably sound ML/TF risk understanding. Most DNFBP supervisors have developed sector-specific methodology to identify higher-risk institutions with a varying level of maturity and understanding. For LTCs, there is concern over the process of MAS' establishment of their understanding of institutional residual risk of LTCs due to the lack of a systematised mechanism for consolidation of MAS' three supervisory components and the lack of proper documentation of the residual risk. MinLaw, having recently taken over supervisory obligation from LawSoc, demonstrated limited understanding of the ML/TF risks associated with lawyers and LPEs.

c) Singapore have taken efforts to promote a good understanding of AML/CFT obligations across the DNFBP sectors with most DNFBPs demonstrating a reasonable understanding of their ML/TF risks. There was stronger awareness and compliance of AML/CFT obligations observed in sectors subject to regulation for longer periods (e.g. LTCs, CSPs, accountants,

[25] When assessing effectiveness under Immediate Outcomes 4, assessors should take into consideration the risk, context and materiality of the country being assessed. Assessors should clearly explain these factors in Chapter One of the mutual evaluation report under the heading of DNFBPs, as required in the instructions under that heading in the Methodology.

and casinos), while others (e.g. PSMDs) have a less granular but improving understanding and implementation of their AML/CFT obligations.

d) While all DNFBP sectors submitted STRs and reporting has increased by 250% since 2020, two casinos continue to account for the vast majority (88%), with relatively lower reporting levels in other medium-high risk sectors.

e) DNFBP supervisors generally implement risk-based supervision to varying degrees with implementation being recent in some sectors (e.g. developers). There is a centralised mechanism to resource allocation and oversight of DNFBP supervision approaches; however, this has not led to fully consistent supervisory approaches or treatment across the DNFBP sectors. Some lower risk sectors are subject to a higher intensity of supervision than higher risk sectors. For LTCs, supervisory activities are not planned in accordance with institutional level of residual risks and while there is a good level of coverage for controls-based activities, MAS does not track complete statistics of their scope and findings to develop an understanding of the effect that supervisors are having on their supervised population. When supervisory activities are conducted, supervisors implement a reasonable quality of supervision.

f) Singapore has established a comprehensive remedial actions and sanctions framework for DNFBPs, with varying levels of enforcement across sectors, but active follow-up on remediation to promote compliance. Supervisors use a range of remedial actions and sanctions depending on the nature and severity of issues observed but are reliant on remedial measures. Where sanctions were applied, the level of financial penalty is usually not dissuasive. Taking into consideration the various sanctions imposed complemented by remedial actions, improvements in risk understanding and execution of AML/CFT controls are observed in some sectors.

Recommended Actions (RAs)

a) Allocate resources and refine existing risk-based supervision across sector in alignment with the level of ML/TF risks faced by the sector to ensure consistent and proportionate supervisory coverage and intensity.

b) Continue to conduct outreach to enhance reporting entities' understanding of suspicious transactions for DNFBP sectors, particularly in the more newly regulated sectors rated as being of higher risk in the NRA.

c) Review sanctions framework to impose more dissuasive and proportionate sanctions for DNFBPs found with breaches of AML/CFT obligations, including individuals within institutions who have contributed to the breaches.

d) Have MAS systematise its model of identifying and assessing residual risks at institutional level and integrate this consolidated view of institutional residual ML/TF risk into a planning process for supervisory activities, ensuring sufficient coverage and intensity for high and medium-high risk LTCs.

e) Have MinLaw enhance its understanding of ML/TF/PF risks associated with the lawyers and LPEs, considering their role as gatekeepers and improve its risk-based supervisory plan.

Overall Conclusions on IO.4

Singapore has implemented strong market entry controls and fit and proper tests to prevent criminals from owning or controlling DNFBPs. Supervisors actively detect and investigate unlicensed activities within their respective regulatory remit, and SPF investigates into unlicensed activities, such as illegal gambling.

DNFBP supervisors demonstrate varying yet improving understanding of ML/TF risks they face at the country- and sector-level and with some DNFBP supervisors such as MAS, ACRA, GRA and MinLaw (for PSMDs) demonstrating reasonably sound ML/TF risk understanding. Most supervisors have an improving understanding of the institutional level risks facing their supervised population. For LTCs, there is no documented institutional level residual risk. DNFBPs show a reasonable awareness of their AML/CFT obligations, with stronger understanding in more mature sectors. Some sectors (e.g. LTCs, CSPs, accountants, and casinos) generally demonstrated good understanding and compliance of AML/CFT obligations, while others (PSMDs) demonstrated a less granular and mature understanding and implementation.

Singapore generally applies a risk-based supervisory approach across DNFBPs with its implementation only being recent in some sectors (e.g. developers). There is a centralised mechanism to resource allocation in line with ML/TF risk, however some lower risk sectors are being subject to a higher intensity of supervision than higher risk sectors. At the supervisor level, the risk-based approaches adopted by respective DNFBP supervisors could be more nuanced and aligned across sectors. When supervisory activities are conducted, supervisors implement a reasonable quality of supervision.

Remedial measures and sanctions frameworks are in place for all DNFBP sectors, but supervisors are more reliant on remedial actions than sanctions. Where sanctions were applied, the level of financial penalty is usually not dissuasive, especially taking into account the relative scale of company and transactions. Supervisors actively follow up on remediation and publish sanctions, which serve to promote compliance. Taking into consideration the various sanctions imposed complemented by remedial actions, improvements in risk understanding and execution of AML/CFT controls are observed in some sectors.

Singapore is rated as having a Substantial level of effectiveness for IO.4.

Immediate Outcome 4

277. There are six AML/CFT supervisors for DNFBPs in Singapore: MAS supervises LTCs, ACRA supervises CSPs, accountants; MinLaw supervises PSMDs and pawnbrokers; MinLaw and LawSoc supervise lawyers and LPEs; GRA supervises casinos; CEA supervises EAs and RESs; URA supervises developers.

278. Private trust companies (PTCs) are regulated for AML/CFT/CPF by MAS; and are exempted from licensing and supervision but are required to engage an LTC to ensure that they comply with MAS' requirements on AML/CFT/CPF. A PTC is a company that does not solicit trust business or provide trust business services to the public but solely to connected persons which cover blood and family relations only.

279. For the assessment of the effectiveness of preventative measures and supervision for DNFBPs, the Assessment Team placed the most weight on CSPs and LTCs given their important roles as gatekeepers to legal persons and arrangements structures, and PSMDs which are assessed as relatively higher risks. Casinos, EAs, RESs and developers, as well as lawyers and law practice entities (LPEs), are weighted moderately important. Lower weight is placed on sectors with lower risk and/or materiality, including pawnbrokers and accountants.

4.1. Licensing, registration and controls for DNFBPs preventing criminals and associates from entering the market

4.1.1. Market entry controls

280. Singapore has robust licensing frameworks in place for all DNFBPs. DNFBP sector supervisors generally assess and screen prospective DNFBP persons, entities and their key personnel (i.e. substantial shareholders, board of directors and key appointment holders), where relevant, to ensure that only fit and proper DNFBP entities are licensed, and that only fit and proper persons control or manage DNFBPs. Criminal background checks are also conducted on DNFBP applicants. The number of rejected applications is generally low across all sectors except for PSMDs and Singapore-qualified lawyers.

281. MAS is the regulator and supervisor of LTCs, which are regulated as FIs in Singapore and subject to same process and standard of AML/CFT supervision. Please refer to IO.3 for relevant analysis applicable to LTCs. During the assessment period, three new LTC applications were withdrawn, while none were rejected. PTCs are exempt from licensing requirement. Notwithstanding, given that the PTCs serve high net worth individuals, PTCs are (i) subject to MAS' AML/CFT requirements, and (ii) are required to engage an LTC to carry out trust administration services for the purposes of conducting the necessary checks and ensuring its compliance with MAS' requirements on AML/CFT, and (iii) are regulated/supervised indirectly via the LTC to mitigate the risks.

282. ACRA licenses and supervises CSPs since 2015 when the regulatory regime was set up. Prior to the CSP Act effective in June 2025, CSPs were regulated under the ACRA Act and the ACRA (Filing Agents and Qualified Individuals) Regulations 2015 which set out the AML/CFT regime for Registered Filing Agents. The CSP Act came into effect on 9 June 2025, requiring all entities that carry on a business in Singapore of providing any corporate service must register as CSPs and submit declarations to ACRA confirming fulfilment of registration and fit and proper criteria. Prior to the CSP Act, Singapore-based entities that provide corporate services to overseas clients and do not transact with ACRA were not licensed nor regulated. This recent legislative amendment is an important policy step that Singapore has taken to address a previous regulatory gap in relation to the potential exposure to the misuse of legal persons outside of Singapore. More time is required before effectiveness of this measure can be demonstrated.

283. ACRA conducts fit and proper checks on all CSP applicants including their directors, beneficial owners and RQIs[26]. This includes the evaluation of all material including government and commercial databases, to ascertain if the CSP applicant is fit and proper. ACRA conducts fit and proper checks upon renewal applications, which occurs every two years. While ACRA does not specifically conduct fit and proper checks when there are changes in ownership, ACRA monitors for material/adverse news on an on-going basis, and key officers related to a CSP (e.g. Directors/RQIs) who do not meet the fitness and propriety requirement would not be allowed to continue their registration (see Box 4.1).

[26] If a person wishes to apply to be an CSP, the person will need to first employ, appoint, or engage at least one Registered Qualified Individual (RQI).

Box 4.1. Cancellation of CSP registration and subsequent denial of RQI registration

Individual A working at CSP A came under ACRA's scrutiny for incorrectly filing information in the Register of Registrable Controllers of one of the CSP's clients with ACRA. While denying having made the filing, Individual A admitted to sharing the SingPass credentials with other workers of CSP A. These workers used the credentials to submit filings for clients of CSP A. As these workers were not registered employees of CSP A, they were not authorised to make filings with the Registrar. CSP A's registration was cancelled following the investigation.

Individual A subsequently attempted to register as an RQI. According to the Regulations, an RQI must be fit and proper and is responsible for supervising employees of the CSPs for transactions filed on the electronic transaction system. ACRA considered Individual A's past conduct and determined that the individual was not fit and proper for registration and denied the registration.

284. ACRA requires applicants of accountants to satisfy prescribed requirements relating to qualifications, practical experience, continuing professional education, etc., and considers factors including whether the applicant has a criminal record or is under investigation for offences involving dishonesty. All applicants for registration of PAs should have obtained the Chartered Accountant (Singapore) designation. The Singapore Chartered Accountant Qualification Programme administered by ISCA is subject to annual renewal, completion of continuing professional education requirements and compliance with the Ethics Pronouncement 200 (EP200) containing AML/CFT requirements. If found to be not fit and proper, ACRA will reject the application. ACRA also regularly screen accountants with screening software and against adverse news, etc. During the assessment period, there were no cases of such rejection.

285. MinLaw conducts criminal record and open-source checks, and checks whether applicants are on UN sanctions lists for licensees, controllers and substantial shareholders for PSMDs, pawnbrokers, and LPEs. Applicants may be rejected if found guilty of a ML/TF/PF offence or an offence involving fraud or dishonesty punishable with imprisonment for three months or more. MinLaw rechecks all persons and entities subject to fit and proper checks on an annual basis, where there is adverse news or where there are notification requirements (i.e., changing ownership). MinLaw took a range of actions in handling registrations with fit and proper concerns (e.g. refusal, withdrawal or impose of conditions for new registrations; suspension or cancellation for existing registration) (see Table 4.1). In 1H 2025, MinLaw further cancelled another two registrations and imposed conditions on another three PSMDs.

Table 4.1. Statistics on registration (including refusals, withdrawals, impose of conditions, suspensions and cancellations) by the Registrar of Regulated Dealers on MinLaw

Registration	Refused	Withdrawn	Conditions Imposed	Suspended	Cancelled
Number	73	95	14	1	4

286. GRA was established in August 2022 as the single regulator for all forms of gambling in Singapore, including the two existing casinos, taking over responsibility from its predecessor the Casino Regulatory Authority. GRA conducts extensive probity and financial investigations to ascertain the suitability of casino applicants and performs suitability assessment through screening with LEAs and overseas regulators (if applicable), conducting background checks of controllers (including beneficial owners), reviewing their business associations, and assessing the applicant's financial position and source of funds. In the last five years, GRA rejected the renewal of an application for a special employee, an employee working in a managerial role, and approved three new controllers. The requirements of fit and proper controllers are monitored by GRA. Statutorily, there is a re-examination of the propriety of controllers if there is a change

in ownership or if they are involved in material litigation, under criminal investigation subject to ongoing monitoring under S63 of the Casino Control Act 2006.

287. CEA conducts background checks on all applicants and key executive officers for EAs/RESs, including criminal record checks and open-source checks. Licenses and registrations must be periodically renewed, and fit and proper checks are conducted again upon renewal. URA conducts criminal and open-source checks on all licence applicants including their directors, substantial shareholders, and beneficial owners. URA would not issue a licence to developers who have been convicted of ML/TF/PF offences, and/or fraud or dishonesty offences in the past five years. In addition to ongoing monitoring, fit and proper checks are re-done when new information is received from STRs, updates to sanction lists, adverse news, intelligence from other agencies, and whistleblowing. From 2020-2024, CEA and URA rejected five (out of 187 applications) and three (out of 156 applications) licence applications respectively, mostly due to reasons other than fit and proper concerns (e.g. applicants not having met the minimum experience requirement or absence of planning permission).

288. Market entry controls and fit and proper tests prevent criminals and their associates from being the beneficial owner or holding a controller position in DNFBPs in Singapore to a large extent.

4.1.2. Detecting and addressing breaches

289. DNFBP supervisors implement certain measures to detect and address unlicensed activities. Supervisors generally detect breaches and business carrying out unlicensed activities through proactive monitoring during license and registration renewals, supervisory activities (both on-site and off-site), ongoing surveillance, complaints and whistleblowing channels, and other channels (e.g. referrals from other authorities). Some supervisors maintain public registers and online reporting tools, which help the public and industry participants identify and report unlicensed entities. Some supervisors also put in place measures to mitigate the harm that could be caused by an unlicensed provider. For example, an unlicensed CSP would not be able to file transactions (e.g. incorporating an entity) on ACRA's system on behalf of others without the necessary credentials.

290. When unregistered dealing is detected or reported, supervisors commence an investigation, apply escalation protocols and take enforcement actions where warranted. Enforcement actions range from advisories and warnings to cancellation of licence and composition penalties. Stronger enforcement action is taken for more severe offences and where the circumstances of the case warrant it (e.g. deliberate commitment of the offence). There have been some instances of the detection of unlicensed activities and, where addressed, penalties are sometimes not proportionate to the offence committed. Some sectors (e.g. PSMDs) saw a gradual increase in imposition of compositions from 0 case in 2020 and 2021 to a total of 36 cases from 2022 to 1H 2025. This demonstrates a slightly more enforcement-oriented posture, with a total of SGD 330 000 (USD 244 200) in 36 composition penalties imposed, but the level of penalties remains not dissuasive.

291. The SPF has taken proactive efforts such as public information monitoring and AI analytic information to identify illicit gambling activities, which generally are manifest as websites offering gambling services in Singapore. These websites may be legal and regulated in other jurisdictions, but they do not have the appropriate licensing authority to offer services to Singaporeans or those in Singapore. Over the course of the assessment period, more than 4 000 illicit gambling websites were blocked. The SPF takes some intelligence and investigation measures when blocking the websites to establish actionable leads for further investigation.

4.2. Supervisors identifying, understanding and promoting DNFBP understanding of ML/TF risks

4.2.1. Identifying and maintaining an understanding of the ML/TF risks in the different sectors and types of DNFBPs and of individual DNFBPs over time

292. DNFBPs supervisors generally have a reasonable understanding of country-level and sector-level risks, largely informed through discussions at the RTIG which oversees the identification and assessment of ML, TF and PF risks at the WoG level. CAD and STRO in particular, provide DNFBP supervisors with updates on new ML/TF trends or information from STRs, ML/TF cases and the global FIU community. Feedback and inputs from MAS and other DNFBP supervisors are fed into RTIG's ML/TF/PF risk assessments. At sectoral level, most DNFBP supervisors have developed sector-specific methodology to identify higher-risk institutions and activities, with a varying level of maturity and understanding.

Table 4.2. Breakdown of DNFBPs by ML/TF Risk Rating

Sector ML NRA Risk Rating	Sector TF NRA Risk Rating	Sector	High	Medium-High	Medium-Low	Low
Medium-High	Low	LTCs	1 (1.67%)	5 (8.33%)	29 (48.33%)	25 (41.67%)
Medium-High	Low	CSPs	21 (0.70%)	1 090 (36.15%)	1 463 (48.52%)	451 (14.96%)
Medium-Low	Low	PAEs	18 (2.52%)	42 (5.89%)	152 (21.32%)	501 (70.27%)
Medium-High	Medium-Low	PSMDs	206 (10.47%)	579 (29.43%)	400 (20.34%)	782 (39.76%)
Low	Low	Pawnbrokers	38 (15.77%)	43 (17.84%)	134 (55.60%)	26 (10.79%)
Medium-Low	Low	LPEs	112 (9.65%)	311 (26.79%)	204 (17.57%)	534 (45.99%)
Medium-High	Low	Casinos	0 (0%)	2 (100%)	0 (0%)	0 (0%)
Medium-High	Low	EAs	14 (1.27%)	65 (5.91%)	192 (17.47%)	828 (75.34%)
Medium-High	Low	Developers	8 (4.32%)	15 (8.11%)	47 (25.41%)	115 (62.16%)

Note: Pawnbrokers are rated as "medium" risk level rather than "medium-low".

293. Singapore, for the purpose of fitness and propriety and making basic and BO information available, has relied on LTCs (who are responsible for the creation of most trusts in Singapore, operate as the trustee for most trusts in Singapore, and must be engaged in the case of a PTC) and CSPs (who form the majority of companies in Singapore and have a legal duty to ensure the accuracy of basic and BO information). Given the reliance on these institutions, compliance failures would result in both AML/CFT failures, as well as failures in making basic and BO information available (see IO5).

294. LTCs are regulated and supervised by MAS which considers them FIs. As detailed in IO.3, MAS' understanding of residual risks at institutional level was established through daily co-ordination between the AMLD and the nine prudential supervisory departments. AMLD conducts an inherent risk assessment (FIRA) and the risk surveillance programme, and both AMLD and the nine supervisory departments look into controls information. These three components are conducted separately, and the assessment is not done in a systematised manner or resulting in a documented institutional level risk rating. Overall, MAS has a sound understanding of country-level and sector-level ML/TF risks, but concerns remain over the process of MAS' understanding of institutional level residuals risk of LTCs due to the lack of a systematised mechanism for consolidation of the three supervisory components and the lack of proper documentation of the residual risk. Please also refer to the more detailed analysis on MAS' approach to risk supervisory approaches in IO.3. ACRA produces risk ratings for each DNFBP under their purview based on factors including customer profile, jurisdiction where they are operating, services offered, as well as STRs filed against it. Risk ratings are periodically updated according to the findings from LEA intelligence, adverse news, review and inspection outcomes, etc. ACRA regularly reviews and updates its risk assessment

framework to ensure it remains relevant and effective, and leveraged data analytics to focus on key risks such as the misuse of shell companies and nominee directorship arrangements. Based on these activities, ACRA has developed a reasonably sound understanding of their supervised population at the institutional level.

295. At institutional level, MinLaw collects information from PSMDs and pawnbrokers to assess risk profile of each entity, considering customer, product and service, and delivery channel risks. MinLaw assesses the risks of individual PSMDs based on a Compliance Risk Scoring Framework which takes into consideration PSMDs' risk profile, key threats and existing and emerging typologies in the sector. MinLaw reviews and recalibrates the risk ratings on a regular basis (at least once every 18 months) or when there is a material event, taking into consideration supervisory findings, audit reports, LEA intelligence or referrals, etc. For PSMDs and pawnbrokers, MinLaw has a reasonably sound understanding of their supervised population's institutional level risk.

296. MinLaw had taken over the supervision for LPEs from LawSoc in 2024. During the onsite visit, both MinLaw and LawSoc provided explanations on understanding of the ML/TF risks associated with lawyers and LPEs, which were limited, and were not able to provide details on the methodology used to develop the sectoral or institutional risk assessments. MinLaw indicated that it is still developing a framework to systematically assess sectoral risks. MinLaw subsequently clarified that it had been closely engaging with LawSoc on supervision of LPEs since 2021 and had refined its understanding of the sectoral and institutional risks leveraging data collected through a sector-wide request for information exercise in 2024. MinLaw also clarified after the onsite visit that the data collected in 2024 was analysed in January 2025 to update the risk-rating of each LPE, which it used to prioritise inspections carried out from April to June 2025. Overall, MinLaw demonstrated limited understanding of the ML/TF risks associated with lawyers and LPEs.

297. GRA has a high-level understanding of ML/TF risks of the gambling sector through environmental scans, monitoring of local and international typologies, participation in RTIG discussions and international events, and bilateral engagement with domestic and foreign counterparts, etc., which assisted GRA in designing mitigative strategies. GRA also demonstrated clear understanding of institutional risks through close supervision of the two industry players.

298. CEA implements a risk assessment model that incorporates factors that reflect ML/TF risks in the sector, including outcome of previous supervisory examinations, client base, etc. CEA classifies EAs/RESs into four risk categories and reviews the categorisation every three years or when there is a material event or LEA intelligence. URA adopts a risk assessment matrix which considers various factors including market segments of the properties sold, proportion of foreigner purchase, country of origin of developer, as well as adverse news and intelligence from LEAs. The risk factors will be updated if new risk typologies surfaced, and each developer is assigned with a risk rating that will be reviewed every 3 years or when new intelligence is provided by LEAs.

4.2.2. Promoting DNFBP understanding of ML/TF risks and AML/CFT obligations

299. DNFBP sector supervisors have been active in promoting DNFBPs' understanding of their ML/TF risks and AML/CFT obligations by (i) publishing guidance, best practices and circulars; (ii) partnership with industry associations; (iii) face-to-face outreach, including townhall events, briefings, consultations; and (iv) distribution of national and thematic risk assessments, as well as updated red-flag indicators[27] for the various sectors to facilitate the identification of suspicious activity. These various efforts have collectively promoted a clear understanding of ML/TF risks and obligations in the respective sectors. This is a strength of Singapore's regime.

[27] www.police.gov.sg/Advisories/Commercial-Crimes/Suspicious-Transaction-Reporting-Office/Suspicious-Transaction-Reporting

300. In particular, MAS collaborates with the Singapore Trustees Association to publish best practice papers and hosts regular industry engagements for LTCs. ACRA has also introduced mandatory AML/CFT training and proficiency tests for CSP registration and renewal. For accountants, ACRA works with ISCA to deliver targeted training and practical tools, such as CDD templates and sanctions resources. MinLaw has made significant efforts to support the relatively new regulated sector of PSMDs, including digital training via the myPal portal and developing infographic and video training materials. LawSoc provides lawyers with comprehensive AML/CFT resources via a dedicated portal and regular seminars. GRA maintains close communication with casino operators through monthly engagements to clarify expectations. In the real estate sector, CEA and URA promote AML/CFT compliance through consultations, examinations and training. These co-ordinated efforts reflect Singapore's commitment to fostering a strong culture of compliance across all DNFBP sectors.

4.3. DNFBP understanding of existing and evolving ML/TF risks

301. DNFBPs met during the onsite have varying yet improving understanding of ML/TF risks they face. All demonstrated a reasonable level of understanding of ML/TF risk and have an AML/CFT regime in place to mitigate those risks. This understanding is usually more mature in DNFBP sectors that have been subject to AML/CFT regulations for longer time (e.g. LTCs, CSPs, accountants, and casinos, etc.). DNFBPs interviewed are generally aware of risk identified in the ML and TF NRAs and considered the NRAs useful in understanding risks facing their institutions. DNFBPs are required to assess and understand their ML/TF risks, implement measures to mitigate identified risks, and document relevant assessments and procedures for inspection by supervisors. Such requirements are applied to varying extent in different sectors, with more mature sectors such as casinos having the highest level of risk understanding. PSMDs demonstrated a less granular and mature understanding as a relatively newly regulated and supervised sector.

302. Similar to FIs covered under IO.3, LTCs are subject to the requirement to conduct and review EWRA to identify and understand their risks in relation to their trust business, trust relevant parties (TRP), trust structures, countries where the TRPs are from, and where trust assets are located. MAS found LTCs to have established AML/CFT policies and procedures and good risk understanding.

303. CSPs and accountants are required to take steps to identify, assess and understand the ML/TF risks, and document such risk assessments, which will be subject to ACRA's review as part of inspection. They are also required to develop and implement internal policies, procedures and controls (IPPCs) to manage and mitigate identified risks. ACRA has observed significant progress in risk awareness in CSP sector and good understanding of nature and level of ML/TF risks in accounting sector.

304. PSMDs and pawnbrokers are similarly required to assess and document ML/TF risks and implement IPPCs to mitigate these risks. MinLaw monitors compliance through examinations, guidance and enforcement actions, leading to improved sector-wide AML/CFT awareness and practices. PSMDs are also required to submit risk assessments and IPPCs to MinLaw in semi-annual returns. PSMDs as a relatively newly regulated and supervised sector witnessed a relatively high number of breaches (205 instances in 2020-24) in relation to risk understanding, but the number of breaches is in a sharp downward trend from 120 instances in 2021 to 24 instances in 2024.

305. LPEs are also required to identify and assess their ML/TF risks and put in place AML/CFT controls to mitigate those risks. LawSoc has found that the number of LPEs which were observed to have put in place steps to identify, assess and understand the ML/TF risks stayed relatively consistent over time, with an average of 91% between 2019 and 2024 having done so in a satisfactory manner.

306. Casino operators in Singapore have demonstrated a structured and evolving approach to understanding and mitigating ML/TF risks through their "prevention of money laundering and terrorism

financing framework. These frameworks are endorsed at the Board level and reviewed annually to incorporate emerging risks, regulatory updates, and global best practices. Casino operators take into consideration profile risks, transactional risks relating to the country which the patron is transacting from, as well as the patron's behavioural risks. Overall, the procedure in place demonstrates effectiveness in identifying, assessing, and adapting to ML/TF risks in the casino sector.

307. EAs/ RESs are required to perform and document their risk assessments of their real estate agency business, keep these assessments updated, and furnish them to CEA during examinations. CEA reviews the risk assessments and notes that EAs/RESs are aware of their ML/TF risks and AML/CFT obligations. URA has implemented AML/CFT requirements for developers since June 2023, requiring them to conduct risk assessments, implement IPPCs, and perform CDD/ECDD checks. Large developers have shown strong compliance, with senior management-approved frameworks, staff training, and independent audits.

4.4. DNFBP understanding and compliance with AML/CFT obligations and mitigating measures

308. Singapore have taken efforts to promote a good understanding of AML/CFT obligations across the DNFBP sectors, but the implementation by DNFBPs for the newer sectors could be further improved. Interviewed DNFBPs generally demonstrated a reasonable understanding of AML/CFT obligations and risk control measures and AML/CFT requirements are implemented to various extent in different sectors. PSMDs, as a relatively newly regulated sector and with large number of players in the industry, had relatively higher number of breaches identified during supervisory activities than other sectors, with the number dropping in the later years. For developers where supervisory regime was put in place recently, awareness and implementation of risk mitigation are gradually levelling up. All DNFBP sectors submitted STRs, but the vast majority were submitted by casino operators and the number of STRs submitted by some higher risk sectors (e.g. PSMDs) is lower but has been gradually increasing.

309. As with the case of financial institutions, Singapore distinguishes between deficiencies and breaches, where *deficiency* refers to weaknesses in AML/CFT controls (but is not itself a violation of AML/CFT requirements set out in legislation); and *breach* refers to a violation of AML/CFT requirements set out in legislation. Moreover, supervisors report deficiencies/breaches based on the number of regulatory requirements/areas affected, rather than the actual number of individual instances. Taking these into account, the number of deficiencies/breaches reported by Singapore would be understated.

4.4.1. CDD, record-keeping, BO information, ongoing monitoring

310. All DNFBPs are required by AML/CFT regulations to conduct CDD measures, identify and verify BO information and conduct ongoing monitoring of business relationships. In practice, basic CDD requirements are consistently implemented across most DNFBPs, and interviewed entities generally indicated sufficient guidance from supervisors on supervisory expectations. Supervisors do occasionally find errors in CDD, especially in real estate sector.

311. From the results of MAS's supervisory activities, as well as the onsite interviews, LTCs understand and apply their AML/CFT obligations in relation to CDD, BO information and ongoing monitoring appropriately and generally have strong AML/CFT internal controls. MAS has identified 2 deficiencies and 9 breaches in 2020-24 from 70 supervisory activities and acknowledged that LTCs' monitoring of higher risk TRPs, particularly in relation to source of wealth checks and scrutiny of their transactions, could be further strengthened.

312. CSPs generally complies with their AML/CFT obligations to conduct CDD and have procedures to address cases where client identity or background information is insufficient, including terminating

transactions, rejecting clients, and filing STRs in line with regulatory obligations. ACRA verifies CSPs' compliance by reviewing files from long-standing business relationships to confirm that ongoing monitoring is conducted, and relevant records are retained. That said, ACRA still identified a limited number (20 cases from 1572 examinations) of breaches related to CDD or BO information over the past five years. Accountants are subjected to similar requirements and were found to be compliant with no breaches identified.

313. MinLaw and LawSoc's supervisory activities showed that most PSMDs, pawnbrokers, and lawyers have implemented core AML/CFT obligations such as CDD, record-keeping, and BO information requirements. While PSMDs recorded a higher number of deficiencies (25) and breaches (93) from 1125 examinations, there was also an observed reduction in the number of breaches from 2021 to more stable numbers in 2022 to 2024, reflecting the sector's recent regulatory inclusion. On the other hand, pawnbrokers and lawyers demonstrated stronger compliance, with only single-digit breaches (three for pawnbrokers and six for lawyers) and 49 deficiencies (for lawyers) identified. Where high risk factors exist and a client is unable to provide an adequate, satisfactory and credible explanation in response to enquiries, the lawyer would consider whether a STR needs to be filed (see Box 4.2).

Box 4.2. Prospective Client rejected by lawyer due to ML/TF concerns detected when conducting CDD

A lawyer was approached by a company in Feb 2021 to offer legal services relating to the sale of a yacht. Screening conducted by the lawyer revealed that the company was owned by an individual under investigation in a foreign country for investment fraud. The lawyer noted that victims of the investment fraud had alleged that the individual used a yacht to demonstrate his wealth, as part of his marketing tactic to convince victims to invest. The lawyer suspected that the yacht for sale is the one used in the fraudulent scheme and may be proceeds of crime. The lawyer declined to provide legal services to the company and filed an STR with the name and owner of the yacht.

314. Casino operators in Singapore apply robust CDD and monitoring measures commensurate with the sector's ML/TF risks. The casinos conduct identity checks at entry and BO information are obtained and verified prior to establishing patron accounts or conducting transactions above the SGD 4 000 (USD 3 000) threshold. Ongoing monitoring includes income and occupation-based profiling and assessing third-party relationships to detect inconsistencies between patrons' gaming activity and known financial profiles and ensure lawful entitlement to usage of funds. GRA examinations confirm that operators maintain adequate records and apply CDD measures effectively, with three deficiencies and no relevant breach detected in 135 examinations conducted in the past five years.

315. EAs/RESs and developers demonstrated a basic understanding of CDD obligations before facilitating or accepting any property transactions when interviewed onsite. However, the number of breaches by EAs/RESs in relation to CDD, BO information and record keeping is relatively high (zero deficiency and 128 breaches from 62 examinations in 2020-24). The supervisory regime for developers is relatively new and all eight developers assessed to be of high risk and one developer of medium-high risk (which are mainly of larger scale) had been inspected, with no relevant deficiencies nor breaches identified. During onsite interviews, the sectors also observed lack of AML/CFT awareness and co-operation from buyers as key difficulties in complying with CDD and BO requirements but reported that they are bound by contract to complete the property transaction despite incomplete CDD/BO process. This reflected gaps in understanding and implementation of AML/CFT obligations by real estate sectors. Singapore has very recently taken measures to address gaps in the technical framework for some DNFBPs, for example,

mandating EAs/ RESs and developers to conduct CDD on unrepresented counterparties involved in property transactions, but it is premature to assess the effectiveness of these measures.

4.4.2. Enhanced or specific measures

316. DNFBPs apply EDD to customers (or BO of customers) that is a PEP or a family member or close associate of a PEP, as well as those linked to high-risk jurisdictions identified by FATF or supervisors. On top of normal CDD, EDD includes verifying source of wealth and source of funds, senior management approval, and ongoing monitoring. To assist DNFBPs in establishing SoW of customers, some supervisors published guidance documents and information papers to set out regulatory expectations and best practices. In general, DNFBPs met during the onsite indicated that they would conduct EDD on customers who are PEPs or are from higher-risk jurisdictions. Examinations by DNFBP supervisors also identified single-digit deficiencies and breaches in this regard for most sectors, except for PSMDs (six deficiencies and 12 breaches) and lawyers (54 deficiencies and 15 breaches).

317. DNFBPs are also required to identify and assess the ML/TF risks arising from new product, business practice or technologies, and put in place appropriate risk mitigation measures, before their implementation.

4.4.3. AML/CFT reporting obligations, tipping off

318. DNFBPs met onsite generally understood their reporting obligations and all DNFBP sectors had filed STRs during the assessment period (see IO.6 for the breakdown of STRs per sector). There was an overall positive trend in the number of STRs filed by DNFBPs, increasing by approximately 250% since 2020. However, the vast majority of all STRs reported by DNFBPs continue to be reported by the two casinos (88%), and the number of STRs reported by other sectors remain at relatively lower levels. This raises concerns on the ability of medium-high risk DNFBP sectors, such as LTCs, CSPs, PSMDs, EAs/RESs and developers, to detect and report suspicious transactions, but it is also noted that the differences in discrepancies in number of STRs submitted across different sectors could in part be attributed to the higher volume and transactional nature of casino activities over the rest of the DNFBPs.

319. Some DNFBP sectors (e.g. PSMDs and pawnbrokers) reported a relatively large number of STRs (45%) that were initiated by adverse news, showing that their knowledge of ML/TF typologies to proactively detect suspicious transactions, may not be fully developed. (see also IO.6). Interviews with real estate agents and developers also indicated that there is room for improvement in understanding detailed ML/TF typologies in Singapore's risk environment. Most DNFBP supervisors identified only single-digit deficiencies and zero breaches in STR filing over the assessment period, with the exception of MinLaw in regards of deficiencies found among PSMDs. MinLaw advised that the near 400 deficiencies were mostly related to failures in setting up SONAR accounts to facilitate the timely filing of STRs electronically. Such deficiencies were considered minor in nature as it is an administrative issue and straightforward to set up a SONAR account with STRO. These deficiencies do not constitute formal breaches of applicable AML/CFT requirements.

4.4.4. Internal controls, procedures and audit to ensure compliance

320. All DNFBP sectors are required to implement IPPCs to ensure AML/CFT compliance. These procedures typically cover risk assessments, CDD, record-keeping, STR, staff training, compliance oversight, and audit functions. Casino operators are required to submit the IPPCs to GRA for formal approval, while other sectors such as LTCs, CSPs and LPEs generally validate adequacy of IPPCs via supervisory activities. PSMDs as a relatively newly regulated sector identified higher number of deficiencies (463) and breaches

(172), although the numbers have declined since 2021, while limited breaches and deficiencies were observed in some sectors, such as LTCs, CSPs, lawyers/LPEs and EAs/RES.

321. Internal audits are widely used in LTCs, PSMDs, casinos, and developers, either through in-house teams or external providers. These audits focus on assessing the effectiveness of AML/CFT measures, adequacy of controls, and staff adherence to established procedures.

4.4.5. Legal or regulatory impediments to implementing AML/CFT obligations and mitigating measures

322. There are no legal or regulatory requirements impeding the implementation of AML/CFT obligations and mitigating measures. Confidentiality and privacy requirements are lifted for the combating of ML/TF.

4.5. Supervisors risk-based monitoring or supervising compliance by DNFBPs

323. The supervisory framework for DNFBPs varies in terms of maturity, with some sectors (e.g. casinos, LTCs) subject to long-established supervisory framework, and some sectors having been brought into AML/CFT regime more recently. All DNFBP supervisors have put in place frameworks to implement risk-based supervision, with a varying levels of sophistication and levels of coverage and intensity.

Table 4.3. Number of Onsite and Offsite Supervisory Activities in Each DNFBP Sector by Year

Sector (No. of entities)		2020	2021	2022	2023	2024	Total
LTCs (65)	Onsite	5	2	1	1	2	11
	Offsite	39	6	1	6	7	59
CSPs (2 883)	Onsite	109	379	367	300	417	1572
	Offsite	0	0	0	0	0	0
Accountants (4 347) / PAEs (713)	Onsite	32	55	14	10	20	131
	Offsite	0	0	0	0	0	0
PSMDs (1 967)	Onsite	218	136	209	241	191	995
	Offsite	5	46	50	19	10	130
Pawnbrokers (241)	Onsite	61	60	78	60	60	319
	Offsite	1	3	2	3	8	17
Lawyers (7 400)/ LPEs (1161)[28]	Onsite	50	50	50	52	0	202
	Offsite	0	0	0	0	26	26
Casinos (2)	Onsite	26	24	24	26	20	120
	Offsite	3	2	3	2	5	15
EAs/ RESs (1 135)	Onsite	12	0	0	2	14	28
	Offsite	0	24	0	0	10	34
Developers (208)	Onsite	NA	NA	NA	NA	9	9
	Offsite	NA	NA	NA	NA	0	0

324. LTCs are regulated as FIs and subject to the MAS' supervisory approach comprising three components: (i) FIRA (i.e. inherent risk assessment) and (ii) risk surveillance managed by the AMLD, and (iii) AML/CFT controls managed primarily by the nine supervisory departments as part of their daily prudential supervision (please refer to Section 3.5 for detailed description and assessment on the different

[28] Lawyers are covered during LPE examinations as lawyers can only practise through LPEs.

components of the approach). LTCs are considered as a Tier 2 (medium-high risk) sector, with high risk LTCs being subjected to a four-to-six-year baseline supervisory examination cycle; and medium high risk LTCs are subject to a six-to-eight-year baseline examination supervisory cycle. On top of baseline supervisory cycles, insights from ongoing controls assessment and risk surveillance, allows supervisors to mobilise resources to address key and emerging ML/TF risks. These supervisory activities are not planned considering institutional level residual ML/TF risks, which is of particular importance given LTCs' gatekeeper role for legal arrangements.

325. Supervisory coverage for LTCs is limited for FIRA and risk surveillance supervisory activities, but there is much broader coverage of controls-based supervisory activities. There are 65 LTCs in Singapore and from 2020-2024, MAS has conducted 70 supervisory activities, which covers 100% of high risk and 80% of medium high-risk LTCs. As identified in IO.3, there is a good level of coverage for these controls-based activities, in terms of frequency. However, they vary in scope and intensity significantly and Singapore does not track complete statistics of their scope and/or findings to develop an understanding of the effect that supervisors are having on their supervised population. Together, these supervisory activities have identified 21 breaches in LTCs, resulting in eight remedial actions and sanctions, and appointment of independent parties to closely monitor the completion of remediation in four LTCs.

326. For CSPs, ACRA similarly adopts a multi-prong approach to supervision of CSP sector. ACRA regularly assesses risk profile of individual CSPs and subjects high-risk and medium-high risk CSPs to two-year and three-year examination cycles respectively. The CSP's risk rating evolves continuously and can change in view of trigger events including intelligence reports or adverse media coverage, as well as review and inspection outcomes. In line with this approach, all high risk CSPs and medium high risk CSPs were examined over the course of 2023 and 2024. Since 2023, on top of the fixed cycle approach, ACRA has also introduced the risk surveillance approach to conduct focused or thematic examinations, as well as examinations to address key concerns or allegations of AML/CFT lapses. Findings from examinations are fed into the risk rating of inspected CSPs and the examination cycle would be adjusted accordingly. Where deficiencies are identified, CSPs are required to prepare and submit a detailed remediation plan demonstrating the steps taken to address them, along with evidence of rectification within two months of receiving the inspection outcome. Of the 1 572 examinations conducted by ACRA on 2 883 CSPs over the past five years, 72 CSPs were selected for follow-up examinations. These examinations have identified 69 breaches in CSPs, resulting in 46 remedial actions and sanctions. This approach is appropriate given the importance of CSPs to the creation of legal persons in Singapore.

327. For accountants, ACRA conducted wide examination coverage in earlier years to obtain a broader understanding of the level of compliance across the sector. Since 2020, ACRA moved towards a risk-based supervisory approach, focusing examinations on higher-risk accountants based on factors such as services offered, client profiles, and jurisdictional risks. The risk assessment was refreshed in 2023. High-risk accountants are inspected every two years, while medium-high risk ones follow a three-year cycle, with additional examinations triggered by complaints, adverse media, or intelligence from LEAs. ACRA conducts ongoing risk profiling through regular surveys and ISCA complements with compliance monitoring and follow-up remediation. ACRA did not identify any breach warranting sanctions in its 131 examinations of 713 PAEs.

328. There could be a potential issue with double supervisory coverage, where a single person or entity provides different services covered by FATF Recommendations (e.g. around 45% and 15% of CSPs are also practicing as accountants and lawyers) and therefore falls under the regulation and supervision regime of different DNFBP supervisors (or separate teams of the same supervisor). Indeed, ACRA provided a case of PAE being selected for follow up inspection in respect of the work in the capacity of a CSP. However, relevant authorities are committed to co-ordinate examinations on institutions that perform multiple roles and have in place a discussion arrangement to avoid duplication and an overly burdensome approach to

these people/entities. MinLaw and ACRA also share supervisory findings, e.g., examination reports for CSPs inspected by ACRA that are also LPEs.

329. MinLaw adopts a risk-based supervisory approach for PSMDs, using semi-annual data submissions and analytics to classify entities into risk tiers and prioritise oversight accordingly. High-risk PSMDs are examined at least once every three years, with medium-high and medium-low risk entities inspected every four to eight years. Supervision includes supervisory engagement, off-site monitoring of returns and CTRs, and targeted examinations triggered by intelligence, adverse news, or suspicious transaction reports. Examinations assess compliance with AML/CFT/CPF obligations, and PSMDs must submit remediation plans for any deficiencies, which are verified through follow-up examinations. From 2020 to 2024, MinLaw has conducted 1125 examinations on 1967 PSMDs, covering all 207 high risk and 611 medium-high risk PSMDs, while maintaining a coverage rate of 18.5% on medium-low risk and 13.2% on low-risk entities. Examinations were also triggered by risk insights received from FIU (see Box 4.3). These examinations have identified 760 breaches among PSMDs, together with sanctions taken due to tip-offs and other sources, resulted in 1114 remedial actions and sanctions, amongst which 308 supervisory reminders and 117 advisories were issued due to a one-off review in 2023.

Box 4.3. Follow-up on PSMD-related intelligence received from FIU

In 2020, as part of the PSMD Workgroup under the RTIG, STRO conducted a comprehensive analysis on the PSMD sector. STRO reviewed STRs filed on high risk PSMDs and over 7 000 CTRs filed by the PSMDs and identified a number of red flags. STRO provided its findings to MinLaw, which then initiated examinations on 10 PSMDs to assess their compliance with the requirements under the PSPM Act and PSPM (PMLTF) Regulations. With information obtained from its examinations and received from STRO, MinLaw successfully identified instances where some registered dealers failed to file CTRs or failed to comply with CDD/ECDD requirements.

The examinations resulted in multiple sanctions, including composition penalties totalling over SGD 250 000 (USD 185 000), stern warnings, and cancellation of registrations for several PSMDs due to failures in conducting CDD/ECDD, filing accurate CTRs, and other regulatory breaches. The examinations also uncovered potential offences where dealers are suspected to be operating a GST Missing Trader Fraud (MTF) using precious metals. The information was further analysed by STRO and MinLaw and subsequently referred to IRAS for follow-up. This referral has led to IRAS focusing on MTF involving precious metals and the issuance of IRAS' guidance on MTF typology in the PSMD sector which was shared with the PSMDs in September 2023.

330. MinLaw adopts a similar supervision approach for pawnbrokers, but there is not a fixed examination cycle applicable to the sector. MinLaw conducts around 60 examinations each year covering entities under all four risk categories, but in general with a higher coverage on high and medium high-risk entities. The 336 examinations on 241 pawnbrokers have identified three breaches among pawnbrokers, together with sanctions taken due to tip-offs and other sources, resulted in 29 remedial actions and sanctions.

331. Prior to 2024, LawSoc supervised lawyers and LPEs, categorising them into four risk clusters based on factors such as client profiles, transaction types, STR history, training records, and intelligence from LEAs, and higher-risk entities were prioritised for examinations with a fixed budget of 50 examinations per year. MinLaw has taken over the supervision for LPEs in 2024, conducting 24 offsite examinations on entities involved in the 3B$ case. As explained above, MinLaw did not provide any risk-based supervisory methodology at the time of onsite visit. MinLaw subsequently provided its supervisory framework and inspection plan approved in early 2025 and used to guide the examinations on LPEs from April to June

2025 and advised that it is refining the plan. From 2020 to 2024, 228 examinations on 1161 LPEs by MinLaw/LawSoc have identified 27 breaches among lawyers/LPEs, which did not result in sanctions within the period. 26 of the breaches identified were related to lawyers/LPEs implicated in the 3B$ case, for which sanctions were taken in July 2025.

332. GRA has applied stringent supervision against casinos. Given the limited number of operators and their similar risk exposure and clientele, GRA applies a consistent and rigorous supervisory approach to both casino operators in Singapore. It uses a mix of on-site and off-site tools, including examinations, review of internal audit reports and data submissions, with focused examinations conducted within each three-year license cycle. From 2020 to 2024, GRA has conducted 16 examinations against two casinos covering themes including CDD, ongoing monitoring, STR reporting, etc. Following each examination, GRA will issue a report highlighting instances of deficiencies with the regulatory requirements or areas of weakness and recommending areas for improvement. GRA does not maintain a dedicated team solely for AML/CFT supervision, however indicated they have relevant capacity and there is no issue with resources.

333. CEA adopted a risk-based supervision methodology in 2023. From 2020 to 2022, examinations by CEA were not planned under a risk-based approach. CEA used a simple methodology based on the number of RESs engaged by the estate agent to determine risk ratings, under which no estate agents were identified as high risk before 2023, and most examinations were focused on lower risk entities. There was a pause of examinations during 2022 to 2023 for reviewing and revising its risk-based supervision framework, and since 2024 has followed a risk-based approach, where the majority of examinations (75%) focused on high-risk entities. CEA now applies a cycle based supervisory approach aiming to cover high risk entities on yearly basis, medium high-risk entities every 3 years, while remaining coverage against other lower risk entities. CEA employs various supervisory tools including routine supervision, off-site monitoring, and on-site examinations. The supervisory frequency and intensity is largely in line with risk ratings. From 2020-24, 62 examinations on 1135 EAs/RESs by CEA have identified 153 breaches in EA/RESs, resulting in 140 remedial actions.

334. URA's supervision against real estate developers began in 2024. In 1H2025, URA completed examinations against all eight high risk entities and one medium-high risk entity (out of 208 entities in the industry), which did not identify any breaches for remedial actions. Given the relatively recent implementation of the regime, there remains room for improvement in their understanding of risk and application of the risk-based approach, particularly in assessing the risks of regulated entities and planning supervisory activities commensurate to the identified risk. During the supervisory checks, property purchases by foreigners, foreign legal entities and trusts, as well as purchases made via intermediary agents will be selected for scrutiny to ensure that the developers perform the necessary due diligence.

335. Overall, all DNFBP supervisors implement risk-based supervision to ensure DNFBPs are complying with their AML/CFT requirements to varying degrees. Under Singapore's centralised mechanism for resources allocation by MoF, individual agencies will review if their current resources are sufficient to implement risk mitigation measures and to conduct supervisory activities. If additional resources are required, agencies can submit applications for additional resources to MOF. SC/IAC's provided guidance for higher risk DNFBP sectors (except LTCs which is subject to MAS' approach) to achieve good supervisory coverage (around 90%) for high risk entities and adequate coverage (around 70%) for medium-high risk entities over a period of 2 to 4 years. At the supervisor level, the risk-based approaches adopted by respective DNFBP supervisors could be more consistent across sectors. Some lower risk sectors (e.g. pawnbrokers) are subject to more intense supervision than some higher risk sectors (e.g. LTCs, EAs/RESs etc.). This more intense coverage for the lower risk sectors is in part due to the fact that supervisors leverage on their resources and range of supervisory activities which serve a broader regulatory remit to include checks on compliance with AML/CFT requirements. When supervisory activities are conducted, supervisors implement a reasonable quality of supervision, but the consistency of application and resources attributed across sectors could be further improved.

4.6. Impact of monitoring, supervision, outreach, remedial actions and effective, proportionate and dissuasive sanctions on DNFBP compliance

336. Supervisors work with DNFBPs to rectify deficiencies identified in a timely manner through active follow-up on remediation. DNFBP supervisors would engage senior management of DNFBPs to communicate the remedial actions and sanctions to be taken by DNFBPs when AML/CFT obligations are breached. Actions taken against DNFBPs and individuals for severe AML/CFT breaches are generally published to shape industry compliance and public awareness of AML/CFT requirements.

337. DNFBP supervisors have various powers to impose financial penalties in combination with a broad range of administrative sanctions, such as imposing additional conditions on business activities, issuing written directions, revoking, suspension or refusal of renewal of registration or license. Since last ME, Singapore has reviewed and further enhanced the penalty frameworks for DNFBP sectors to bring penalty levels to a baseline of SGD 100 000 (USD 74 000) per breach in most instances, except for lawyers and legal practice entities where the baseline sanction remains as SGD 100 000 (USD 74 000) per case. The technical framework for sanctioning breaches is in place, however the implementation varies among each sector.

338. For LTCs, sanctions against LTCs and their senior management by MAS are guided by the AML/CFT Penalty Framework and Senior Management Accountability Framework respectively. Under the FSMA, MAS can impose criminal penalties of up to SGD 1 million (USD 740 000) per offence and hold individuals personally liable. MAS also has a range of non-criminal sanctions at its disposal, such as financial penalties (up to SGD 500 000 per offence or USD 370 000), prohibition orders, licence suspensions, and supervisory warnings, often accompanied by proactive supervisory follow-up to ensure implementation of remedial actions. The frameworks make clear when financial penalties should be imposed vis-à-vis other sanctions, and ensure such actions are proportionate and consistent. MAS tracks the rectification of lapses through audits, supervisory activities and appointment of independent auditors, and may impose a restriction on new business until remediation is completed. Between 2020 and 2024, MAS meted out remedial actions and sanctions, including imposing SGD 2.4 million (USD 1.8 million) in financial penalties against three LTCs, imposed a moratorium of new business activities to two LTCs as well as issued supervisory warnings against three LTCs. In addition to requiring LTCs to submit regular updates on the progress of remediation and monitoring closely the LTCs' progress until all issues are satisfactorily addressed, MAS also required four LTCs to appoint an independent auditor to monitor the completion of remediation actions. MAS has stepped up efforts in remedial actions and sanctions in 1H 2025, with SGD 2.6 million (USD 1.9 million) in financial penalties imposed against two LTCs, two supervisory warnings issued and an LTC required to appoint an independent auditor to monitor the completion of remediation actions.

339. Since the CSP Act came into effect in June 2025, the financial penalty for CSPs has increased from SGD 25 000 (USD 18 500) to SGD 100 000 (USD 74 000). ACRA has also reported to adopt more stringent enforcement stance against AML/CFT breaches since 2021, issuing warnings and financial penalties for more minor deficiencies and applying suspension or cancellation of registration for more severe breaches and higher risk CSPs. During the assessment period, ACRA imposed 15 financial penalties totalling SGD 80 200 (USD 59 000), 36 cancellations of registration and one suspension of registration against CSPs. For accountants, while ACRA has a range of sanctions, the sector has overall demonstrated good compliance and there were no findings warranting sanctions. Accountants are also subject to strict fulfilment of annual renewal criteria and requirements to complete Continuing Professional Education hours that includes AML/CFT as compulsory content.

340. In regards of PSMDs, from 2020-24, MinLaw issued a total 584 warning letters, 48 composition fines totalling SGD 628 000 (USD 464 000), seven cancellations of registrations and 1 suspension of registration for breaches of AML/CFT requirements. MinLaw has also actively taken actions against senior management and key personnel of PSMDs for breaches and issued five compositions fines totalling

SGD 119 500 (USD 88 400) against them in 2020-24. MinLaw has stepped up efforts in its sanctions in 1H 2025, with 22 composition fines totalling SGD 1 054 000 (USD 780 000) and two cancellations of registrations issued against breaches by PSMDs, and three composition fines totalling SGD 376 000 (USD 278 200) issued against senior management and key personnel. Regarding pawnbrokers, MinLaw has an internal penalty framework that guides sanctions depending on circumstances of the case. MinLaw would inform pawnbrokers to rectify deficiencies identified during onsite examinations within a required timeline and reported that all deficiencies observed have been promptly rectified. MinLaw has issued 21 warning letters, eight compositions totalling SGD 69 000 (USD 51 000).

341. Regarding lawyers and LPEs, LawSoc, as the SRB, promotes understanding of AML/CFT obligations through guidance materials and trainings, and can impose disciplinary actions ranging from financial penalties or suspension from practice or revocation of license. MinLaw/LawSoc would follow up remediation of deficiencies through re-examinations and indicated that re-inspection results demonstrate positive outcomes. For breaches, stronger sanctions are taken where warranted, and LawSoc can convene a disciplinary tribunal to hear cases of professional misconduct. However, LawSoc had very rarely used its disciplinary power against breaches by lawyers, with no disciplinary action taken between 2020-2024. Following the 3B$ case, MinLaw imposed financial penalties of a total of SGD 130 000 (USD 96 200) against two LPEs and reprimanded one LPE, which included the meting out of the maximum financial penalty to one of the LPEs. MinLaw also referred one lawyer to LawSoc for disciplinary action in July 2025, the investigation of which is ongoing.

342. GRA has applied intensive supervision against casino operators and promoted a strong compliance mindset among casino operators and licensed Special Employees through issuance of directions and guidance. GRA actively used various sanction tools against breaches of AML/CFT requirements, and casino operators engaged external consultants to review and improve their AML/CFT frameworks. Where deficiencies are observed, GRA requires casino operators to take remedial measures within a stipulated timeline. During the assessment period, GRA has imposed a total of nine warning letters, six financial penalties totalling SGD 2 695 000 (USD 2 million) relating to breaches of AML/CFT controls against the two casino operators. Interviewed casino operators expressed that GRA's intensive supervision has brought pressure and resulted into a stronger compliance culture.

343. For EAs and RESs, legislative amendments took effect in July 2025 to apply the financial penalties on a "per breach" basis, with a view to fostering a culture of compliance in the sector. Where CEA finds breaches during examinations, it takes a range of actions to address the breaches. During the assessment period, CEA has issued a total of 27 letters of warning/censure, seven financial penalties totalling SGD 24 000 (USD 17 800), and three suspensions of registration regarding EAs and RESs. For developers, URA introduced composition of offence for AML/CFT breaches and increased composition amount through the legislative amendments effective July 2025, but there has not been any case of application as there had not been any breach identified through the limited number of examinations conducted for this newly regulated sector.

Table 4.4. Remedial and Sanctions applied by DNFBP Supervisors across all DNFBP Sectors Combined

Remedial Actions/Sanctions	2020	2021	2022	2023	2024
Reports requiring remediation	75	273	223	218	201
Supervisory reminders	82	18	0	309	19
Supervisory warnings	6	151	74	84	99
Private reprimands	2	0	0	0	0
Financial penalties (total amount of penalties imposed)	3 (SGD 1.3mm)	16 (SGD 1.5mm)	5 (SGD 0.1mm)	10 (SGD 2.5mm)	15 (SGD 0.4mm)
Others (e.g., curtailment of business, license revocation)	1	2	5	6	9

344. Overall, DNFBP supervisors have undertaken 1 906 remedial and sanctions in five years against almost 12 600 DNFBPs in Singapore, with the vast majority taking the form of reports requiring remediation, supervisory reminders or warnings. There have been 49 cases of financial penalties, and 23 cases of business curtailment or licence revocation. Supervisors have observed improvements in the overall compliance culture and number of AML/CFT breaches. Stronger sanctions have been applied through the period, but there remains a reliance on remedial measures. While there are limited number of sanctions throughout the assessment period, particularly apparent in sectors such as LTCs, EAs/RESs, lawyers and LPEs, DNFBP supervisors have demonstrated stronger stance against AML/CFT breaches and taken stronger actions, especially in relation to the 3B$ case. Where sanctions were applied, the level of penalty is usually not dissuasive. That said, taking into consideration the various sanctions imposed complemented by remedial actions, some positive outcomes were observed as DNFBP sectors have demonstrated improvements in risk understanding and some newly regulated sectors (e.g. PSMDs) showed gradual improvements in execution of AML/CFT controls.

5 Transparency and beneficial ownership

The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The Recommendations relevant for the assessment of effectiveness under this chapter are R.24-25 and elements of R.1, 10, 22, 37 and 40.[29]

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Singapore conducted risk assessments for legal persons (LPs) and legal arrangements (LAs) in 2024. Singapore demonstrates a reasonable understanding of the risks stemming from most domestically incorporated companies, but a weaker understanding of the risks posed by legal arrangements, Unregistered Foreign Companies and the misuse of multi-legal person/arrangement structures. Within legal arrangements, Singapore's competent authorities had a reasonable understanding of the risks stemming from those created through LTCs and wakafs but a weaker grasp of the risk posed by complex legal arrangement/person structures, foreign trusts operating in Singapore and trusts not formed through an LTC.

b) Singapore's efforts to mitigate risks associated with LPs and LAs focuses on some transparency requirements, registration requirements with ACRA (for LPs), and supervision and monitoring of reporting entities. While these three limbs of mitigation provide some risk mitigation, they all face challenges due to their application being recent or limited use of the measure. There are areas of higher risk, such as Unregistered Foreign Companies and trusts, where there are insufficient mitigation measures in place. For Unregistered Foreign Companies, this is connected to the threshold for registration being set 50 years ago, and without consideration of Singapore's current ML/TF/PF risk.

c) Basic and BO information for almost all domestically created legal persons must be filed with ACRA. There are gaps in coverage, namely for Unregistered Foreign Companies, VCCs, or circumstances where a company is recorded as the beneficial owner of a legal person.

d) Competent authorities have direct and immediate access to the central BO registry. However, mechanisms to ensure the information on the registry is accurate are limited. Singapore does not verify BO information on the ACRA central registry before it is published; they instead rely,

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

at the point of incorporation, on the CSPs conducting proper CDD to identify the BO, and a limited amount of auditing post-incorporation (<1% of legal persons). Information is not available in a timely manner in all cases or at all in the cases where a foreign legal person is recorded as the beneficial owner (approx. 1% of cases). Where information is not available through the ACRA central registry, there are alternative mechanisms available if LEAs are able to identify from which reporting entity to seek information.

e) Singapore's approach to accessing BO information in relation to trusts primarily relies on the BO information being held by an LTC or PTC, where they were engaged, and/or an FI, if a bank account is maintained for the trust in Singapore. There are limitations in the measures adopted by Singapore to ensure the BO information is accurate and up to date as this is done by MAS during supervisory examinations. There is insufficient coverage and intensity for high and medium high-risk entities for BO obligations. The supervision of FIs/LTCs can be better systematised on the basis of ML/TF risks.

f) ACRA has a robust and automatic enforcement regime for non-compliance with annual report obligations which contain basic information on legal persons. Enforcement for breaches of BO information requirements is more nascent, particularly for LTCs, but is progressively improving. The sanctions implemented are not yet dissuasive as increased penalties were very recently enacted.

Key Recommended Actions (KRAs)

Singapore should:

a) Review and enhance the risk assessments of legal persons and arrangements in Singapore to ensure a robust and practical understanding of risks. Risks should be identified, analysed and understood to mitigate significant risks more quickly including for:
   a. Unregistered Foreign Companies maintaining bank accounts, investing in funds and/or purchasing real estate (and whether, on the basis of ML/TF/PF risk, this constitutes a sufficient link).
   b. Trusts not formed in Singapore, trusts not formed through an LTC; and whether the current supervisory intensity to LTCs ensures accuracy of BO information and mitigates the misuse of trusts.
   c. Legal persons not operating in line with original policy intent (e.g. VCCs not being used as CIS).
   d. Complex arrangements comprising multiple types of legal persons and/or arrangements.

b) Review, enhance, and implement additional mechanisms to ensure accuracy (i.e. verification and triangulation) of BO and nominee information in ACRA's central registries to improve the registries' accuracy.

c) Based on findings arising from review of risk assessment, identify and implement necessary enhancements to Singapore's multi-pronged approach to trusts.

Other Recommended Actions

Singapore should:

a) Systematically and proactively share intelligence ACRA generates from its information holdings with STRO/SPF to assist early detection and response to networks of legal persons being established for misuse.

Overall Conclusions on IO.5

Singapore is a major IFC, and a hub for company formation and for wealth management, where trusts are used. As such, the assessment team placed considerable weight on both legal persons and arrangements: within legal persons, most weight has been placed on companies, including foreign companies registered with ACRA and Unregistered Foreign Companies; within legal arrangements, most weight has been placed on trusts used in wealth management and complex structures.

Competent authorities demonstrate a reasonable understanding of the risks stemming from most domestically incorporated companies, but a weaker understanding of risks posed by legal arrangements, Unregistered Foreign Companies and the misuse of multi-legal person/arrangement structures. There was a reasonable understanding of the risks stemming from legal arrangements created through LTCs and wakafs, but a weaker grasp of the risks posed by complex legal arrangement/person structures, foreign trusts operating in Singapore and trusts not formed through an LTC. The areas where Singapore's risk understanding is weak correlate with areas of higher risk and are particularly concerning in the context of a large financial centre.

Singapore's efforts to mitigate risks associated with LPs and LAs focuses on transparency requirements, registration requirements by ACRA and supervision and monitoring of reporting entities. These measures may mitigate the risk of misuse of LPs/LAs but are either too recently implemented or have deficiencies in their implementation to be considered highly effective. There are also higher risk areas with insufficient risk mitigation measures.

BO information for legal persons is largely available to competent authorities through the central RORC but there are some instances (Unregistered Foreign Companies) where it is unavailable, and other instances (VCCs) or circumstances (where legal persons are the beneficial owner) where the information is not available in a timely manner. Where information is not available through the ACRA central registry, there are alternative mechanisms that can make information available if LEAs know which reporting entity to ask. In practice, LEAs approach reporting entities rather than referring to the ACRA central registry.

The basic and BO information on ACRA's central registry is largely unverified beyond CDD, making the accuracy of the information questionable. Singapore's approach to transparency of BO information in relation to trusts relies on the access of BO information through an LTC or PTC, where they were engaged, and/or the FI, if a bank account is maintained for the trust in Singapore. There are limitations in the measures adopted by Singapore to ensure the BO information is accurate and up to date.

Enforcement for basic information of legal persons is an area of strength, but it is much less developed for BO. The sanctions implemented are not yet dissuasive as increased penalties were just enacted.

Singapore is rated as having a Moderate level of effectiveness for IO.5.

Immediate Outcome 5

5.1. Identifying, assessing and understanding ML/TF risks of legal persons and arrangements

345. Singapore completed separate ML/TF risk assessments of legal persons (LPRA) and legal arrangements (LARA) in 2024, which supplements and updates the 2019 Legal Persons Risk Assessment and follow on from the 2024 National Risk Assessment. The LPRA and LARA were developed concurrently under the auspices of the RTIG; as such understanding of risk is supported by the other work of the inter-agency RTIG platform, which oversees the identification and assessment of ML/TF/PF risks at the whole-of government level. Singapore's risk assessment process included reference to qualitative and quantitative information from competent authorities and a range of other sources. Further, competent authorities have a good level of engagement with industry, including through the ACIP's Legal Persons and Arrangements Working Group (LPAWG).

Risk Posed by Legal Persons

346. The 2024 LPRA assessed the ML/TF risks associated with the types of legal persons operating in Singapore.

Table 5.1. Residual ML/TF Risks for Legal Persons in Singapore

Legal Person	ML Risk	TF Risk
Companies	High	Medium low
Unregistered foreign companies	High	Medium low
Limited liability partnerships	Medium high	Low
Sole proprietorships/General partnerships	Medium low	Low
Limited partnerships	Medium low	Low
Variable capital companies	Medium low	Low
Societies	Low	Low
Co-operative societies	Low	Low
Mutual benefit organisations	Low	Low

347. The risk assessment process is substantially similar to the NRA processes described in IO.1. Accordingly, it has the same positives and negatives as seen in the dynamic risk assessment process and NRA. In addition, the risk assessments did not conduct proper analysis of vulnerabilities. This includes how well the controls are working, in particular whether reporting entities are correctly identifying the BO in response to their AML/CFT obligations; and did not present fulsome analysis of the extent and operations/transactions of Unregistered Foreign Companies holding bank accounts in Singapore.

348. Singapore established a legal framework for the creation of Variable Capital Companies (VCCs) during the assessment period with the intended use of operating as a Collective Investment Scheme (CIS). Many VCCs in Singapore are not being used as a CIS. The LPRA assessment did consider the misuse of VCCs for ML/TF purposes (in terms of the structure and intended use of VCC) but does not consider how VCCs may be used outside of their intended use as a CIS. It did not consider SFOs and their formation as, and use of, legal persons.

349. The risk assessment appropriately considered the characteristics of the legal persons and arrangements separately, but did not adequately analyse the structures involving multiple interconnected legal persons and/or arrangement, which occurs in practice. The risk assessments do not sufficiently analyse the increased ML/TF risk in structuring various legal persons and arrangements together. In particular, the

risk assessments do not analyse the various possible ways in which structures can and are being used, nor how they are most commonly used in Singapore. For example, Singapore provides substantial wealth management services for HNWI and UHNWI individuals. Singapore has not considered the vulnerabilities of complex structuring involving SFOs which attract these customers.

Box 5.1. Single Family Offices (SFOs) in Singapore

SFOs refer to an entity (with separate legal personality) which manages wealth for, or on behalf of one family and is wholly owned or controlled by members of the same family. SFOs generally involve a complex structure of legal persons and arrangements underneath the overarching legal person that is the SFO. SFOs are an attractive mechanism for wealth management amongst HNWIs and UHNWIs, and Singapore has seen an increase in demand for wealth management using SFOs with 43% year-on-year growth (totalling over 2 000 in number). This growth is driven by favourable tax treatment and Singapore's reputation as a wealth management centre. Many SFOs are also looking to use VCCs to hold and manage assets of HNWIs or UHNWIs, furthering the complexity of legal persons and arrangements used.

Six SFOs have been linked to individuals convicted in the 3B$ Case; and at least two in the Prince Group case.

Where a single family and connected persons (extended family) seeks to set up and manage a trust for wealth management purposes, they may use a Private Trust Company (PTC) or LTC. A PTC does not need a license but has to engage an LTC to discharge its AML/CFT obligations set out by MAS associated with the legal arrangements. In the case of a PTC, it does not need to be licensed by MAS because it is managing its own trust assets but is subject to MAS' AML/CFT requirements and are required to engage an LTC (see IO.4). LTCs are required to conduct checks on the PTC to ensure that the PTC complies with the full suite of AML/CFT obligations in MAS Notice TCA-N03.

The PTC may act as trustee for multiple trusts for the one family. As at end 2024, there were a total of 65 regulated LTCs in Singapore, of which 33 serve PTCs. Approximately 11% of the assets under trusteeship by the LTCs in Singapore are managed within an PTC.

Going forward, SFOs will be required to form as a company but prior to this could have been formed as any legal person to qualify for an exemption from licensing by MAS. SFOs will also have to open and maintain a bank account with an MAS-licensed bank.

350. Competent authorities generally demonstrated a reasonable understanding of the risks stemming from Singapore incorporated companies; primarily the abuse of nominee directors, Unregistered Foreign Companies and, more recently, abuse of natural persons through gaining access to a Singapore national's SINGPASS. Competent authorities showed a lesser understanding of the more complex situations posing risk, which are common in Singapore's context.

Risk Posed by Legal Arrangements

351. Singapore's 2024 risk assessment for legal arrangements covers all legal arrangements operating in Singapore and takes into account several factors such as the number of trusts, the total assets under trusteeship, and limited law enforcement data regarding trusts. Singapore assessed that there is a lack of data surrounding the misuse of legal arrangements for ML/TF risks, with only four ML investigations involving trusts. Singapore took steps to overcome this lack of central information by engagements with the private sector and using international typologies and risk indicators. The results of the risk assessment are largely reflective of the ML/TF risk environment in Singapore (see Table 5.2 below), however, Singaporean authorities provided differing views on the risks of misuse of legal arrangements in Singapore.

352. As with the LPRA, the same process as the NRA was used so the positive and negatives also apply here. As with the LPRA, there was insufficient analysis of the extent to which related controls are working: for LA, this particularly relates to the CDD obligations of LTCs and FIs. The analysis of use of trusts in complex structures was also lacking and did not include consideration that the risk is different depending on whether the legal arrangement is in a complex structure. Singapore's analysis post on-site showed that trusts involved in complex structures were all sole shareholders of companies and did not hold the assets themselves/have financial transactions occurring in their name, whereas for trusts not in a complex structure the trust itself held the assets.

353. Lastly, the LARA differentiates and assigns significantly different risk ratings to trusts where a trustee is a trust company, and those where a non-professional is the trustee. While reasonably plausible to be true in most cases, there is also evidence of some trusts with a non-professional trustee being used in wealth management. Most importantly, the LARA had limited evidence for this differentiation, despite very significantly differing mitigation measures applied to these two types of trusts.

Table 5.2. Residual ML/TF Risks for Legal Arrangements in Singapore

Legal Arrangement	ML Risk	TF Risk
Express trusts where the trustee is a trust company	Medium High	Low
Foreign Legal Arrangements with links in Singapore	Medium High	Medium Low
Registered business trusts	Low	Low
Collective investment schemes (including real estate investment trusts)	Low	Low
Securities depository	Low	Low
Express trusts covered by Part 7 of the Trustees Act and Trustees (Transparency and Effective Control) Regulations 2017	Low	Low
Charitable purpose trusts	Low	Medium Low

354. Singapore's competent authorities demonstrated a lesser understanding of the ML/TF risks of legal arrangements. Competent authorities generally demonstrated a reasonable understanding of the risks stemming from legal arrangements created through LTCs and wakafs. They demonstrated a weaker grasp of the risk posed by complex legal arrangement/person structures, foreign trusts operating in Singapore and trusts not formed through an LTC.

5.2. Mitigating measures preventing misuse of legal persons and arrangements

355. Singapore has implemented several measures to mitigate the risks of LPs and LAs being used for ML/TF purposes. These mitigation measures are:

a) requirements to **register** with ACRA as the Registrar of Companies;
b) measures in relation to **transparency** (in relation to legal persons, Unregistered Foreign Companies and legal arrangements); and
c) **supervision** of reporting entities (see IO4; supervision as it relates to BO information and its accuracy is assessed in core issues 5.3 and 5.4 below).

356. Overall, Singapore has put a number of mitigation measures across the three limbs of mitigation. These three limbs of mitigation measures have all been implemented and do provide some risk mitigation, but all face challenges in their effective implementation either due to the recency of their application or insufficient investment into their application. There are areas of higher risk, such as Unregistered Foreign Companies and trusts, where there are not sufficient mitigation measures in place.

357. These mitigations do not cover all identified higher risk areas.

Requirements to Register with ACRA as the Registrar of Companies

358. The requirement for domestic and registered foreign companies, LLPs and VCCs to be registered with ACRA provides for a central registry of basic information on legal persons in Singapore but there are some gaps (see R.24). The deficiencies are minor and technical and as such do not appear to be hamper the effectiveness of Singapore's system with respect to basic information.

359. In 2020, Singapore instituted of a central BO registry held at ACRA, the RORC, and an obligation on most legal persons to hold a Register of Registrable Controllers (internal RORC). The BO information on both these registers is identical, is largely unverified or audited, and allows legal persons to be listed as beneficial owner without corresponding controls in place (see R.24 and Core Issue 5.3 for more details).

Measures in relation to transparency

Legal Persons

360. Information on the different types, forms and basic features of legal persons and the processes for creating legal persons is publicly available. Basic information held at ACRA is publicly available, BO information in the RORC is not publicly available.

361. Singapore requires that each foreign company operating a business in Singapore has a local nominee director, i.e., a responsible person residing in Singapore. Since 2017 and 2022, domestic and foreign companies operating a business in Singapore have been required to maintain registers of nominee directors and shareholders respectively. As of July 2025, these companies are now required to also maintain their registers of nominee directors and shareholders through ACRA's ROND and RONS, Singapore's central databases for nominee directors and shareholders. The creation of these registries is positive, but they were in effect for only days prior to the onsite visit; their implementation and contribution to ensuring transparency in Singapore cannot be evaluated. These transparency measures on nominee directors may be of limited value as Singapore has had difficulties in attributing liability to local nominee directors when a legal person is party to criminal conduct (see IO.7).

362. Bearer shares and bearer share warrants are prohibited in Singapore.

Supervision of reporting entities

363. For Unregistered Foreign Companies and legal arrangements, the only mitigations in place are the AML/CFT programs of FIs and DNFBPs. As such, the supervision of those FIs and DNFBPs are an important determination of whether the mitigation works in practice. As noted in IO 3, the supervision of FIs is not done on the basis of ML/TF risks assessed in a systematised manner. Further, there is insufficient coverage and intensity for high and medium high-risk entities, including for BO obligations. Similarly, concerns are noted in IO 4 for LTCs as they have the same supervisor.

Higher risk areas without sufficient mitigations

Unregistered Foreign Companies

364. Unregistered Foreign Companies are those companies that are not regarded as carrying on business in Singapore and who only have specified activities in Singapore, such as: maintaining any bank account, conducting isolated transactions, investing any of their funds or hold any property in Singapore. Singapore's LPRA identifies Unregistered Foreign Companies as High Risk for ML and there is a high volume of STRs filed in relation to Unregistered Foreign Companies.

Table 5.3. STRs Relating to Legal Persons and Arrangements in Singapore

Legal Person/ Arrangement	2020	2021	2022	2023	2024	Total
Companies	5 182	6 575	5 415	6 395	7 267	30 834
Unregistered Foreign Companies	1 608	1 870	1 560	1 822	2 392	9 252
Trusts	266	202	170	229	257	1 124
LLPs	30	55	28	31	37	181
VCCs	-	4	8	14	27	53

365. Unregistered Foreign Companies are not subject to any transparency measures with ACRA. FIs, VASPs and DNFBPs have obligations to identify and verify customers that are legal persons and identify their beneficial owners. This acts as the only real mechanism to mitigate the risks posed by Unregistered Foreign Companies.

366. Being exempt from the category of companies "carrying on business" in Singapore carves out these foreign companies from critical mitigation measures related to minimum information requirement (see c24.3). The exemption allowing Unregistered Foreign Companies to access and use the Singaporean financial system, without an assessment of the nature of ML/TF risks posed by these activities, is concerning. Singapore did not consider whether registration could mitigate risks from financial transactions and relationships involving Unregistered Foreign Companies.

367. Overall, what constitutes a substantial link to business in Singapore has not been considered on the basis of ML/TF risk. This is particularly concerning in light of the international, large and connected nature of Singapore's financial system. While MAS conducted a survey of some FIs to determine the nature and extent of activities of Unregistered Foreign Companies in Singapore, at the time of the onsite, there was not a comprehensive understanding of how many are operating in Singapore, nor what their activities are.

Legal arrangements

368. Singapore relies on the information obtained and held by the relevant trustees and trustee-equivalent of a trust, and information collected by FIs, VASPs and DNFBPs, to determine BO of legal arrangements. As noted in R.25, there are deficiencies in relation to risk assessment, mitigation and access to timely, accurate and up-to-date information in Singapore. In the absence of a public authority that holds this information, and the lack of verification requirements in relation to some trusts, it cannot be concluded that transparency through information requirements offers strong mitigation in relation to legal arrangements.

5.3. Legal persons: Timely access to adequate, accurate and current basic and beneficial ownership information

369. Singapore has put measures in place to ensure that competent authorities have timely access to basic and BO information for most legal persons but have limited mechanisms to ensure this information is accurate. For the emerging VCC sector, access is less timely as VCCs do not have to file their BO with the central register and thus it can be more difficult to locate the keeper of such information. Unregistered Foreign Companies only have to make basic and BO information available for CDD processes when engaging reporting entities.

Basic information

370. Basic information on legal persons is filed centrally with ACRA, while only some of the information needs to be separately maintained by the legal persons. This does not appear to impact effectiveness. The public can access this information for a small fee, and the information is audited by ACRA as part of the audit of the BO register. Companies and LLPs are required to submit annual returns. There is a 78% compliance rate, on average for the assessment period, with the annual returns. The information submitted is used to update basic information held by ACRA. ACRA has conducted about 2 000 examinations over the assessment period to support the accuracy of registered office addresses.

371. Singapore nationals forming a legal person must verify their identity with ACRA using SINGPASS. SINGPASS provides secure direct access to government digital services to incorporate a company. Foreign nationals without SINGPASS may only form a Singaporean company through a CSP and must further engage a local resident to act as a local nominee director on an ongoing basis. During the on-site, the legal requirement has been imposed requiring CSPs to conduct "fit and proper" testing on the nominee director. Prior to that date, there were no checks for fitness and propriety that were legally required.

372. LEAs and the private sector are regularly using this basic information for their investigation and CDD work respectively. Legal persons are not permitted to have other legal persons as directors.

BO Information

Central BO registry (RORC)

373. Singapore implemented a central BO registry though ACRA for most legal persons in 2020. These legal persons are required to both maintain a register of registrable controllers (BOs) and file that information into a central BO register maintained by ACRA. Approximately 91% of companies and LLPs have filed their BO information with ACRA to populate this registry. Competent authorities have direct and immediate access to the central BO registry but it is not publicly available.

374. There are shortcomings in the mechanisms in place to ensure BO information is accurate under the private RORC, and ACRA central register:

a) Companies may be listed as controller without a corresponding natural person (even though this is not permitted under legislation);
b) No substantive verification (via audits) is done post incorporation or filing; and,
c) Inadequate supervisory interventions to check the BO determined by CSPs and thus filed into the registry.

375. Companies, foreign companies and LLPs are required to ensure that the particulars in their private RORC are accurate and up to date by sending a notice at least annually to every registrable controller and promptly updating the RORC with any changes. There is no need to update the RORC information lodged with ACRA annually if there are no changes to the existing RORC information, as changes are lodged as and when they occur. Domestic companies, foreign registered companies and LPPs are not required to verify the identity of the registrable controllers or identify the ultimate BO of a legal entity that has a significant interest in, or significant control over, the company.

376. In limited circumstances, legal persons are permitted to be listed as a controller. For domestic legal persons, competent authorities can follow through the relevant profiles to identify the natural person for any Singaporean legal person. However, the situation is less helpful where foreign legal persons are listed as controllers. Information provided by Singapore shows that in ACRA's central BO registry, a natural person is not always listed as a controller. As a recent example, at December 2024, 4 165 companies (1% of registry) had listed only foreign corporations as its beneficial owners into the RORC without identifying any other individuals. This also leaves the RORC vulnerable to 'corporate loops' being formed.

377. There is a significant limitation to the ability for LEAs to access timely and accurate BO information when a foreign corporation has been listed as the BO. The Assessment Team was not provided with information on how many corporations, foreign and domestic, have been listed as the BO but understand that approximately 10% of legal persons on the central BO registry have a company listed as the majority shareholder, suggesting this is a significant deficiency.

378. Singapore does not verify this BO information before it is published on the registry; they instead rely, at the point of incorporation, on the CSPs conducting proper CDD to identify the BO and ensure that information is accurately filed to ACRA's registry, as is their legal obligation. Most, but not all, legal persons engage a CSP to assist with formation. See IO4 for more details on ACRA's supervision of CSPs: whilst adequate for general AML/CFT supervision purposes, a large portion of CSPs (45% of all CSPs, who are of medium-low to low risk), were not inspected over the review period) do not receive a regular intervention, meaning their BO collection and filing goes unchecked by ACRA, the supervisor.

379. In addition to CSP supervision, ACRA conducts limited registrar audits to check accuracy of BO information after the information is made available on the RORC. ACRA has conducted audits for less than 1% of legal persons (domestic companies, foreign companies and LLPs) on the registry. Further, ACRA's audits are activity-agnostic; as such they do not target legal persons operating higher-risk business (such as maritime services) for their audits.

380. Overall, there are concerns around the accuracy of information in the RORC due to legal persons being listed as BO on the RORC, a significant number of CSPs not being subject to a supervisory activity in the last five years, and the extremely limited coverage of audits of BO information requirement for the central ACRA registry.

Other BO information

381. VCCs must maintain an up to date register of BOs and verify the accuracy of the information obtained for the register. This information would only be made available through the use of law enforcement powers, and they have been rarely used in Singapore for these purposes.

382. VCCs are not required to submit information on BO to the central BO registry. BO information would be accessed through the Eligible Financial Institution (EFI) of the VCC, but it may not be known to the requesting LEA who the EFI is to make that request. Singapore maintains that the close interagency co-ordination in Singapore, means this alternative mechanism has not hampered the availability and timeliness of such information. In 2025, Singapore conducted an exercise asking the top 50 VCCs through their respective EFIs to provide the BO information of the VCCs within two business days, which was satisfactorily complied with. EFIs have shown that they are able to provide VCCs' BO information in a timely manner if it is known which EFI has been engaged for a particular VCC, but the EFI may be unknown to the investigating LEA. This is currently a minor issue but would become more of an issue as the VCC sector continues to grow.

383. Unregistered Foreign Companies are not required to register with ACRA or file their BO information with the central register. Singapore would only be able to access BO information for these companies by requesting the information from the reporting entity where the Unregistered Foreign Company is a customer. The CDD done by FIs, VASPs and DNFBPs is the key mechanism for Singaporean authorities to access BO information on Unregistered Foreign Companies. In addition, Singapore is also able to seek BO information on Unregistered Foreign Companies from its international counterparts or foreign BO registries (where available). In turn, supervision of these FIs, VASPs and DNFBPs is therefore a key check for Singaporean authorities to ensure the accuracy of this information. The risk-based supervision of FIs, VASPs and DNFBPs for compliance with these obligations is in varying stages of implementation (see IO3 and IO.4) and checks of BO information are done during supervisory activities.

384. STRO has access to all of ACRA's registries, and as such can pass information obtained from these registries to share information with foreign counterparts. As noted above, Singapore authorities would have to request for BO information on an Unregistered Foreign Company from a reporting entity (or via international co-operation/tapping on overseas BO registries).

385. Overall, in Singapore, basic information is publicly available. BO information is largely available to competent authorities through the central ACRA registry but there are some instances (Unregistered Foreign Companies) where it is unavailable, and other instances (VCCs) or circumstances (where legal persons are the beneficial owner) where the information is not available in a timely manner in all cases. The basic and BO information is largely unverified beyond CDD, making the accuracy of the information questionable. Where information is not available through the RORC, there are alternative mechanisms that can make information available if LEAs are aware the reporting entity to ask.

5.4. Legal arrangements: Timely access to adequate, accurate and current basic and beneficial ownership information[30]

386. Singapore accesses basic and BO information on trusts through LTCs, PTCs and FIs. These methods can provide adequate and accurate information, but there is little verification on the quality of information and the decentralised holding of information may result in information not being available in a timely manner. Also, where basic information of LTCs, trustee managers or PTCs (as regulated agents of legal arrangements) is required, competent authorities are able to access it through the ACRA registry for legal persons.

387. While Singapore does not maintain statistics on the number of requests that LEAs send to reporting entities to obtain information, Singapore demonstrated a number of cases where LEAs had requested and successfully obtained information on legal arrangements from FIs and LTCs for the purposes of ML investigations. Singapore has had only four ML investigations involving legal arrangements. In these instances, CAD sought BO information from LTCs in two of the investigations, whilst in the other two ML investigations, CAD obtained the BO information on the legal arrangements in question from FIs.

388. Singapore considered implementation of additional prongs to support timely access to accurate information on legal arrangements and decided against implementing any additional prongs (namely a trust registry). This consideration was not documented and relied on the premise that information was available from LTCs (and to a lesser degree other relevant FIs and DNFBPs that conduct CDD). Singapore's consideration of which limbs of the multi-pronged approach to adopt did not properly take into account its context and materiality. In particular it did not adequately take into account trusts formed in Singapore but not by an LTC. Further, Singapore does not routinely check whether the information received from LTCs is accurate, particularly as the information provided by the LTC would be limited to the information provided by trust parties themselves. Lastly, in light of issues with verification mechanisms (see c25.8), the multi-pronged approach would allow a triangulation or double-check mechanism to ensure accuracy of information that would assist Singaporean authorities to identify networks (such as back-office data). Singapore acknowledged the risk understanding of trusts is limited by little data, but did not consider whether additional prongs would provide new and more comprehensive data to build their risk understanding or ultimately prevent and detect misuse.

389. The supervision of LTCs can be better systematised on the basis of ML/TF risks. Further, there is insufficient coverage and intensity for high and medium high-risk entities, including for BO obligations. Importantly, many LTCs went without a supervisory engagement during the review period, meaning their

[30] See the Methodology for Recommendation 25 regarding beneficial ownership information for legal arrangements.

CDD and determination of BO has not been checked for accuracy by a supervisor. Many medium-high risk LTCs received just one supervisory engagement in the review period.

390. The LARA identified wakafs to be of low ML risk and medium-low TF risk, and Singapore. Despite these identifications that wakafs are of lower risk, Singapore will be auditing all wakafs for their BO information in 2025, which is overburdensome for these lower risk entities, particularly in contrast to the lack of auditing of other legal arrangements.

391. Overall Singapore relies on requesting BO information from an LTC, PTC, MUIS or other reporting entity in order to provide basic and/or BO information to the requesting jurisdiction. There are no mechanisms in place to ensure the information provided is accurate, and no other 'prongs' are in place. These are significant deficiencies given trusts managed by an LTC and foreign trusts are rated as medium-high risk by Singapore. The issue of competent authorities not being able to quickly identify the holder of the information can prevent timely responses in cases.

5.5. Effectiveness, proportionality and dissuasiveness of sanctions

392. ACRA has a robust and automatic enforcement regime for non-compliance with annual report obligations which contain basic information. Enforcement for breaches of BO information requirements is relatively more nascent although penalty caps have recently increased to SGD 25 000 (USD 18 500) per offence. Singapore has shown willingness and ability to enforce against natural persons as well as legal persons.

393. Enforcement in regard to trusts usually against the LTC is negligible when considering the risk and materiality of the sector. From 2019-2024 MAS has taken nine supervisory actions against LTCs; three of these are in relation to breaches of BO obligations.

394. Singapore has progressively increased its enforcement efforts, concentrated on non-compliance with annual returns lodgements. ACRA records showed 70% compliance after the issuance of a fine or commencement of prosecutorial action. The fines imposed are comparatively low in value. More recent enforcement in relation to the RORC involve the pursuit of custodial sentencing to create a more dissuasive environment to criminal non-compliance. There is also a recent increase in the level of penalties applied. Overall enforcement is strongest for non-compliance in annual returns lodgement, and weaker in other areas.

Non-compliance with annual report obligations

395. Singapore has demonstrated a comprehensive approach to enforcement for non-compliance relating to basic information obligations. This is done through sanctions for late and non-filing of annual returns.

396. Legal persons that fail to file annual returns (containing basic information) are automatically tracked by ACRA systems. They will be charged an SGD 300-600 (USD 222-444) late filing penalty, and if automated enforcement (prosecution of the criminal offence of non-filing annual return) commenced, an additional composition fine of SGD 500 (USD 370) may be offered, in lieu of prosecution, to errant companies provided it files its annual returns. Companies can be and are prosecuted for a criminal offence of non-filing, and upon conviction by the State Courts, fined between SGD 600-1500 per charge (USD 444-1 110) in addition to the late filing, and additional fine. It is positive that ACRA is systematically pursuing these cases, but the sanctions administered are not dissuasive.

Table 5.4. Enforcement actions taken for annual returns non-compliance

Enforcement Actions	2020	2021	2022	2023	2024
Number of cases	425	1 899	3 214	14 432	4 795
Late filing penalties collected	SGD 4 662 050	SGD 10 520 855	SGD 10 864 525	SGD 17 726 110	SGD 19 553 940
Composition sum collected	SGD 111 900	SGD 366 870	SGD 687 770	SGD 2 686 690	SGD 3 253 060
Number of prosecutions	0	162	270	642	969

397. Approximately 70% of companies ACRA have enforced against for non-compliance of the requirement to file annual returns in 2022-2024 (totalling 22 441 cases), were found to be fully compliant with their subsequent annual return filing obligations as of 31 December 2024. This leaves 30% in continued non-compliance and such companies may be subjected to other sanctions and mitigating measures such as striking off (data provided on occurrence of this does not support a view that this always occurs). However, there still remains approximately one quarter of all legal persons not filing annual returns per year. Directors are disqualified if they have three or more companies struck off by ACRA within a five-year period. Companies are struck off after two years of non-filing of annual returns. Directors are also prosecuted if their companies are not compliant with the requirement to file annual returns.

Non-compliance with BO

398. Singapore's approach to enforcement for BO information is much more nascent as it corresponds to the introduction of the central BO register in 2020. In 2024 ACRA commenced prosecutions against 312 companies for the non-filing of BO information.

Box 5.2. Enforcement Actions for False Information

In 2021, ACRA received information that an Individual's identity had been misused to be appointed as a nominee director of more than 200 Singapore-incorporated companies.

Investigations conducted by ACRA into the CSP revealed that RQI (Natural Person T) had authorised staff of her CSP to lodge with ACRA various incorporations and company documents which falsely appointed the Individual as the director, shareholder and/or beneficial owner of the companies. Investigations also revealed that the companies to which the individual was appointed to without the Individual's consent or awareness were primarily owned by foreign nationals.

As a result of the breaches, ACRA cancelled the registrations of the CSP and its associated RQI in 2021. The companies involved have either been struck off from the Register of Companies or have updated their BO information with ACRA.

This case remains in Singapore's courts after being commenced on 23 May 2023.

399. ACRA has taken stringent action against individuals and CSPs for knowingly filing inaccurate BO information. From 2021 to 2024, the registration of six CSPs has been cancelled by ACRA for knowingly submitting inaccurate BO filings. To date, six individuals have also been prosecuted of which five were convicted and fined with fines ranging from SGD 2400 (USD 1800) to SGD 27 000 (USD 20 000) and disqualified from acting as a director for five years. It is positive that Singapore is pursuing liability against individuals knowingly submitting inaccurate or false BO information; however, this is not yet systematic and there are opportunities to pursue more of such individuals and create a more dissuasive environment against such criminal activity.

Table 5.5. Number of enforcement actions taken against FIs, VASP and DNFBPs for failure to collect basic or BO information of customers that are Legal Persons

AML/CFT obligated parties	2020	2021	2022	2023	2024
FIs	3	2	4	7	-
CSPs	-	11	2	-	10
PSMDs	-	12	4	4	10
REAs	3	1	-	2	1

400. There have been no sanctions applied for reporting obligations of wakafs.

401. Overall, Singapore's authorities are working to apply sanctions against persons who do not comply with the information requirements and have shown progress over the reporting period. The sanctions implemented, however, are not yet dissuasive as the legislative change to increase sanctions was recent and those sanctions have not yet been systematically applied).

6 Financial intelligence

The relevant Immediate Outcomes considered and assessed in this chapter is IO.6. The Recommendations relevant for the assessment of effectiveness under this chapter are R.29-32 and elements of R.1, 2, 4, 8, 9, 15, 34, and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) STRO, Singapore's FIU, is well resourced, has access to a large number of cross-governmental data sets and leverages on sophisticated systems to produce financial intelligence.

b) There is some ambiguity about the internal delegation of authority and, by extension, the full level of STRO's operational independence, but this did not affect its operation in practice (see R.29).

c) STRO has received approximately 282 000 STRs since 2020, predominantly from the banking sector, most of which are relevant, of good quality and submitted on a timely basis. There is limited STR reporting from a few medium-high risk sectors and certain threats (e.g. CSPs, LTCs and PSMDs), and retroactive submission of STRs in some medium-high threats/sectors could lead to delayed detection of criminality. To some extent, this constrains STRO's ability to analyse and produce comprehensive financial intelligence in relation to these sectors. As outlined in IO.5, there are also some cascading deficiencies with lack of accuracy of BO information and the timely availability of some information which can hinder the ability of STRO to perform analysis and LEAs to conduct effective investigations.

d) STRO and other competent authorities have access to a wide and expanding range of financial information (e.g. STRs, CMRs and CTRs), data and other information to facilitate investigations, enabling timely analysis through WINGS X. STRO makes available financial information through Machine-Analysed Spontaneous Disseminations (MASDs) and self-screening tools. It also produces financial intelligence products: Fin-IRs and financial intelligence packages and strategic analysis reports. The financial intelligence disseminations align with risks to a good extent. Most disseminations are related to standalone ML involving undefined foreign predicate offences and fraud, in line with Singapore's risk profile. There are comparatively fewer disseminations in respect of other high-risk threats, such as corruption and bribery, TBML and tax crimes.

e) Financial intelligence from STRO is being used to initiate and support investigations (26% of packages initiate an investigation and 14% of packages support investigations) to a good extent. Financial intelligence plays a smaller role when considering Singapore's significant investigation volume - only 2% of all the ML investigations and 38% of TF investigations have been initiated by financial intelligence. More could be done to leverage financial intelligence for higher risk

offences (except fraud). Competent authorities regularly use financial information to support investigations, develop evidence, identify and trace criminal proceeds or instrumentalities, including high-value and significant ML cases, but do not use financial intelligence to support investigations to the same degree. Both financial information and financial intelligence are used more often in larger cases.

f) STRO and competent authorities regularly and proactively co-operate with each other, as exemplified in AC3N and ACIP. They routinely exchange financial intelligence and information and co-ordinate on joint operational planning and responses, which has resulted in initiating and supporting cases.

Recommended Actions (RAs)

Singapore should:

a) Develop financial intelligence that more appropriately meets the needs of competent authorities, enhancing its use in ML investigations in line with risks.

b) Enhance the volume of STRs from key ML risks sectors (CSPs, LTCs and PSMDs) and on major threats (corruption, TBML, environmental crime), and ensure that reporting entities systematically apply red flag indicators, to improve timely detection by these sectors and on these threats.

a) Implement additional safeguards to ensure that STRO is operationally independent from SPF-CAD

b) Ensure that STRO secures access to additional strategically important sources of data, including cross-border information, to enrich the quality of its financial intelligence.

c) Maintain more granular statistics to ensure that its products better support the operational needs of competent authorities, including LEA feedback on the usefulness of financial intelligence, frequency of additional requests to STRO, and outcomes of disseminations.

Overall Conclusions on IO.6

STRO is a well-resourced FIU that uses its advanced IT systems to analyse a broad range of reports, including STRs, data and other cross-governmental information. Singapore has taken efforts to expand the data available to STRO since the last MER, and STR submissions have risen substantially due to outreach from Singapore's authorities. STRO's operational and autonomy is legislatively enshrined, but there is a minor issue that has not affected STRO's operations in practice.

STRO and other competent authorities demonstrate strong co-operation, particularly through platforms like ACIP. While Singapore has made efforts to enhance data integration across government, gaining information on cross-border money flows and improving the availability of STRs from certain high-risk FIs and DNFBPs would allow STRO to enrich its analysis further. The STRs that are submitted are generally of good quality and are submitted in a timely manner.

STRO's financial information is made available to LEAs through Machine-Analysed Spontaneous Disseminations and self-screening tools. STRO also produces generally good quality financial intelligence, in the form of Fin-IRs and financial intelligence packages, but these are not sufficiently risk aligned. STRO's financial intelligence supports the needs of competent authorities to a good extent, with40% of packages having initiated or contributed to investigations. Financial intelligence from STRO

is being used to initiate and support investigations to a reasonable extent but more could be done to leverage financial intelligence for higher risk offences (except fraud). Competent authorities regularly use financial information to support investigations, develop evidence, identify and trace criminal proceeds or instrumentalities, including high-value and significant ML cases, but do not use financial intelligence to support investigations to the same degree. Both financial information and financial intelligence are used more often in larger cases.

Singapore is rated as having a Substantial level of effectiveness for IO.6.

Immediate Outcome 6

6.1. Timely access to relevant, accurate and up-to-date information

402. Singapore places priority on cross-government data integration. As a result, competent authorities have access to a broad spectrum of reports, data and information. This integrated access provides accurate and timely information, supports intelligence gathering and facilitates the investigation of ML/TF and predicate offences.

6.1.1. By the FIU

403. Singapore's FIU, STRO, has access to a broad range of information including reports submitted by REs and governmental data to perform its functions. STRO is responsible for receiving, analysing and disseminating STRs, cash transaction reports (CTRs) and cash movement reports (CMRs) (see R.29). These are filed electronically using standardised fields on the STRO Online Notices and Reporting Platform (SONAR). This platform allows for direct interaction between STRO and REs, who can track their STR's utility on the platform.

404. STRO received 282 354 STRs since 2020 (Table 6.1), representing a 154% increase over the reporting period and a significant uptick in later years due to increased awareness-raising conducted by the FIU. In line with risks, the majority (82%) were submitted by FIs, primarily banks, followed by payment institutions offering money transfer services. STRs submitted by DNFBPs are comparatively lower (15%), notably from higher-risk sectors such as CSPs, LTCs, PSMDs and real estate agents/developers. As stated in IO.4, some of this discrepancy in reporting between DNFBP sectors can be attributed to the higher volume and transactional nature of casino activities over other DNFBPs.

Table 6.1. STR submission by reporting entity

Sector	ML NRA risk	2020	2021	2022	2023	2024	Total (% of total)
Financial Institutions	--	28 817	39 313	39 524	51 532	71 710	230 896 (82%)
Banks	High	19 651	27 584	28 799	40 815	59 945	176 794
Brokers dealers and corporate finance adv. Firms	Medium-Low	496	403	370	470	1 137	2 876
Direct life and composite insurers	Low	1 151	1 166	1 334	1 131	1 611	6 393
EAMs	Medium-High	30	23	19	51	46	169
Finance companies	Low	22	16	21	29	37	125
Financial advisers	Medium-Low	84	106	56	96	67	409
Fund management companies	Medium-Low	42	20	25	37	56	180
Moneychangers	Medium-Low	507	169	342	783	988	2 789
Non-bank credit card companies	Low	51	56	25	53	123	308
PSPs	Medium-High	6 082	9 202	7 367	7 676	6 881	37 208
Other FIs	--	701	568	1 166	391	819	3 645
DPTSPs	Medium-High	265	1 372	1 591	1 335	1 872	6 435 (2%)
DNFBPs	--	4 467	4 634	8 109	12 634	11 347	41 191 (15%)
Casinos	Medium-High	3 598	3 752	7 389	11 158	10 261	36 158
PSMDs / (incl. pawnbrokers)	Medium-High (PSMDs)	11	24	19	158	53	265
	Low						
CSPs	Medium-High	456	488	442	335	331	2 052
LTCs	Medium-High	145	100	82	92	115	534
Real Estate Agents/Developers	Medium-High	124	122	61	280	305	892
Lawyers	Medium-Low	107	117	98	556	207	1 085
Public and Professional accountants	Medium-Low	26	31	18	55	75	205
Others (non-REs)	--	333	578	622	1 240	1 059	3 832 (1%)
Total	--	**33 882**	**45 897**	**49 846**	**66 741**	**85 988**	**282 354 (100%)**

405. STRs are generally of good quality, largely due to the electronic submission process via SONAR. The system validates entry fields and prompts filers to correct errors prior to submission, which improves data accuracy and timeliness. STRO does not track STR quality metrics or statistics on clarifications sought from REs. However, STRO only rejected a negligible number of STRs during the reporting period. STRO does receive a high number of STRs without a clear offence, which is understandable as it is reasonable that REs do not always know the offence suspected of being committed, and this has a limited impact on STR useability in practice. Over the reporting period, 28% of STRs did not have an indication of the underlying offence (these are branded as "untagged STRs"). The numbers of untagged STRs have halved over the course of the reporting period due to ongoing outreach to REs and overall better reporting practices over time. STRO re-categorises the underlying offence associated to STRs once received, taking into account their broader information holdings. Detailed statistics on this re-categorisation process are unavailable, but case studies suggest that LEAs find value in untagged STR disseminations once re-categorised.

406. STRs by crime type somewhat align with risks identified in the NRA. STRO receives a high volume of reports related to fraud, organised crime and tax offences (Table 6.2). Conversely, STRs concerning some high-risk offences such as corruption, TBML and other notable ML threats such as environmental crime are comparatively lower given Singapore's risk and context. The limited volume of STRs on specific high-risk

offences/methodologies constrains STRO's ability to produce financial intelligence on these higher risk offences.

407. A significant proportion of STRs concerning medium-high risk sectors were initiated by adverse news or were filed reactively in follow-up to ACIP meetings. This includes 94% of corruption-related STRs (2021-2022) and 45% of STRs in relation to PSMDs and pawnbrokers (2020-2024). This indicates that red flag indicators are not fully systematised by some REs and may result in delayed reporting as suspicions arise only after public allegations emerge. This limits the operational value of these STRs.

Table 6.2. STR submission by crime type

STR by crime type	2020	2021	2022	2023	2024	Total (% of total)
Corruption	610	779	668	793	884	3 734 (3%)
Counterfeiting and piracy of products	56	81	81	75	43	336
Counterfeiting currency	5	6	2	6	14	33
Environmental crime	12	11	12	24	57	116
Extortion	13	28	11	24	90	166
Forgery	516	576	684	927	926	3 629 (3%)
Fraud	6 050	8 212	12 162	15 553	21 845	63 822 (45%)
Human trafficking and migrant smuggling	32	40	106	60	78	316
Illicit arms trafficking	10	13	21	40	23	107
Illicit trafficking in narcotic drugs and psychotropic substances	97	72	110	189	202	670
Illicit trafficking in stolen and other goods	9	20	11	15	10	65
Insider trading and market manipulation	337	361	303	343	476	1820 (1%)
Kidnapping, illegal restraint and hostage-taking	3	1	9	3	32	48
Murder, grievous bodily injury	5	6	9	5	22	47
Organised crime and racketeering	2 297	2 973	2 826	6 444	14 434	28 974 (20%)
Piracy	-	-	-	1	-	1
Proliferation Financing	37	17	25	70	33	182
Robbery or theft	43	125	126	50	78	422
Sexual exploitation, including sexual exploitation of children	10	13	9	20	30	82
Smuggling (incl. in relation to customs/excise duties & tax)	32	39	37	59	21	188
Tax crimes (related to direct/indirect taxes)	2 083	2 200	1 634	1 788	1 568	9 273 (7%)
Terrorism and TF	94	113	176	329	323	1 035 (1%)
TBML	206	158	120	171	216	871 (1%)
Other offences (1)	3 280	4 141	5 676	6 363	6 796	26 256 (18%)
Total	**15 837**	**19 985**	**24 818**	**33 352**	**48 201**	**142 193 (100%)**

Note: The total number in this table is different than in Table 3.1 as filers can tag more than one offence to each STR filed. Untagged STRs are excluded from this table. (1) These offences – which include regulatory-type offences – refer to 25 different offences, including sanctions-related offences, offences under the Casino Control Act, Payment Services Act, etc.

408. STRs are submitted in a timely manner. To ensure prompt reporting, STRO introduced a time-stamp feature on SONAR in 2018 to track how long REs take to file STRs after a suspicion arises. This mechanism has incentivised timely submission, with data showing that STRs are typically filed within five business days. To improve STR submission, quality and timeliness, STRO conducts regular outreach to REs, in co-ordination with supervisors. Information on the frequency of the outreach to REs is unavailable.

409. In addition to STRs, STRO benefits from a growing range of data points to enrich its analysis and support both operational and strategic analyses. This information, which can be accessed in a timely manner, includes CTRs and CMRs (a majority of which involve high-value cash declarations above SGD 100 000 or USD 74 000), databases and other closed sources of information (SPF's CRIMES3 case management system and administrative and tax records) (Table 6.3). STRO can also request additional information from REs via Section 5(3) CDSA powers, or ACIP to enrich its analysis, though statistics on such requests are unavailable. Singapore has introduced several legislative amendments since the last MER to broaden the range of available data points. Since 2024, for instance, STRO has been able to access trade data on a pre-emptive and direct basis, where previously this was only available upon request. This shift reflects a positive move toward a more proactive and automated approach to enriching information.

410. Singapore has yet to fully implement a 2016 MER recommended action to secure strategically important data like international electronic fund transfer reports. STRO does have some access to information relating to cross-border money flows and is able to develop broad macro understanding of these flows through the ACIP Risk Surveillance Workgroup. However, given that Singapore's greatest ML/TF risks originate from abroad, it is particularly important that Singapore can detect these criminal funds entering their financial system. Requiring REs to submit cross-border wire transfer reports would improve early detection of illicit funds into Singapore and support strategic analysis by enabling early detection of anomalies in cross-border transactions and facilitate periodic reviews of transactions involving high-risk jurisdictions.

411. STRO is equipped with advanced IT tools to hold and analyse information it collects and perform its functions. WINGS X analyses STRO's holdings through enriching various data-points (CTRs, STRs, CMRs) and cross-analysing this enriched information with external information, intelligence and data from both STRO and other databases (e.g. CRIME3, World Check, etc.). This is done with a view to establishing links between potential investigative targets and possible proceeds of crime, ML, predicate offences or TF.

Table 6.3. Data and other information available to STRO

Direct access	
CMRs	
Total (% increase over reporting period)	220 834 (332%)
CTRs	
Total (% increase over reporting period)	1.6 million (140%)
Database information and Owner	
INTERPOL data	SPF
BO registry	ACRA
Trade information	Singapore Customs
COSMIC information	MAS
STR, CMR and CTR data	STRO
Bankruptcy records	Insolvency & Public Trustee's Office (IPTO)
Criminal records	SPF
Household particulars	ICA
Ownership of cars	Land Transport Authority (LTA)
Ownership of land and private properties	Singapore Land Authority (SLA)
Travel records	ICA

Indirect Access	
Work pass details	Ministry of Manpower (MOM)
Tax information	IRAS
Employment details	MOM / Central Provident Fund (CPF)
Family records	Ministry of Social and Family Development (MSF) / ICA
Ownership of public housing	Housing & Development Board (HDB)
Ownership of shares and securities	Singapore Exchange (SGX)

6.1.2. By other competent authorities

412. Competent authorities spoke highly of their ability to access STR, CMR and CTR information from STRO. This information is either accessed through self-screening or 'Machine Analysed Spontaneous Disseminations' (MASDs).

413. Self-screening by competent authorities, which has increased 65% over the reporting period, is done through direct access to WINGS X. Competent authorities have used self-screening over 11 000 times over the assessment period. Some agencies were only onboarded in 2025, but Singapore's major investigative and regulatory bodies, such as SPF, ICA, ISD, CPIB and MAS, are the biggest users. While competent authorities may occasionally request STRO to conduct additional analysis based on this self-screening (Analysis on Request), the frequency is unknown. In respect of TF, STRO makes available self-screening and MASDs to both ISD and CFTB, ensuring that they have prompt access to financial information.

414. Singapore has invested significant human and financial resources into the creation and dissemination of MASDs (201 000 disseminations, primarily to LEAs such as SPF). WINGS X performs analysis of the FIU's and government's holdings to enrich the financial information received by STRO. Based on human designed rules, the result of this machine analysis is automatically disseminated to LEAs as MASDs. This is a product that identifies potential targets, their linkages, associated financial transactions and may include network visualisations where necessary. This process is entirely machine-led. The only human intervention is in developing/calibrating the system, defining the dissemination triggers[31] (co-developed with LEAs) and periodic audits of the results by the FIU's staff of some MASDs months after they are disseminated to ensure they are relevant.

415. While the technology is impressive, the AT therefore considers MASDs to be financial information rather than financial intelligence, with more limited actionable value in comparison to financial intelligence packages. Moreover, there are no detailed statistics on the breakdown of MASDs by risk area given the pre-set dissemination triggers, nor on the outcomes of disseminations, which hinders the AT's ability to assess whether MASDs fully support operational needs of LEAs in line with risks. However, interviews with the authorities and case studies indicate that despite the high volume of disseminations which could impede effective prioritisation, LEAs use MASDs to perform their functions. (see section 6.4).

416. Beyond STRO data, LEAs have direct access to a wide range of databases to support intelligence and investigations. These include administrative and tax records (e.g. income tax and GST returns), trader declarations relating to imports, exports and transhipments, travel history, telecom data, employment records, etc. SPF's case management system integrates with other databases to retrieve biodata and asset details (e.g. telephone numbers, vehicle and property details, etc.). The launch of 'Project POET' (Production Order Electronic Transmission project) in 2019 enables LEAs to electronically request information from dedicated FIs, hence accelerating asset tracing. As highlighted in Box 6.1, the NAVIGATE initiative reflects

[31] Disseminations occurs if the report matches: i) the suspect of an ongoing criminal investigation involving serious offences listed under the Second Schedule of the CDSA 1992; ii) previous screening conducted by competent authorities; and iii) other pre-agreed criteria/thematic rules.

Singapore's ongoing efforts towards greater data integration across agencies, including LEAs, STRO and financial supervisors.

Box 6.1. WoG co-operation through 'NAVIGATE' platform

NAVIGATE is a data-sharing project launched by the IMC-AML in 2024 enabling competent authorities to access each other's information (such as database information on individuals or entities of concern) and take appropriate supervisory or law enforcement action. Agencies involved include SPF, STRO, ACRA, MAS, URA, MinLaw, CEA, MOM.

417. As indicated in IO.5, while BO information for legal persons is largely accessible to competent authorities, gaps remain in the verification to ensure that data is accurate. Further, there are instances where data would sit outside the central registry (e.g., trusts, UFCs, VCCs or when legal persons are the beneficial owner) affecting timely accessibility from other sources. Overall, these challenges hinder the ability of the FIU to perform analysis and LEAs to conduct effective investigations.

418. Overall, STRO and Singapore's competent authorities have access to a wide range of reports, data, and information to investigate ML/TF and predicate offences. Singapore has demonstrated great efforts in enhancing data integration across government. Direct electronic access has enabled STRO and competent authorities' timely access to financial information in a consistent and up-to-date manner from the data sources of the FIU and competent authorities. LEAs have direct access to WINGS X and obtain a substantial volume of MASDs from STRO, however the extent to which these disseminations help other competent authorities perform their function and are commensurate with risks cannot be meaningfully assessed given the current limitations in statistical data. Furthermore, some challenges remain in the availability of a sufficient volume of STRs, especially from DNFBPs in higher-risk sectors and high-risk threats (other than fraud and organised crime) and access to BO information. The lack of systemic use of red-flag indicators utilised by REs operating in medium-high threats/sectors could lead to delayed reporting and timely detection of criminality.

6.2. Production and dissemination of financial intelligence

419. STRO is a well-resourced FIU that operates within SPF's Commercial Affairs Department (CAD) Intelligence and Administration Group, with a staff of 50, a 10% increase from the 2016 MER. Staff are distributed across three teams: analysis (23 staff), which handles operational and strategic work, systems development (15 staff) and FIU policy and international co-operation (12 staff). STRO has made significant investments in digitalisation, data analytics and automation, leveraging advanced IT systems to produce financial intelligence, trace assets and develop evidence. This includes SONAR and WINGS X, a customised analytical tool that was upgraded in 2022 to accommodate a growing number of reports and which allows for the analysis of large volumes of data.

420. STRO's operational independence and autonomy is legislatively enshrined within the CDSA. The Head of STRO is also the Director of SPF CAD, the principal investigative body for ML in Singapore. A Deputy Director (DD) sits under the Head of STRO, and according to STRO's SOPs is responsible for strategic workplan and operational decisions on the exchange and dissemination of financial intelligence. The DD is assisted by two Assistant Directors (ADs), who are responsible for (1) FIU Policy and International Co-operation, and (2) STRO Analysis and Disseminations. Decision-making of all operational matters, including financial intelligence disseminations is the purview of the operational staff themselves. Where necessary, dissemination decisions are escalated to the AD and/or DD. There is some ambiguity as the delegation of authority is not formalised or clearly identified in any policy/procedure. Furthermore, in

practice, Singapore has indicated that certain complex and high-profile cases are escalated to the Head of STRO for information only. The absence of a formal delegation of authority implies that legal responsibility for STRO lies with the Head of STRO and additional safeguards in this regard would be useful. This is, however, seen as a Technical Compliance issue (see R.29) as the AT has not observed this ambiguity affecting STRO's operations in practice.

6.2.1. Production of financial intelligence

421. STRO produces two types of financial intelligence products, which based on onsite discussions and samples consulted, are generally of good quality: (1) Financial intelligence packages ('packages') and (2) strategic analysis reports disseminated to competent authorities and REs. A 'Fin-IR' is an STR that has been analysed and augmented with other reports such as CTRs, CMRs, and is subsequently disseminated. Multiple Fin-IRs can be part of a single package.

422. The upgrade to WINGS X resulted in enhanced operational analysis capabilities and significantly reduced the need for manual assessment and prioritisation of reports. Upon receiving an STR, WINGS X will automatically overlay the STR with relevant information from secondary datasets. The system then prioritises STRs using thematic rules based on risks and typologies, NRA information, and customised rules pre-agreed with other competent authorities. These thematic rules are periodically updated through consultations with other authorities (e.g. through RTIG) to reflect the evolving typologies and the operational landscape. WINGS X automatically identifies entities mentioned in STRs and visualises their relationships in network diagrams highlighting links between individuals/entities. Based on this automated triage, WINGS X escalates STRs to staff for further analysis to identify links between targets and possible ML, TF or associated predicate offences. The volume of prioritised STRs to analyse further is unknown.

423. As many cases in Singapore contain international elements, STRO plays an active role seeking international co-operation to produce financial intelligence and disseminating these to competent authorities in Singapore. During the reporting period, STRO issued 1 465 Request for Analysis (RFAs) through the Egmont channel (an average of 293 per year), 88% of which were addressed (see IO.2). In respect of TF, STRO has a dedicated team of analysts reviewing and analysing potential TF STRs and enhancing financial information with other sources of information to produce TF-related packages.

6.2.2. Dissemination of financial intelligence

424. Historically, Singapore has tracked the dissemination of Fin-IRs. Statistics on the dissemination of packages are only available for 2023-2024 and the lack of longer-term statistics on these undermines the AT's ability to determine to what extent they support the needs of competent authorities. While the AT relied on statistics for both packages and FIN-IRs, figures for packages should not be aggregated with the numbers for FIN-IRs since packages consist of Fin-IRs and would be double counted.

425. As shown in table 6.4, STRO disseminates both Fin-IRs and packages. STRO also disseminates financial intelligence to its counterparts in response to the 1 744 Requests for Assistance (RFAs) it received, with a 97% response rate. STRO also spontaneously disseminated financial intelligence to its counterparts in 823 instances (see IO.2).

Table 6.4. STRO's disseminations

Type	2020	2021	2022	2023	2024	Total
Fin-IRs	9 428	4 833	3 382	6 139	7 136	30 918
Financial Intelligence Packages	--	--	--	236	233	469
RFA Executed	368	342	332	347	355	1 744
Spontaneous Exchange of Information	301	158	141	109	114	823

426. In addition to this, STRO also produces strategic intelligence reports and various guidance documents which aim to enhance understanding of the crimes/emerging risks and inform the development of red flag indicators. These are shared with competent authorities and REs. Since 2020, STRO produced 13 strategic reports on a range of topics: scams, tax crimes, BEC, corruption, and sector-specific reports e.g. legal practitioners, DPTSPs, PSMDs, etc. Strategic analysis focuses primarily on reviewing and evaluating submitted STRs, particularly the initiates for filing and indicators of suspicious financial activity. However, these strategic intelligence products make use of CTRs, CMRs, data from other competent authorities to a lesser extent than STRs. STRO also does not have complete access to data on cross border money flows (noted above), which affects its ability to undertake strategic analysis notably to identify and anticipate emerging ML/TF with a cross-border dimension.

6.2.3. FIU financial intelligence supporting needs of competent authorities

427. STRO's financial intelligence generally supports the needs of competent authorities (Box 6.2) and is broadly risk-aligned. 82% of Fin-IRs and 92% of financial intelligence packages are destined for LEAs, a large majority to the SPF, with the remaining going to supervisors. STRO prioritises TF-related packages and promptly disseminates these to both CFTB and ISD upon detection of suspicious TF-related transactions. This dual dissemination enables triangulation of analyses and collaboration between all three agencies as to the course of investigation.

Table 6.5. Categorised Disseminations of Fin-IRs and Financial Intelligence Packages

	Fin-IRs (2022-2024) (% of total)	Packages (2023-2024) (% total)
ML from fraud	2 075 (9.4%)	106 (18%)
ML from corruption and bribery	2 005 (9.1%)	28 (5%)
ML from tax crimes	1 581 (7.2%)	18 (3%)
ML from organised crime	720 (3.3%)	17 (3%)
TBML	308 (1.4%)	16 (3%)
Standalone ML (other ML')	3 728 (17%)	198 (33%)
ML from other predicate offences	6 422 (29.2%)	73 (12%)
Terrorism and Terrorism-financing	1 404 (6.4%)	35 (6%)
Proliferation financing	1 145 (5.2%)	34 (6%)
Other (i.e., UN sanctions, regulatory offences and unlicensed money-changing / remittances)	2 588 (11.8%)	77 (13%)
Total	**21 976 (100%)**	**602 (100%)**

Note: Total Fin-IR and Packages figures in this Table do not align with those in Table 6.4 (Fin-IRs: 30 918; Packages: 469), as each package may be tagged to multiple offence types.

428. Disseminations align with risks to a good extent (Table 6.5). A good number of packages (64%) relate to high-risk offences. Most disseminations (33%) are made in respect of suspected standalone ML cases involving undefined foreign predicate offences, which aligns with Singapore's NRA that indicates that Singapore is exposed to potential ML activities arising from foreign predicate offences. The second most

frequent type of dissemination by category relates to ML from fraud (18%). There are significantly fewer disseminations in respect of other high-risk offences such as bribery and corruption, TBML and, organised crime and more could be done to ensure disseminations are better aligned with risks (Table 6.5).

429. STRO received 282 354 STRs during the reporting period and disseminated 30 918 STRs as Fin-IRs (11%) or 6 184 Fin-IRs on average per year. In light of the significant volume and generally good quality of STRs received, improving the dissemination of Fin-IRs/packages in a way that is better aligned with risks would ensure STRO's disseminations more effectively support the operational needs of LEAs.

430. STRO systematically solicits qualitative feedback from all recipients of financial intelligence products on a twice-yearly basis. Co-ordination with other competent authorities via RTIG or bilateral channels also facilitates feedback on the usefulness of STRO products and case-specific information. STRO has six seconded officers to various competent authorities, both supervisors and LEAs, which has helped it develop a better understanding of operational needs of different competent authorities and tailor disseminations to their needs. Interviews with the competent authorities and case studies suggest that they find value in the FIU's disseminations (Box 6.2 and 6.4). However, statistics on the quality of financial intelligence, on the LEA's assessment of the relevance and usefulness of financial intelligence, and the extent to which it meets LEA's operational needs are not available. For example, there is no data on frequency of requests for additional information from STRO after receiving financial intelligence.

6.2.4. Other competent authorities producing financial intelligence (where relevant)

431. Other competent authorities also generate financial intelligence resulting from the analysis of available information to support their operational needs. LEAs use in-house analytical tools to aggregate financial intelligence packages disseminated by STRO and other financial information, enabling data mining and visualisations (Table 6.6). They also conduct independent intelligence probes, including database reviews, background checks, analysing financial records, and consultations with domestic or foreign partners. All AML/CFT supervisors have direct access to STRs filed by their respective REs, which supports network analyses and helps detect patterns relevant to supervisory activities.

Box 6.2. Production and use of financial intelligence

STRO disseminations supporting a drug ML investigation

A Singaporean national was arrested abroad and repatriated to Singapore in 2023, whereupon he was charged for drug-trafficking offences by CNB, who led the case. At CNB's request, STRO conducted an analysis of the entities and accounts of interest to CNB. STRO identified transaction flows and detected a pattern involving multiple large transfers from the syndicate's bank accounts to common counterparties in other jurisdictions within a similar time period. The analysis also identified up to 34 counterparts (e.g. money mules) transacting with the person of interest. STRO sent an Egmont RFAs to foreign FIUs (on behalf of CNB) seeking information on known subjects of interest. ACIP banks were also requested to provide additional information of relevant transactions (see Box 6.3). STRO disseminated within two months 37 Fin-IRs to CNB as well as information obtained from foreign counterparts, which supported its ongoing investigations. CNB pressed charges against the accused and two co-accused persons for drug trafficking and ML offences. The main accused person was convicted in December 2024 to 28 years' and 9 months' imprisonment (under appeal).

Spontaneous dissemination to foreign FIU

STRO received STRs on Person J, suspected of laundering proceeds from foreign tax fraud, with links to Person G, a hedge fund manager at Company C. STRO's analysis revealed Company C's account may have facilitated transfers tied to a €22 million tax fraud involving dividend withholding refunds in Country U. STRO spontaneously disseminated intelligence to foreign FIUs and CAD, which resulted in CAD initiating a ML investigation and the seizure of GBP 12.9 million and USD 7.9 million (respectively SGD 21.9 and 10.5 million) from Person J's account in Singapore.

Table 6.6. Financial information and intelligence available to competent authorities

	Financial Information		Financial Intelligence	
	Self-screening Requests (2020-2024)	MASDs (2020-2024)	Fin-IRs (2020-2024)	Packages (2023-2024)
LEAs	**11 312**	**200 990**	**25 469**	**433**
SPF	5 248	189 872	14 357	329
CNB	238	259	662	21
CPIB	1 076	899	3 076	18
IRAS	439	5 094	2 615	7
SC	161	273	124	10
ISD	1 191	915	3 856	43
ICA	2 648	3 664	756	2
HSA	12	-	2	-
NParks	21	1	4	1
MOM	278	13	17	2
Supervisors	**197**	**169**	**1 238**	**36**
ACRA	11	-	309	9
MAS	25	76	392	17
Charities Unit	7	2	25	3
MinLaw	86	58	499	7
GRA	29	4	1	2
CEA	2	-	11	-
URA	37	29	-	-
Law Society	-	-	1	-
Others	8	4	**48**	-
Foreign FIUs	-	-	**4 163**	-
Total	**11 517**	**201 163**	**30 918**	**469**

432. In conclusion, as a well-resourced FIU, STRO produces financial information, generally good quality financial intelligence, and strategic intelligence reports. Disseminations generally support the risks of competent authorities and are broadly risk aligned. Other competent authorities generate some financial intelligence, but this is weighted much lower compared to STRO's role.

6.3. Co-operation and exchange of information/financial intelligence

433. STRO and competent authorities regularly and proactively co-operate with each other. They exchange financial intelligence and information, strategic intelligence and co-ordinate on joint operational planning and responses, through a variety of channels and platforms using secure and confidential mechanisms.

6.3.1. Co-operation and exchange

434. As noted in IO.1, inter-agency co-operation is a strength of Singapore's AML/CFT regime. Singapore has been, and continues to be, actively exploring more effective avenues for co-operation, including to consider ways of better exchanging and exploiting financial intelligence.

435. STRO is a key participant in RTIG and AC3N. Within these platforms, STRO shares financial intelligence with MAS, ACRA, CAD and CPIB and other AML/CFT agencies. There is free exchange of financial information to prioritise and co-ordinate investigative or regulatory action, for example MAS shares financial information and intelligence with STRO emerging from its supervisory activities. Moreover, STRO uses RTIG to share information from its strategic analysis and exchange typological information on key trends in order to plan for and co-ordinate cross-government responses. AC3N provides competent authorities an opportunity to overlay financial intelligence with information from other sources, held by different agencies, such as business registration information, transactional data, and intelligence leads from LEAs. Between 2020-2024, 26 cases were initiated through AC3N, demonstrating the effectiveness of this mechanism.

436. Singapore's public-private partnership (ACIP) has proven to be a highly effective mechanism for fostering collaborative operational and tactical support between competent authorities and a limited number of REs (see IO.3). ACIP was set up in 2017 to collaboratively identify and assess key transnational ML risks confronting Singapore's financial and non-financial sectors, as well as measures to mitigate the risks and enhance the AML/ CFT regime. STRO co-operates closely with other LEAs and financial supervisors within ACIP, both in sharing strategic analysis through advisories to raise awareness about growing risks, as well as tactical financial intelligence sharing to facilitate case-specific responses (there have been six specific ACIP projects to share tactical information). This co-ordination has resulted in detecting, investigating and successfully prosecuting cases (see IO.1).

Box 6.3. Information Exchange within ACIP

Established in April 2017, ACIP fosters public-private collaboration between leading banks, LEAs, and authorities to address transnational ML risks. ACIP is co-chaired by MAS and CAD and supported by a steering group of senior compliance officers from major banks.

ACIP issues advisories, alerts, and best practice papers that enhance risk understanding and STR quality. Since 2019, tactical information-sharing has enabled case-specific intelligence exchange, leading to successful investigations in TBML and misuse of legal persons, leveraging private sector data to uncover previously undetected ML networks.

437. Legislative amendments introduced in 2019 allows STRO to proactively exchange information with all foreign FIUs without a need for an MoU or LoU. STRO can also exchange information with over 170 FIUs through Egmont's Secure Channel (ESC) and encrypted email with non-Egmont members. See IO.2 for more information.

6.3.2. Security and confidentiality

438. STRO is located within the SPF's premises, which are secured, restricted to the FIU's staff and separate from other SPF branches. Security and confidentiality are also an important feature of STRO's hiring practices. Various legislative provisions within CDSA and the Official Secrets Act ensure that competent authorities exchange information in a confidential manner, including when interacting with foreign partners. STRO has SOPs guiding the handling and dissemination of sensitive and confidential

information and to ensure the secure dissemination of financial intelligence to both domestic and foreign counterparts. According to guidelines, LEAs must seek consent from STRO to further disseminate information.

439. Reports are submitted by REs on SONAR, which has appropriate information security safeguards. STRO's IT systems capture and disseminate information in an electronic and encrypted manner and is audited regularly for security purposes. Information exchanged with foreign FIUs also benefit from the same level of security and confidentiality. STRO's database is accessible to relevant competent authorities, with appropriate information security safeguards.

6.4. Using information/financial intelligence

6.4.1. Using information / financial intelligence for investigations and developing evidence

440. Financial intelligence from STRO is being used to initiate and support investigations into ML, associated predicate offences and TF to a good extent but more could be done to leverage financial intelligence for higher risk offences (except fraud). Competent authorities regularly use financial information to support investigations, develop evidence, identify and trace criminal proceeds or instrumentalities, including high-value and significant ML cases, but do not use financial intelligence to support investigations to the same degree.

Use of financial information

441. As illustrated by case studies, statistics and discussions with authorities, competent authorities regularly use self-screening to support investigations and develop evidence. There is limited information on the use of MASDs, or on the outcomes of the use of financial information through the course of investigations.

442. LEAs leverage self-screening requests through WINGS X to support their ongoing investigations. During the reporting period, competent authorities submitted 11 517 requests, covering over 70 000 entities. The information obtained from these screenings helps LEAs trace financial flows and identify assets linked to specific entities or individuals. This may include details such as bank account information, criminal history and other relevant data, enabling investigators to build a comprehensive picture of potential illicit activity (see Box 6.4). It is difficult to extrapolate the usefulness of self-screening information in aggregate given limited statistics on how the information was used. However, that these requests are being performed by investigators at a high volume of requests (over 2 000/year) indicates that competent authorities find this information useful to contribute to developing evidence and tracing criminal proceeds.

443. MASDs overwhelmingly benefit LEAs, particularly SPF, which is appropriate considering its main role investigating ML, associated predicate offences, and TF (Table 6.6). Onsite discussions and case studies indicate that competent authorities use MASDs in investigations to develop evidence, identify assets and trace criminal proceeds or instrumentalities related to ML, associated predicate offences and TF (Box 6.4). MASDs can enhance investigations by corroborating suspicious transactions, hence enabling investigators to strengthen evidence and progress a case. Despite the substantial volume of disseminations, there is no statistics on how the MASDs were used and the AT cannot conclude on their usefulness.

Use of financial intelligence

444. Financial intelligence from STRO is being used to initiate and support investigations to a good extent: 26% of financial intelligence packages and 17% of Fin-IRs led LEAs to initiating an investigation, while 14% of packages and Fin-IRs supported investigations. Packages have a higher level of actionability (the summation of their use in initiating or supporting investigations) at 40%, compared to 31% for Fin-IRs. Overall:

a) Case studies indicate that financial intelligence is used to initiate and support ML investigations but plays a negligible role overall in initiating ML cases as only 2% of all the ML investigations conducted by LEAs have been initiated by financial intelligence (see table 7.1). The AT has weighted this accordingly under IO.7.

b) Case studies and discussions with LEAs indicate that financial intelligence is used in investigations and to develop evidence into a range of predicate offences. Data on the 'actionability' of STRO's financial intelligence (Table 6.8) indicates that Fin-IRs and packages help initiate investigations to a reasonable extent. However, as discussed in Section 6.2, financial intelligence produced and disseminated by STRO aligns with the country's risks to a good extent.

c) Singapore makes good use of financial intelligence to initiate and support TF investigations. 11% of TF-related financial intelligence packages initiated a TF investigations while packages supported 28% of ongoing investigations. The AT has weighted this accordingly under IO.9.

Table 6.7. Breakdown of financial intelligence from STRO to initiate and support investigations

	2020 (% total)	2021 (% total)	2022 (% total)	2023 (% total)	2024 (% total)	Total (% total)
Fin-IRs	**9 428**	**4 833**	**3 382**	**6 139**	**7 136**	**21 490**
Of which *initiated* investigations (% of total)	298 (3)	411 (9)	588 (17)	1 148 (19)	1 450 (20)	3 597 (17)
Of which *supported* investigations (% of total)	1 047 (11)	783 (16)	244 (7)	1 441 (24)	595 (8)	3 063 (14)
Financial intelligence packages	**-**	**-**	**-**	**236**	**233**	**469**
Of which *initiated* investigations (% total)	-	-	-	53 (22)	68 (29)	121 (26)
Of which *supported* investigations (% of total)	-	-	-	31 (13)	35 (15)	66 (14)

Note: For years where both financial intelligence packages and Fin-IRs are reported, there is a risk of double counting and figures should therefore not be aggregated. (packages contain Fin-IRs). Figures from 2020 are excluded from the Totals, as Fin-IR figures for 2020 include MASDs. Totals are therefore for 2021 to 2024 only.

Table 6.8. Impact of Fin-IRs and packages on investigations (by type of offence)

	Fin-IRs			Packages		
Type of offence	**Dissmn't (2022-2024)**	**Inv. *initiated* (% dissmn't)**	**Inv. *supported* (% of dissmn't)**	**Dissmn't (2023-2024)**	**Inv. *initiated* (% dissmn't)**	**Inv. *supported* (% dissmn't)**
Fraud and related ML	2 075	874 (42%)	125 (6%)	106	31 (29.2%)	13 (12.3%)
Corruption and bribery, and related ML	2 005	51 (2.5%)	19 (1%)	28	4 (14.3%)	4 (14.3%)
Tax crimes and related ML	1 581	134 (8.5%)	48 (3%)	18	11 (61%)	1 (5.6%)
Organised crime and related ML	720	239 (33%)	56 (8%)	17	3 (17.6%)	2 (11.8%)
TBML	308	84 (27%)	10 (3.2%)	16	5 (31%)	1 (6.3%)
'Other ML' (suspected domestic ML cases related to foreign predicate offences)	6 422	1 880 (29%)	1 776 (27.6%)	198	60 (30%)	24 (12%)

	Fin-IRs			Packages		
Type of offence	**Dissmn't (2022-2024)**	**Inv. *initiated* (% dissmn't)**	**Inv. *supported* (% of dissmn't)**	**Dissmn't (2023-2024)**	**Inv. *initiated* (% dissmn't)**	**Inv. *supported* (% dissmn't)**
All other predicate offences and related ML	3 728	932 (25%)	1 666 (44.7%)	73	24 (32.9%)	14 (19.2%)
Terrorism and Terrorist Financing	1 404	71 (5%)	58 (4.1%)	35	4 (11.4%)	10 (28.6%)
Proliferation Financing	1 145	2 (0.2%)	13 (1.1%)	34	1 (3%)	2 (5.9%)
Other sanctions, regulatory offences and unlicensed money-changing / remittances	2 588	379 (14.6%)	160 (6.2%)	77	16 (20.8%)	7 (9.1%)
Total	**21 976**	**4 646**	**3 931**	**602**	**159**	**78**

Note: Totals may be different than the above Tables, as Fin-IRs and financial intelligence packages may involve multiple offences. Each row accounts for both the predicate offence, and the related ML investigations.

Use of financial information/intelligence by other competent authorities

445. While there are some issues with STRO's disseminations in respect of ML, case studies and onsite discussions indicate that competent authorities regularly use financial information and financial intelligence for investigations, developing evidence and tracing assets. They use a broad range of data points (see 6.2.2) and information (e.g. disseminations from STRO, database information, searches, human intelligence, and information from international counterparts – the latter two are especially used in TF cases) to develop evidence, identify assets and trace criminal proceeds or instrumentalities related to ML, associated predicate offences and TF. For example, CNB utilises link charting software to visualise money flows between entities, uncover relationships and identify nodes of interest. CPIB has similarly incorporated new technologies to review financial statements and automate the digitisation of bank statements into structured data, thus facilitating data mining and visualization. LEAs also leverage private sector capabilities in data analytics (ACIP) to improve the detection of ML networks. Other sources of information include PPPs (e.g. ACIP) and information gathered from foreign counterparts. STRO sent 1 465 RFAs to foreign FIUs, with an 86% response rate, mostly on behalf of SPF. This is further highlighted in case studies below (Box 6.4).

6.4.2. Using information / financial intelligence to assist in identifying and tracing criminal proceeds or instrumentalities

446. Competent authorities regularly use financial information to support investigations, develop evidence, identify and trace criminal proceeds or instrumentalities, including high-value and significant ML cases, but do not use financial intelligence to support investigations to the same degree. Most high-value seizures undertaken by LEAs involve investigations that used financial information and/or intelligence, amounting to SGD 5 billion (USD 3.7 billion), showing that there is increased likelihood of using financial information and intelligence in larger cases.

447. As case studies demonstrate (Box 6.4), both STRO disseminations and financial intelligence undertaken by competent authorities are used to identify and trace assets, where necessary through a co-ordinated process both domestically and abroad (via EGMONT). STRO also contributed to tracing assets and determining financial connections, both proactively and upon request, in some high-level cases (such as the 3B$ case in 2023, Singapore's largest ML case).

Box 6.4. Using of financial information and financial intelligence

MASDs supporting the needs of CAD

In 2021, STRO supported IRAS in reviewing four GST-registered PSMDs suspected of gold-related Missing Trader Fraud (MTF) by conducting fund tracing and network analysis, identifying red flags such as circular trading . IRAS uncovered a GST fraud scheme involving the purchase of Investment Precious Metal (IPM) gold and referred the case to CAD for ML investigations. CAD traced over SGD 250 000 (USD 185 000) in illicit funds through cash withdrawals and remittances to Country X, linking back to the dealers, after screening STRO's database, linked suspicious gold sales and bank transactions. In August 2024, STRO automatically disseminated three new STRs linked to the initial screening conducted by CAD, confirming GST evasion and fund flows. This helped corroborate evidence and support ongoing investigations.

Asset tracing, whole of government response and international co-operation

In late 2020, CAD uncovered a large BEC fraud scheme involving over 3 000 Singaporean shell companies used to receive fraudulent payments from overseas victims, totalling over USD 107.6 million (SGD 144 million). Funds were then quickly moved to accounts in another country. The syndicate behind this operation used Singaporean CSPs to incorporate companies, set up bank accounts and recruit nominee directors in Singapore. A joint RTIG–ACIP project generated 990 STRs, 40 RFAs, and Fin-IRs from STRO, enabling the seizure of USD 33 million and blocking USD 20 million (respectively SGD 44.2 and 26.8 million). 12 individuals were charged for offences related to directorship and CSP roles. As of February 2025, seven were convicted and sentenced to fines and imprisonment. Supervisory actions were also taken, including examinations by ACRA and advisories issued by MAS.

448. In conclusion, financial intelligence from STRO is being used to initiate and support investigations to a good extent but more could be done to leverage financial intelligence for higher risk offences (except fraud). Competent authorities regularly use financial information to support investigations, develop evidence, identify and trace criminal proceeds or instrumentalities, including high-value and significant ML cases, but do not use financial intelligence to support investigations to the same degree. Both financial information and financial intelligence are used more often in larger cases.

7 Money laundering investigations and prosecutions

The relevant Immediate Outcomes considered and assessed in this chapter is IO.7. The Recommendations relevant for the assessment of effectiveness under this chapter are R. 3, 30, 31 and elements of R.1, 2, 15, 32, 37, 39 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Singapore has an appropriate legal and operational framework to identify and investigate ML, supported by competent, well-resourced and trained LEAs. Over 80% of ML investigations are initiated from victims' complaints in relation to CEF. Other sources, such as financial intelligence, referrals from predicate agencies, and international co-operation, are underutilised to identify ML. The use of financial intelligence to detect ML involving foreign predicates is comparatively better than for domestic predicates, but this is still not in line with Singapore's higher exposure to foreign predicate offences.

b) LEAs opened 11 189 ML investigations, a very significant number for a country of Singapore's size. 93% involve domestic predicate offences, a majority of which focus on money mules linked to CEF, which only partly aligns with Singapore's risk and context. While LEAs focus on laundering of the proceeds from fraud to an overly appropriate extent, there are fewer investigations into other higher-risk areas like tax crimes, corruption and TBML, which aligns with Singapore's risk and context only to some extent. Resources are primarily focussed into ML from simpler cases targeting CEF at the expense of major transnational investigations.

c) Singapore experienced challenges converting investigations into prosecutions, owing to both the nature of the investigations pursued (money mule investigations with a foreign nexus) and challenges in establishing *mens rea*. Singapore has introduced legislation to facilitate the prosecution of ML cases, but these changes are recent and their impact remains to be established. Singapore prosecutes few legal persons, local directors and professional intermediaries, which is not in line with its risk and context.

d) Singapore pursues different types of ML (including third party, and standalone ML). As demonstrated by the 3B$ case, Singapore has shown an ability to conduct ML investigations

into higher-risk predicates and complex investigations (both domestic and foreign), including organised crime, tax, and TBML.

e) Overall, Singapore achieves a good conviction rate (82%), including in complex cases, although the majority of sanctions are made for low-level money mule cases, rather than professional syndicates, professional intermediaries, and legal persons. Singapore has a high incidence of guilty pleas (including plea bargaining), which undermines the overall deterrence of sanctions.

f) ML sanctions for natural persons are proportionate, but not effective or dissuasive. Most sanctions are on the lower end of the spectrum even for the most aggravated cases, and ML penalties are usually lower than those for the predicate offence. Recent sentencing guidelines, which are not specific for ML, also limit the deterrent effect of ML prosecutions. There have been few convictions for legal persons, and therefore it is not possible to assess the effectiveness of sanctions imposed.

g) To some extent, Singapore employs a combination of criminal, administrative and regulatory tools as alternative measures when it is not possible to secure ML convictions. Some of these (like the Money Mule Offence) were recently introduced and it is premature to assess effectiveness. There is a low use of alternative measures when compared to the number of cases where a conviction cannot be secured. Evidence from recent years suggests Singapore is becoming increasingly reliant on alternative measures, potentially rather than pursuing ML convictions.

Key Recommended Actions (KRAs)

Singapore should:

d) Review and refine the process for prioritising ML investigations (particularly in relation to CEF) to better consider Singapore's risk and context, and pursue complex, high-value investigations.

e) Pursue investigations and prosecutions for local directors and professional intermediaries who are facilitating ML activity within Singapore's borders.

f) Ensure that effective and dissuasive sanctions are applied proportionately to the offence, including tailored sentencing guidelines for ML.

Other Recommended Actions

Singapore should:

a) Review the operational framework to ensure that ML investigations can be opened more frequently from financial intelligence when there is no direct link to a predicate offence.

b) Monitor the application of alternative measures (i.e., the Money Mule Offence) to ensure they are not used as a substitute for pursuing ML offences.

Overall Conclusions on IO.7

Singapore has an appropriate legal and operational framework to identify and investigate ML. Over 80% of ML investigations are identified from CEF victim reports, while financial intelligence and referrals from predicate LEAs are much more rarely used to initiate ML investigations. This systematic opening of ML investigations based on victim complaints does not result in Singapore prioritising major, high-value investigative targets.

While LEAs opened 11 189 ML investigations, a very significant number, a majority relate to low-level money mule investigations rather than significant complex ML investigations. Singapore shows capacity in pursuing complex ML investigations, supported by co-ordination and PPPs, but there are ongoing challenges with the pursuit of subjects located outside of Singapore. ML prosecutions and convictions are aligned with risk only to some extent, as LEAs primarily pursue CEF-related ML, while other major threats (e.g. tax crimes, drugs, TBML) are under-addressed.

Singapore has introduced a case prioritisation model, with limited success. Many thousands of the ML investigations are closed and not considered for prosecution as they are viewed as having a low chance of success. The AGC has a high prosecution to conviction rate (82%). Singapore prosecutes few legal persons, local directors and professional intermediaries, which is not in line with its risks and context. Prioritising prosecutions that are more likely to result in a guilty plea (including plea deals) undermines the deterrent effect of the sanctions for those convicted, even for the most aggravated cases.

To some extent, Singapore has implemented a mix of criminal, administrative, and regulatory measures when ML convictions are not feasible, such as the Money Mule Offence. While promising, some of these measures are recent, and overreliance on these could run the risk of focusing away from core ML enforcement.

Singapore is rated as having a Moderate level of effectiveness for IO.7.

Immediate Outcome 7

449. Singapore has an appropriate legal and operational framework, including good inter-agency co-operation, to identify and investigate ML.

7.1. ML activity identified and investigated

7.1.1. Staffing, resourcing and collaboration

450. Singapore established a robust legal framework to combat ML (see R.3), which is regularly updated to address emerging risks. Recent amendments have enhanced information sharing and expanded intelligence sources available to LEAs. The three primary LEAs responsible for investigating ML linked to predicate offences within their respective mandates are the SPF, the CNB, and the CPIB. In practice, SPF's Financial Investigation Group (FIG) within the Commercial Affairs Department (CAD) is the investigative lead for ML and takes on the most complex ML investigations (see R.30 and R.31). LEAs are well-resourced and trained and leverage a wide range of tools and platforms for investigations, including NAVIGATE and POET (Box 6.1). LEAs also co-operate well together, either bilaterally or through multilateral platforms such as AC3N, ACIP and RTIG.

451. Singapore has enhanced its ability to detect and investigate ML, especially in response to emerging and increasingly prominent threats like CEF. SPF established the Anti-Scam Centre (ASC) in June 2019, and the Anti-Scam Investigation Division within CAD in 2021, expanded to the Anti-Scam Command (ASCom) in 2022. ASCom embeds bank representatives with SPF to enable timely information sharing and rapid responses for freezing and seizing assets. Since 2023, AGC also has a team of specialised Deputy Public Prosecutors (DPPs) within CAD to provide early-stage and quick legal advice to CAD. CAD set up a satellite office at IRAS in 2021 to support the early detection and referral of tax-related ML investigations and to build IRAS' internal ML detection capabilities.

452. LEAs operate under the National AML Strategy and the LEA Strategy to Combat ML, which define operational priorities and promote inter-agency co-operation. 'Predicate agencies' (such as HSA, ICA, MOH, MOM, NEA, NParks, SC, etc.) conduct financial investigations through basic inquiries to establish the presence of proceeds of crime. According to a referral mechanism based on complexity, predicate agencies may refer potential ML activity to CAD where estimated proceeds are above SGD 20 000 (USD 14 800), or where other specific conditions are met (e.g., more in-depth investigations requiring asset-tracing). Where that is not the case, the pursuit of an ML investigation is discontinued.

7.1.2. Identification of ML investigations

453. Singapore faces significant ML risk from foreign predicate offences, particularly CEF, targeting Singaporeans, and subsequent ML from these offences in Singapore, and to criminals misusing Singapore's large and connected financial sector to launder the proceeds of crime. The majority of investigations are reactive, triggered by police reports. While inter-agency co-ordination is a positive measure in detecting ML, there is ample room for improvement to diversify the range of sources to detect ML.

454. ML investigations are largely reactive with 82% triggered by police reports filed by CEF victims, predominantly based in Singapore, which are the domestic component of scam operations with a foreign nexus (Table 7.1). The nearly four-fold increase in ML investigations triggered largely by CEF victim complaints over the years since the previous MER reflects the increasing risk posed by CEF. It also demonstrates growing public awareness due to the efforts of the Singaporean authorities. Singapore does not sufficiently rely on an intelligence-led ML identification and investigation system and the over-reliance on victims' complaints diverts LEAs' attention and resources from more complex ML activities, such as those involving professional enablers, corruption, and complex cross-border structures.

Table 7.1. ML investigations per source (domestic vs. foreign predicates)

	Domestic ML investigations	Foreign ML investigations	Total ML investigations	% of total ML investigations
Complaints from victims	8861	302	9163	82
Referrals from other agencies / Predicate investigation	1496	17	1513	14
Foreign counterparts (1)	2	247	249	2
Financial / other intelligence sources	77	187	264	2
Total	**10 436**	**753**	**11 189**	**100**

Note: Information identified through a fusion of sources, such as with public-private partnership or inter-agency mechanisms, have been subsumed in the most appropriate of the four headers above, to avoid double-counting. (1) this includes cases opened based both on formal and informal co-operation.

455. There is ample room for improvement to diversify the range of sources to detect ML, since referrals from predicate agencies, financial intelligence (from STRO and LEAs), and international co-operation play a limited role. Financial and other intelligence sources, including STRO disseminations, play an insignificant role in identifying ML compared to the total volume of investigations. Only two percent of ML investigations are triggered by financial intelligence, indicating Singapore can be much more intelligence-led in their approach. The contribution of financial intelligence is more pronounced for detecting ML involving foreign predicate cases (25%), but this case number remains modest relative to the overall ML caseload. This disproportion of domestic vs foreign cases is also misaligned with Singapore's heightened exposure to foreign predicate offences.

456. Inter-agency co-ordination mechanisms like AC3N and ACIP are key strengths in Singapore's detection approach. 18 ML investigations were initiated and another 154 investigations advanced through ACIP, while 19 ML investigations were initiated through AC3N. These instances of ML were identified through STRO and LEAs sharing leads with ACIP banks, which then analysed information and submitted new leads or STRs. While these are positive developments, and the AC3N and ACIP models prioritise high value investigations, the overall number of instances that they have collectively resulted in ML investigations (37) is insignificant in comparison to the total number of ML investigations (11 189), showing clear room for improvement.

457. ASCom works together with banks to detect ML, sharing targeted information on leads and leveraging their in-house data analytics models and network detection capabilities. This collaborative approach enables ASCom to identify ML operations orchestrated by criminal syndicates, freeze the associated bank accounts, and effectively disrupt the laundering networks (see Box 7.1). ASCom has resulted in very significant positive results and is the driver behind substantial investigations into ML from CEF.

7.1.3. ML Investigations

458. Singapore opens an overwhelming amount of ML investigations into CEF cases (primarily money mules) and primarily involving domestic predicate offences. This only partly aligns with Singapore's risk and context. While authorities investigate complex cases, there are challenges using international co-operation in order to follow the trail of criminal proceeds. A case prioritisation model is in place to prioritise CEF cases, which has had limited success.

459. LEAs conducted 11 189 ML investigations, a 141% increase overall in the reporting period, although growth has recently plateaued. S17 of the CPC sets out a low threshold for initiating investigations and is also the legislative trigger to be able to use LEA powers. This results in a systematic approach to opening ML investigations whenever there is suspicion of a predicate offence followed by laundering, or when a standalone ML case is opened, which is generally the circumstance for foreign fraud investigations with victims in Singapore. Accordingly, SPF pursues standalone ML investigations for every CEF report, and ML investigations arising from CEF investigations are over-represented as compared to other key threats (discussed further below).

460. 93% of ML investigations involve domestic predicate offences where both the crime and laundering occur in Singapore (Table 7.2). While many of these domestic predicate ML investigations have a foreign nexus due to CEF syndicates operating in a foreign jurisdiction, these are distinctly different from foreign predicate ML in which Singapore as an IFC is misused for laundering. The heavy emphasis on ML investigations into domestic predicates suggests that LEAs focus on targeting domestically generated crimes. This only partly aligns with Singapore's risk and context, since the NRA highlights foreign predicate offences and cross-border ML as higher-risk areas. As an IFC, Singapore is exposed to foreign predicate offences by syndicates operating abroad, targeting victims abroad, but laundering proceeds through Singapore's financial system.

461. The pursuit of laundering of the proceeds from fraud, Singapore's highest ML risk predicate offence, is done to an overly appropriate extent and accounts for over 91% of all investigations (Table 7.2). However, these investigations involving laundering the proceeds of fraud predominantly target domestic money mules (MMs) rather than professional enablers or the controlling minds of the criminal enterprise, who are typically abroad). ML from other higher-risk offences (i.e., tax crimes and corruption) is investigated to a limited extent, which is only in line with Singapore's risks and context to some extent. There were dramatically fewer ML investigations related to the proceeds generated from other higher-risk offences such as tax crimes (34 investigations or less than 1% of all ML investigations) and corruption (100 investigations or approximately 1% of all ML investigations). Further, there were few investigations into higher risk ML methods like TBML, including SBML (49 investigations or less than 1% of all ML investigations). Other potentially significant sources of information on laundered proceeds are underutilised. For example, 1 820 STRs relating to insider trading and market manipulation received by STRO during the review period (Table 6.2) generally did not lead to starting a ML investigation. Overall, the focus on ML from CEF overweighs Singapore's investigative resources into one high risk offence at the expense of others, and the approach to these cases puts resources into predominantly simpler cases targeting MM.

Table 7.2. Investigations (per predicate offence)

Predicate Offence	Domestic ML investigations (% of total)	Foreign ML investigations (% of total)	Total ML investigations (% of total)
Fraud	9 007 (85)	639 (6)	9 646 (91)
TBML	24 (0)	25 (0)	49 (0)
Organised Crime	63 (1)	36 (0)	99 (1)
Tax	18 (0)	16 (0)	34 (0)
Corruption	68 (1)	32 (0)	100 (1)
Drugs	419 (4)	8 (0)	427 (4)
Others	183 (2)	22 (0)	205 (2)
Total	9 782 (93)	778 (7)	10 560 (100)

Note*:* The total figures in this Table do not tally with Table 7.1 as an investigation may relate to more than one category of threat (e.g. TBML and organised crime). Additionally, statistics from SPF's land divisions for 2020 to 2022 cannot be further broken down into threat type due to data migration issues.

462. The authorities demonstrate sophistication and skills in conducting complex ML investigations, including those involving ML from foreign predicate offences. Case studies highlight LEA's ability to dismantle sophisticated organised crime networks (e.g. 3B$ case), with investigations involving a range of asset types (e.g. real estate, virtual assets), legal entities, professional intermediaries, and jurisdictions (see Box 7.1). LEAs are well co-ordinated and make effective use of domestic tools, inter-agency mechanisms and international co-operation channels (e.g. FIU-to-FIU channels and informal (police-to-police) networks, EGMONT, INTERPOL, ARIN-AP, etc.).

463. However, case studies and interviews with the authorities also indicate challenges linking ML to foreign predicate offence. Greater efforts are needed to follow the trail of criminal proceeds through various layers using international co-operation, especially in complex investigations. Singapore's ability to pursue ML cases involving foreign-based criminals is constrained by challenges in international co-operation, such as uncooperative partners, and difficulties in obtaining evidence from abroad. Although recent legislative amendments (discussed below) intend to ease this burden by removing the need for prosecution to prove that the property in Singapore was in fact benefits from criminal conduct, these changes are too recent to assess their effectiveness. As discussed in IO.8, asset tracing in cross-border cases also remains a significant operational challenge.

464. Singapore has made some operational adjustments to better handle the volume of ML investigations, particularly CEF cases. Specifically, SPF introduced a case prioritisation model (co-developed with AGC) with limited success to process the high number of CEF investigations and identify those cases that should be prosecuted. Singapore applies a two-tier approach to prioritise CEF cases and separate out those 'non-egregious' cases, wherein those assessed to fulfil specific offender-specific and offence-specific conditions (about 32%, or 3 595 cases) will be eligible for an 'Advisory' (administrative measure) in lieu of prosecution. Although driven by an assessment of whether available evidence does not meet the evidential thresholds required to prove ML (discussed below), the deprioritisation framework also accounts for few risk factors, and this approach helps Singapore manage the heavy case inventory to an extent. In total, authorities conducted 11 189 ML investigations but prioritised 7 594 cases (submitted for prosecution).

465. Overall, Singapore has well-resourced, capable LEAs to identify and investigate ML. They primarily use ML laws to investigate all CEF cases (which drive the majority of ML cases), irrespective of the value of fraud proceeds. This results in a high volume of investigations, which are usually low in value but high in volume, instead of complex, high-value ML involving professional enablers or controlling minds of the criminal syndicates. Authorities concentrate on domestic elements of ML offences (where they can better control outcomes) and rely heavily on victim complaints. This approach has also diminished resources available to pursue ML from other crime types identified as higher risk by Singapore's NRA.

Box 7.1. ML investigations

3B$ case (2023)

In 2021, authorities noted a surge in luxury property purchases in Singapore, prompting STRO to conduct a thematic review of STRs filed between 2019 and 2021 on high net worth individuals. This showed STRs reporting large inflows into Singapore without any apparent links to criminal proceeds. Several STRs also raised concerns abouts source of wealth, including dubious support documentation.

A multi-agency taskforce (SPF, AGC, STRO) coordinated intelligence and investigations. SPF sent 33 informal requests to 10 jurisdictions, while STRO engaged at least 10 FIUs. Asset tracing was hindered by overseas MVTS, suspected unlicensed PSPs, and complex cross-border fund flows, with insufficient

evidence to recover assets abroad. SPF also investigated over 20 companies linked to 10 suspects of interested and six professional intermediaries, including bankers, CSPs, and real estate agents.

After an 18-month covert investigation, 10 individuals linked to foreign organised crime were arrested in August 2023 and charged with forgery, falsification, and ML linked to foreign remote gambling offences. 2 former relationship managers were also prosecuted for abetting the creation of forged documents and ML offences.

ML investigation from a victim's complaint

CAD received complaints from eight Singapore-based victims of love scams, with losses exceeding SGD 380 000 (USD 281 000). Two overseas culprits had instructed three Singaporean women to open bank accounts to receive the proceeds. Fund flow analysis showed a further SGD 370 000 (USD 274 000) from foreign sources passed through these accounts in Singapore.

The culprits were arrested abroad, extradited, and charged in Singapore, and some funds in Singapore had dissipated. In December 2021, one offender received five years' imprisonment for ML involving over SGD 550 000 (USD 407 000) and another received four years and two months for ML involving SGD150 000 (USD 111 000). The three women were convicted under S44 CDSA and sentenced to between 3.5 and 15-months imprisonment.

7.2. Prosecuting and convicting different types of ML activity[32]

466. Singapore has introduced a case prioritisation model with limited success to process the high number of CEF cases that should be prosecuted. A small fraction of CEF-related investigations leads to prosecutions, which indicate challenges with the prioritisation approach. Evidential challenges with proving *mens rea* for ML offences has undermined the ability to successfully prosecute cases. While Singapore has put in place measures to address these challenges, they are recent and it is too early to assess their impact on effectiveness. Prosecutions are in line with risks to some extent. Overall, while Singapore pursues different types of ML, most cases involve low-level and low-value MM cases. Singapore insufficiently pursues legal persons and professional intermediaries and does not sufficiently prioritise major ML prosecutions, which is not in line with risks. Further, Singapore prioritises prosecutions that are more likely to result in guilty pleas rather than those posing the greatest risk.

7.2.1. Prosecutions

467. The AGC, which is responsible for prosecutions, is led by the Attorney-General, who is also the Public Prosecutor and the legal advisor to the Government. AGC's specialised prosecutors ('Deputy Public Prosecutors') are responsible for prosecuting ML investigations. Since the 2016 MER, there has been one additional head count for prosecutors compared to a four-fold rise in ML investigations. The AGC uses discretion when deciding which case to take on for prosecution. This includes considerations about sufficiency and credibility of the evidence, and whether the prosecution would be in the 'public interest', a term which is loosely defined and refers to common welfare and benefits of the society as a whole. Where prosecutions are discontinued, Singapore pursues alternative measures to some extent (see 7.4).

[32] *See Methodology, IO.7, Note to Assessors 2 and related footnotes*

Table 7.3. Prosecutions and Convictions for ML (natural persons)

# of people	2020	2021	2022	2023	2024	Total (%)
No of ML Investigations	1 089	2 289	2 322	2 854	2 635	11 189
# natural persons prosecuted	87	152	119	123	201	682
# natural persons convicted (% of prosecutions)	53 (61)	101 (66)	95 (80)	105 (85)	125 (62)	479 (70)

Note: investigations prosecuted in one year may be convicted in the next.

468. Since 2020, Singapore prosecuted 682 natural persons (Table 7.3). Only a small fraction of ML investigations progress to prosecutions. While this may reflect challenges in LEA prioritisation, two other main factors explain the low conversion of investigations into prosecutions:

a) Under S17 CPC, LEAs must open an investigation whenever there is '*reason to suspect*' an arrestable offence, even if the case involves low-level criminality or fails to meet prosecutorial thresholds. Singapore opens standalone ML investigations for all CEF cases, typically involving money mules in Singapore acting for foreign syndicates, provide access to their bank accounts or help conceal and move illicit funds. Singapore has maintained that it invariably opens standalone ML investigations in response to victim complaints as only the ML networks and mules exist in Singapore while the ultimate criminal perpetrators (i.e. the subject of any predicate investigation) are overwhelmingly based overseas. In reality, these cases often concern small sums already moved abroad, making them hard to prosecute and inflating investigation numbers. Singapore indicates these cases (when pursued) may generate some investigative leads to open new cases, but there is no evidence this strategy helps systematically disrupt overseas criminal syndicates.
b) Many ML cases have a foreign nexus, making evidence collection on overseas suspects difficult. Proving *mens rea* for local MMs, professional intermediaries and nominee directors is also challenging. These challenges are not unique to Singapore, since highly effective AML/CFT systems routinely prosecute such complex cases. Although Singapore recognises the need for international co-operation, formal channels are rarely pursued and authorities often rely on informal co-operation instead (see IO.2).

469. Singapore has recognised some of the abovementioned systematic weaknesses and introduced major legislative amendments to better pursue these investigations (summarised below). While these reforms are promising and appear to mitigate many of the challenges, they are recent and their full impact cannot yet be assessed. Specifically, Singapore:

a) Added section S55A to the CDSA in February 2024 which contains two offences targeting MM. Singapore has branded these offences as ML offences and pursues them as such.
    - S55A(1) (the Money Mule Offence), under which investigations have been prosecuted, criminalises certain conduct that is typical of ML activity, such as entering into or facilitating an arrangement with another person to allow the use of their bank account. While this offence contains many of the elements of an ML offence, and ultimately targets ML activity, it is not a ML offence. The Money Mule Offence does not require the prosecution to prove that the accused had the knowledge that the property represents the proceeds of crime or that they intended to acquire, conceal or use criminal property. Rather, it targets arrangements facilitated by the accused that enable the transfer of funds, but the accused person does not have to have any knowledge that the funds were criminal property. However, the accused person has a defence to the offence in S55A(3) if he can prove that he did not know and had no reasonable ground to believe that the property represents proceeds of crime. Singapore has used this offence extensively since its enactment (and is detailed as an alternative measure in 3.2.4).

- S55A(2), which is a ML offence and is designed to ease the burden required to prove that an individual is an accessory to an ML offence. Very limited prosecutions have been mounted under S55(A)(2) to date with no resolved cases.

b) Added sections S50(1A), 51(1A), 53(3A) and 54(3A) of the CDSA in February 2024 to pursue investigations where there is insufficient evidence that the person knew or had reasonable grounds to believe that the person he is assisting has engaged in criminal conduct. It is sufficient for the prosecution to prove that the person had acted rashly or negligently.

c) Amended S56 of the CDSA in November 2024 to deal with the evidentiary challenge of proving predicate offences committed abroad. This provision in effect introduces a rebuttable presumption as it removes the requirement for the prosecution to prove this element of the offence but allows an accused person to prove that the property in question are not proceeds of a foreign drug dealing or serious offence. This amendment was operationalised in November 2024 and had not been used to mount prosecution by the time of onsite.

470. As with ML investigations, prosecutions and convictions are in line with risks to some extent, and only when it comes to fraud, rather than for other higher risk offences (Table 7.4). Following prosecutions related to CEF, Singapore's authorities mainly pursue prosecutions relating to ML in corruption investigations. ML prosecutions related to other higher risk offences and notable ML threats such as organised crime, tax crime and drugs are not prosecuted as regularly in line with risk.

Table 7.4. Prosecutions per predicate offence

Agency	Domestic ML Prosecution (as a % of total for the predicate offence)	Foreign ML Prosecutions (as a % of total for the predicate offence)	Total (% of total)
Fraud (CEF)	326 (92)	29 (8)	355 (52)
Fraud (non-CEF)	50 (75)	17 (25)	67 (10)
Corruption (incl. breach of trust)	60(98)	0 (0)	60 (9)
Unlicensed Money Lending	24 (100)	0 (0)	24 (3)
Cybercrime	19 (100)	0 (0)	19 (3)
Drugs	41 (100)	0 (0)	41 (6)
Organised Crime	10 (50)	10 (50)	20 (3)
Tax Crimes	9 (64)	5 (36)	14 (2)
Illicit Wildlife Trade	0 (0)	1 (100)	1 (0)
Others	87 (99)	1 (1)	88 (13)
Total	626 (91)	63 (8)	689 (100)

Note: Each prosecution may involve more than one predicate offence, and totals may therefore differ from above tables.

471. Singapore prosecutes and achieves convictions for different types of ML activity, including third party and standalone investigations (for example against transnational syndicates perpetrating CEF) (Table 7.5). Yet, most of the third-party laundering and standalone ML investigations arising from domestic predicate offences represent prosecutions involving MM rather than sophisticated ML schemes involving foreign perpetrators, syndicates, intermediaries and nominee directors.

Table 7.5. Types of ML prosecuted and convicted (natural persons)

	2020	2021	2022	2023	2024	Total (%)
Prosecutions (Total for self and/or third-party laundering)	87	152	119	123	201	682
Self-laundering	23 (26)	35 (23)	25 (21)	36 (29)	60 (30)	179 (26)
Third-Party laundering	64 (74)	110 (72)	90 (76)	85 (69)	138 (69)	487 (72)
Both (Self-laundering and Third-Party Laundering)	0 (0)	7 (5)	4 (3)	2 (2)	3 (1)	16 (2)
Standalone investigations (1)	44	60	49	72	68	293

	2020	2021	2022	2023	2024	Total (%)
Convictions (Total for self and/or third-party laundering)	53	101	95	105	125	479
Self-laundering	12 (23)	23 (23)	26 (27)	22 (21)	35(28)	118 (25)
Third-Party laundering	41 (77)	76 (75)	68 (72)	80 (76)	85 (68)	350 (73)
Self-laundering and Third-Party Laundering	0	2 (2)	1(1)	3 (3)	5(4)	11(2)
Standalone investigations	33	41	36	63	63	236

Note: (1) As per the FATF Methodology, Standalone ML is a not a type of laundering but rather refers to the prosecution of ML offences independently, without the need to prosecute the predicate offence. These include for example CEF investigations or investigations involving foreign predicate offences.

472. Only 25 Singapore-based nominee directors were prosecuted during the reporting period, which is not in line with its risks and context. As noted in IO.5, Singapore requires legal persons to have at least one local director as a risk mitigation measure. However, authorities face challenges in proving that they are the directing mind behind the ML activity or have the requisite *mens rea* to pursue ML prosecutions. In these cases, Singapore pursues some alternative measures against local directors (see 7.4). These rare prosecutions of nominee directors mitigate the effectiveness of the reason for the requirement to have a local director that is responsible for the legal person. Singapore has pursued legal persons for prosecution (only eight prosecutions and two convictions) despite typologies showing the use of legal persons to launder funds in Singapore. Even though legal persons may be used as pass-throughs with no assets to recover, making prosecutions less worthwhile, they still represent a point of connection with Singapore that should be pursued.

473. Similarly, the AGC prosecuted only 12 professional intermediaries (such as lawyers and TCSPs) who are the key access points to Singapore's economy for foreign criminals. As noted, Singapore is facing an issue where the controlling minds of their highest risk predicate offence are, generally, located outside of the country. Singapore is taking measures to hold more of those contributing to laundering the proceeds of fraud within its borders to account, such as targeting MM. Singapore could do more to pursue local directors and professional intermediaries within its borders when party or accessory to laundering proceeds as they are generally within Singapore's borders.

Table 7.6. Prosecutions and Convictions for Natural and Legal Persons

	2020	2021	2022	2023	2024	Total (%)
Prosecutions	88	152	121	127	203	691
Natural Persons	87	152	119	123	201	682 (99)
Legal Persons	1	0	2	4	2	9 (1)
Convictions	53	101	95	106	126	481
Natural Persons	53	101	95	105	125	479 (99)
Legal Persons	0	0	0	1	1	2 (1)

7.2.2. Convictions

474. Singapore has shown a capacity to prosecute and secure convictions into some of the complex ML activities, including in relation to threats such as organised crime (*3B$ case*), corruption and tax crimes, some involving a transnational nexus. AGC had also secured convictions involving virtual assets as shown in Box 7.2. This is supported by an increasing number of standalone ML prosecutions, for which authorities are generally able to secure a good conviction rate. Singapore secured only two convictions for legal persons, which is not in line with risks.

475. Singapore has a good prosecution to conviction rate (82%), largely driven by guilty pleas, including those made through plea bargaining. As previously noted, AGC pursues prosecutions only when

it believes the evidentiary threshold can be met and when it is in the public interest. This explains the very low rate of discharged investigations with acquittal (2%) and discharged investigations without acquittal (4%). Across all criminal offences, 92% of convictions result from guilty pleas, including plea bargaining, rather than a trial, indicating Singapore's dependence on this approach.

476. While data on guilty pleas for ML prosecutions is unknown, authorities indicated that only a minority involve plea deals[33]. Singapore explained that offenders generally elect to plead guilty earlier in the criminal process due to the quality of evidence and to obtain lighter sentences, and plea deals may be offered in a minority of cases where evidence is weaker. Nonetheless, AGC frequently secures guilty pleas or plea deals, as in the *3B$ case*.

477. In conclusion, Singapore's case-prioritisation model has had limited impact, with few ML investigations progressing to prosecution. Most ML prosecutions still involve low-level money mule cases, with insufficient focus on complex cross-border cases, legal persons and professional intermediaries. Prosecutors prioritise cases more likely to result in guilty pleas rather than those posing the highest ML risks, which undermines the deterrence effect.

Box 7.2. ML prosecutions and convictions

Conviction of a transnational syndicate

This was an intelligence-led investigation into a transnational CEF syndicate laundering proceeds through a ML network in Singapore, led by Person A. Introduced to the criminal enterprise by Person B, Person A procured over 50 bank accounts, mainly from foreigners via Telegram and online ads, and received more than SGD 800 000 (USD 592 000) to convert into USDT. Person A recruited crypto traders and ATM runners to withdraw over SGD 640 000 (USD 474 000) using ATM cards he supplied. He also gave Person B internet banking access to a Singapore bank account which was then used to receive and dissipate another SGD 570 000 (USD 422 000). In February 2024, Person A was convicted and sentenced to 4.5 years' imprisonment for ML offences and other offences under Computer Misuse Act (CMA). Two crypto traders were also convicted and sentenced to 13 and 20 months respectively. Despite the large number of bank accounts misused, only 3 bank account holders were found to remain in Singapore and are currently under investigation. Additional investigations on the fund flow are still underway to uncover further links to criminal syndicates.

Charges against a legal entity

In July 2023, a director of a Singapore-registered company was charged in Court for ML offences, among other offences, for providing his SingPass credentials to unknown third parties for incorporating a company. The director also conspired to deceive a local bank into opening a corporate bank account for the company, by falsely declaring himself as the ultimate BO of the bank account. Investigations revealed that two overseas victims were defrauded into transferring approximately USD 300 000 (SGD 405 500) to the company's bank account in 2021. As a separate legal entity, the company was charged with ML offences as well for possessing property reasonably suspected to be benefits of criminal conduct under the CDSA. Court proceedings against the company and its director are currently ongoing.

[33] In Singapore, "plea deals" relates to situations involving negotiations between the defence and the prosecution, with the latter preferring lesser or lower charges or seeking a lower sentence than it would otherwise have.

7.3. Effectiveness, proportionality and dissuasiveness of sanctions

478. Despite an appropriate legislative framework to sanction ML (see R.3), ML sanctions for natural persons are proportionate but not effective or dissuasive. There have been few convictions for legal persons, due to which it is not possible to assess their effectiveness.

7.3.1. Sanctions for natural persons

479. When considering the overall quantum of penalties meted out, ML sanctions are proportionate but not effective or dissuasive. Under the law (see R.3), ML committed by natural persons attracts a maximum 10 years and/or a fine of SGD 500 000 (USD 370 000), which is proportionate to other comparable offences. However, a majority of the actual penalties for ML convictions, including prison sentences, are on the lower end of the spectrum.

480. These low penalties are a result of Singapore's sentencing guidelines and framework (Huang Ying-Chun). The Sentencing Advisory Panel has issued guidance for ML offences under Sections 51 and 55 of the CDSA, requiring courts to assess investigations based on harm and culpability. One of the factors limiting the deterrent effect of penalising ML is the recommendation to impose monetary fines for lower harm and culpability offences rather than imprisonment (which is reserved for offences involving higher levels of harm and culpability). However, there are still situations in which offenders involved in less serious, but still harmful laundering schemes, may face only financial penalties.

481. In response to the prevalence of CEF, Singapore introduced tailored sentencing guidelines in 2024 for scam-related ML convictions. These guidelines propose a baseline sentence of 18 months' imprisonment, with adjustments for aggravating factors (e.g. large sums, vulnerable victims, multiple accounts, abuse of position) and mitigating factors (e.g. guilty pleas).

482. Singapore applies the 'one transaction' and 'totality' principles to penalties. The one transaction principle means that sentences for offences committed in the course of a single transaction should generally run concurrently, which is relevant when predicate offences generate proceeds, and they are laundered immediately or shortly thereafter. In turn, the totality principle is applied at the end of the sentencing process to ensure that the total sentence is what Singapore's courts consider to be just and proportionate with the overall seriousness of the offender's criminal behaviour when all the offences are considered together (i.e., a predicate offence and ML offence, or multiple ML offences). Singapore therefore metes out concurrent and consecutive sentences for different offences. While Singapore believes that these are common law principles applied by the courts to ensure deterrent yet proportional sentences, in effect these principles, taken together, lower penalties. When ML sentences run concurrently with predicate offences, the proportionality and deterrent effect of ML sanctions is reduced, as ML is a distinct offence. It is seen from a number of case studies provided that the penalty for the ML offence is lower than the predicate offence, meaning that, in the cases where there is a concurrent sentence, no extra time is served in addition to the sentence for the predicate crime. While Singapore provided examples where the ML and predicate offences can run consecutively, 19% of convictions had sentences that were applied concurrently where those found guilty do not spend extra time incarcerated beyond the term of their imprisonment for the predicate offence.

483. The high incidence of guilty pleas (including plea deals) (92%, as noted above) leads to sanctions that are significantly lower than in convictions after trial which undermines the dissuasiveness and effectiveness of sanctions. This is illustrated with the 3B$ case, where 10 of the 27 accused were found guilty mostly through plea deals. Singapore sought plea deals because they felt they had evidentiary difficulties owing to the fact most activities were conducted overseas and evidence was not available from foreign jurisdictions. Despite the very significant proceeds involved in the 3B$ case, one of the largest ML investigations in the entire world, due to evidentiary difficulties, the 10 guilty persons were charged with

lower ML charges and sentenced to 13 to 17 months prison term each. 15 of the other accused who absconded overseas agreed for their assets being confiscated without conviction with the INTERPOL notice against them withdrawn and they being barred from entering Singapore (Singapore was unable to prosecute them for ML charged due to similar evidential limitations and since they were out of jurisdiction). While the sanctions were not dissuasive, as discussed in IO.8, this case is a success from an asset recovery standpoint.

484. On average, natural persons receive a 13 months' imprisonment sentence (in line with other comparable offences in Singapore, such as corruption, cheating or forgery), and 72% of individuals convicted of ML received a prison sentence of less than a year (Table 7.7). The significant number of prison sentences on the lower end of the spectrum (some as short as one week) arises out of the large number of prosecutions mounted against low-level MM, where the sentences imposed remain commensurate with their conduct and roles in the ML activities. Prison sentences of more than four years were used only in 5% of convictions in the review period. Overall, Singapore's approach results in very limited application of dissuasive sentences for even very serious and aggravated ML offences, which is not effective in penalising ML.

Table 7.7. ML Sanctions

# of convictions	2020	2021	2022	2023	2024	Total (%)
Prison Sentences						
= 48 months	1	7	3	5	7	23 (5)
36 to < 48 months	1	5	0	4	7	17 (4)
24 to < 36 months	5	7	6	7	4	29 (7)
12 to < 24 months	7	10	8	13	11	49 (12)
< 12 months	36	55	63	62	86	302 (72)
Total	**50**	**84**	**80**	**91**	**115**	**420 (100)**
Fines						
Persons fined	2	3*	2	0	2*	9
Total amount fined	9 000	63 590	7 000	0	5 000	84 590
Average fine	4 500	21 197	3 500	0	2 500	9 399

Note: Some individuals – not accounted for in this table - received probationary sentences and/or fines, mainly due to their ages. (*) Includes accused persons who were sentenced to both fines and imprisonment.

7.3.2. Sanctions for legal persons

485. Due to the few convictions for legal persons, it is not possible to assess their full effectiveness. The four sanctions secured against legal persons, while proportionate, do not help the AT make any conclusions on their effectiveness or whether they are in line with risks. In these four investigations, fines ranged from SGD 10 000 (USD 7 400) to SGD 500 000 (USD 370 000), the maximum being SGD 1 million (USD 740 000) or twice the value of the property involved/benefit of criminal conduct, whichever is highest. In two of the investigations, the courts did not provide a reasoning in passing a sentence. The other two investigations reflect situations in which the courts considered culpability to be higher. In one the court applied an SGD 10 000 fine (USD 7 400) against a shell company, which did not have any assets. In the remaining case, the court found the harm to be moderate and culpability high and imposed an aggregate fine for ML of SGD 500 000 (USD 370 000).

7.4. Use of alternative measures

486. To some extent, Singapore employs a combination of criminal, administrative and regulatory approaches as alternative measures when it is not possible to secure ML convictions. These ensure that offenders are still held accountable and subject to legal consequences in the absence of a formal ML charge. However, there is a low use of alternative measures when compared to the number of cases where a conviction cannot be secured. Moreover, evidence from recent years indicates that Singapore is becoming increasingly reliant on alternative measures, particularly the Money Mule Offence, rather than the potential pursuit of ML convictions.

487. AGC prosecutes offenders under a range of offences when it is not feasible to obtain an ML conviction (Table 7.8). This includes charging individuals under alternative offences including but not limited to: Penal Code, Computer Misuse Act (CMA), breach of director's duties under the Companies Act (CA) for nominee directors, Payment Services Act (PSA). Asset confiscation and forfeiture as well as administrative and regulatory actions are also considered. Singapore maintains limited statistics on all alternative measures used, but it does attempt to pursue robust and pragmatic enforcement where ML evidence thresholds are difficult to meet. Based on the limited data available (Table 7.8) and qualitative information provided, Singapore applies these alternative measures to some extent when considering the number of ML convictions.

Table 7.8. Alternative measures

# Number of persons convicted	2020	2021	2022	2023	2024	Total
S55A(1), CDSA [(1)]	Operationalized in 2024				15	15
S157, Companies Act	7	10	15	16	16	64
S5, PSA	4	14	20	15	28	81
Total	11	24	35	31	59	160

Note: [(1)] S55A was operationalised in February 2024. Statistics exclude ongoing prosecutions.

488. As described above, the codification of the Money Mule Offence constitutes a significant, albeit recent, alternative measure that complements Singapore's core ML offences and strengthens LEA's capacity to pursue ML activity. While Singapore is credited for identifying mechanisms to pursue its high-risk predicates, this amendment is recent. So far, the use of the Money Mule Offence has proven useful in a limited number of prosecutions. Between its operationalisation in February 2024 and May 2025, Singapore's authorities have mounted 286 prosecutions demonstrating its high usage.

489. Singapore is praised for identifying mechanisms to address ML activity from CEF (its highest ML risk area) when ML convictions are not possible. Singapore's authorities have a clearly stated goal of ML prosecution and asset recovery at the commencement of a ML investigation, but Singapore considers the pursuit of the Money Mule Offence as an ML offence. Given the low rate of conversion from ML investigations to prosecutions, there is a risk that investigators and prosecutors may be inclined to systematically prioritise investigations which can be prosecuted under the Money Mule Offence, rather than for ML. It is too early to assess whether the slight downturn in ML investigations during the time period of the enactment of this offence is as a result of Singapore relying on this alternative measure.

490. Other alternative measures taken by Singapore include administrative and regulatory actions. For instance, ACRA helps prevent the misuse of legal entities for ML by screening new companies, striking off illicit shell companies, and taking regulatory action when prosecution is not possible, via proactive sharing of information by CAD. ACRA can also make debarment orders against directors if there is information to suggest that any company under their directorship is in default of relevant regulatory requirements. It can

also sanction CSPs and Registered Qualified Individuals (RQIs) for serious AML/CFT breaches. Similarly, MAS has broad enforcement powers to address breaches of AML/CFT obligations. MAS can require FIs to remediate areas of weaknesses, impose financial penalties, revoke or restrict licenses, and issue reprimands. MAS can also impose fines against finance professionals, issue prohibition orders to bar them from taking up specified roles, activities and functions in the financial sector, and issuing reprimands to these individuals.

491. In conclusion, Singapore has applied alternate measures with success and is credited for this approach where justified. With the creation of the Money Mule Offence, Singapore has positioned itself for an approach more heavily relying on alternative measures in the future. However, as Singapore considers this offence to be an ML offence, it is systematically pursuing this offence as a policy objective where it may be more appropriate to pursue ML convictions instead. Considering the volume of ML investigations that are not pursued by the AGC (i.e., multi-thousands), the application of these alternative measures remains limited at this time.

8 Asset recovery

The relevant Immediate Outcomes considered and assessed in this chapter is IO.8. The Recommendations relevant for the assessment of effectiveness under this chapter are R. 1, 4, 32 and elements of R. 15, 30, 31, 37, 38 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Asset recovery is a political priority, supported by the National Asset Recovery Strategy (NARS), SOPs, and WoG approach. Singapore has a strong operational and legal framework for asset recovery, including to manage and return assets, which is regularly reviewed. Effective agency structures and co-operation mechanisms enable the use of government data, public-private partnerships (e.g. RTIG, AC3N, etc.), and international co-operation to facilitate broad and effective information exchange to trace assets.

b) LEAs have a strong legislative framework and operational powers through which they proactively and routinely identify and trace criminal property. Yet some deficiencies identified in IO.7 and IO.5 (accuracy of BO information) affect the identification of assets, including a heavy focus on money mule-related fraud cases, difficulties in mounting ML prosecutions for foreign predicate offences, and insufficient targeting of complex structures and professional intermediaries. In depth investigative techniques to uncovered unexplained wealth, such as concealed income analysis are not utilised enough.

c) LEAs actively freeze and seize criminal property to prevent the dissipation of assets, including through expeditious measures. Authorities use provisional measures with good results, seizing close to SGD 6.3 billion (USD 4.7 billion) over the reporting period, including in high-value and complex cases (e.g. the *3B$ case*). While a third of ML investigations lead to seizures, the bulk of seizures (95%) are driven by lower-value non-ML cases and align with risks to a reasonable extent.

d) Singapore achieves a positive seizure to confiscation rate (61 %) and has obtained a significant amount of confiscation: SGD 3.9 billion (USD 2.9 billion) between 2020 and 2024. LEAs demonstrated they can confiscate a wide variety of assets across complex cases using a combination of CBC, NCB and tax recoveries in criminal cases. Confiscations align with risks to a reasonable extent, although more granular statistics in this area are missing.

e) While authorities proactively seek assistance from foreign counterparts through informal channels, Singapore is less successful in its use of formal international co-operation, considering the volume of predicate and ML investigations. Singapore does not seek the enforcement of its

own foreign confiscation orders abroad. This may depress the chances of final confiscation or repatriation of assets to Singapore.

f) While Singapore has a solid legal framework for cross border cash reporting regime (CBCRR), there are issues with its enforcement, particularly the detection of violations. Most individuals who fail to file or file a false declaration are first-time offenders, and the authorities have only been able to link one offender to broader criminality out of 439 cases, showing an issue with follow-up investigations. Sanctions for cash smuggling violations are proportionate and dissuasive in rare cases when offenders are linked to ML, TF or predicate offences, but when links are not established, sanctions are neither proportionate nor dissuasive.

Recommended Actions (RAs)

a) Improve the tracing of assets held through complex ownership structures and trusts and other high-risk areas in order to improve seizure and confiscation results, including through greater use of CIA.

b) Enhance international co-operation in cross-border asset recovery cases and make better use of MLA requests to recover assets abroad, including through the enforcement of Singapore's confiscation orders abroad.

c) Enhance the effectiveness of the investigative process used to follow-up on instances of non and false CBCRR declarations, so as to investigate potential links between cash smuggling and other criminality and review the approach to sanctioning first time offenders in line with Singapore's risk and context.

Overall Conclusions on IO.8

Singapore makes asset recovery a high-level priority, and this priority is operationalised in NARS, SOPs, WoG approaches and supported by regular improvements to the asset recovery framework. LEAs have a strong legislative framework and operational powers through which they proactively and routinely identify and trace criminal property. There are practical limitations which can limit the scope and nature of identified assets that can be recovered, including a focus on small money mule offences, difficulties in mounting ML prosecutions for foreign predicate offences, insufficient targeting of complex structures and professional intermediaries.

LEAs make active use of provisional measures to freeze and seize assets where required resulting in SGD 6.3 billion or USD 4.7 billion frozen/seized). These results are largely driven by a small number of high-value, complex cases. LEAs also follow through and confiscate 61% of seizures, approximately SGD 3.9 billion (USD 2.9 billion), a good amount, across a range of asset types and through a combination of CBC, NCBC and criminal tax recovery measures. Authorities make active use of informal co-operation but there is scope to improve formal international co-operation for asset recovery. Seizures and confiscations are aligned with risks to a reasonable extent with room for improvement in respect of corruption, TBML and fraud.

Singapore has a solid legal CBCRR framework, but there are weaknesses in the detection and identification of breaches. A majority of travellers not or falsely filing CBCRRs are first-time offenders who Singapore cannot link to criminality. This indicates there are issues with CBCRR follow-up and

intelligence value, limiting confiscation and resulting in sanctions that are neither proportionate nor dissuasive.

Singapore is rated as having a Substantial level of effectiveness for IO.8.

Immediate Outcome 8

8.1. Prioritisation of asset recovery as a policy objective and using effective agency structures and co-operation frameworks

492. Singapore places high priority on asset recovery, supported by regular reviews of its regime. Strong agency structures and co-operation frameworks enable the use of government data, public-private partnerships, and international co-operation to facilitate broad and effective information exchange. Competent authorities have sufficient structures, resources, and specialised expertise for pursuing asset recovery.

8.1.1. Prioritising asset recovery as a policy objective

493. Singapore has demonstrated a high-level political commitment to asset recovery, which is integrated into national policy documents, such as the National Asset Recovery Strategy (NARS) and the Law Enforcement Strategy to Combat Money Laundering. NARS, which has received high-level political support, focuses on four operational pillars: detect, deprive, deliver and deter. Aside from confiscation, it also highlights the importance of tax recovery measures and voluntary restitution. Singapore has operationalised these frameworks into strategic objectives which prioritise the pursuit of criminal assets (including virtual assets) moved out of Singapore and the enforcement of a cross-border cash reporting regime (CBCRR). This is reflected in a Whole of Government (WoG) approach to asset recovery and agency-specific SOPs, ensuring that all relevant agencies prioritise and operationalise asset recovery in their work plans.

494. The prioritisation of asset recovery is also perceptible from various innovative measures Singapore has taken, such as Project POET (see IO.6) and PPP initiatives, particularly the co-location of private sector personnel at the ASC, and the ACIP CSIs (see Box 6.3). These initiatives allow LEAs to rapidly freeze and intercept illicit transfers while also leveraging on private sector's resources. STRO's upgrade to Wings X in 2022 has also led to more timely asset tracing through better data-integration. Finally, IRAS is making increasing use of tax clawbacks to recover assets through tax assessments, creating additional pathways for asset recovery when dealing with tax crimes.

495. Additionally, Singapore utilises bilateral agreements and multilateral channels to support its asset recovery efforts. For example, Singapore is an active member of ARIN-AP (it joined its Steering Committee in 2024), INTERPOL's regional body (AseanPol) and dedicated taskforces (e.g. INTERPOL Global Rapid Intervention of Payments, I-GRIP) (see IO.2)

8.1.2. Periodic review of asset recovery regime

496. Singapore leverages on operational experience to regularly review its asset recovery regime. The GST Amendment Act in 2020 enhances IRAS' ability to swiftly identify criminal property and seize instrumentalities of crime to prevent asset dissipation. The 2024 Anti-Money Laundering and Other Matters Act amendments increase cross-government data sharing, enabling STRO to develop richer financial

intelligence and improve asset tracing. These amendments also allow courts to order the pre-confiscation sale of seized or restrained properties under consent from interested parties, or in situations of likely depreciation of property value or high maintenance costs. In 2025, Singapore also took part as a pilot country in INTERPOL's 'Silver Notice' programme, which seeks to facilitate international co-operation for asset tracing and recovery. Considering the cross-border nature of most threats, the review of systemic obstacles in cross-border asset recovery has helped Singapore in identifying weaknesses and take corrective actions on a timely basis. The prioritisation of returning confiscated property to victims is reinforced by enhancements to the victim compensation regime under section 359 of the CPC implemented in 2024, allowing victim participation in compensation proceedings and requiring judicial explanation when compensation is not granted.

8.1.3. Effective agency structures and co-operation frameworks

497. Strong institutional frameworks for co-operation in asset recovery are in place, such as RTIG, ISTRA/AC3N, and ACIP (Box 8.1). Singapore also maintains a well-resourced and trained operational capacity for pursuing asset recovery at the agency level. Dedicated units have clear organisational responsibility and tools for ML investigations and asset recovery. This includes FIG within the CAD, whose staff count has more than doubled since the 2016 MER. Within FIG is the Asset Confiscation Branch, which focuses on unexplained wealth confiscation proceedings and undertakes Concealed Income Analysis (CIA, discussed below). The ASC is another strong feature to help Singapore address CEF. Other LEAs (like CNB and CPIB) also have dedicated and trained teams which target proceeds of crime for seizure and confiscation. Agencies send officers on secondment to other relevant agencies to foster greater operational level co-operation. Beyond these dedicated asset recovery teams, all Investigation Officers across LEAs are involved in asset recovery in the entire life cycle of investigations, guided by the WoG Guidelines on Asset Management and WoG Guidelines on Management of Cryptocurrencies.

498. IRAS and other competent authorities have mechanisms to co-operate in asset recovery in tax predicate offences. CAD has an SOP with IRAS to detect and investigate ML from tax offences, and a satellite office in IRAS with a seconded CAD officer to enhance the detection of tax-related ML activity for parallel ML investigations. STRO has also been cooperating with IRAS since December 2023 on cases involving foreign predicate ML cases with a suspected tax angle. Further, IRAS can refer to and receive information from relevant LEAs, including CAD, concerning suspected commission of serious non-tax offences, in accordance with the "Guidelines for LEAs and STRO to request for information from IRAS".

Box 8.1. Use of WoG approaches and PPPs for Asset Recovery

In 2020, CAD uncovered a large network of over 3 000 Singapore incorporated shell companies – created by CSPs – linked to Business Email Compromise scams. A joint probe by CAD, MAS and relevant ACIP banks (within the framework of RTIG), led Singapore to blocking SGD 21 million (USD 15.5 million).

8.2. Identifying and tracing criminal property and property of corresponding value

499. LEAs take a proactive approach at identifying and tracing criminal property, including virtual assets. Singapore routinely conducts financial investigations without obstacles related to resourcing or adequacy of legal or investigative tools or techniques. NARS instructs LEAs to pursue asset recovery in all cases,

irrespective of the amounts involved, although some prioritisation happens based on the nature of the case (e.g. complexity and assets involved). However, several practical constraints limit Singapore's effectiveness in identifying and tracing a broad scope of property.

500. LEAs benefit from a strong legislative framework and operational powers to identify and trace assets. The CPC and CDSA give LEAs broad powers to compel the production of financial information from individuals, entities, FIs, VASPs, and DNFBPs. LEAs are guided by SOPs which place priority on the identification of assets for seizure and confiscation. Singapore also leverages several tools to trace criminal assets, including initiatives like Project POET, the ACIP and COSMIC frameworks. Authorities have also shown an ability to exploit a wide array of information, cross-government data integration (i.e. NAVIGATE) and international co-operation for asset recovery purposes, using both formal and informal channels to prevent asset dissipation.

501. Case studies and discussions with Singaporean authorities show that LEAs routinely identify and trace assets without any major issues. However, as identified in IO.7, there are challenges in ML investigations which affect the identification of criminal property and may result in some assets going unidentified (compounded to an extent by the limited accuracy of BO information, see IO.5):

a) IO.7 shows that over 80% of Singapore's ML investigations involve low-level money mule cases related to CEF. LEAs are understandably targeting fraud, an important threat area. However, by nature, these money mule-related fraud cases typically involve minimal asset values and small-value transactions. While Singapore has seized SGD 590 million (USD 452 million) linked to CEF (which only aligns with risk to some extent, as detailed below), this operational focus limits the pursuit of higher-value and more complex ML networks, and the recovery of more substantial criminal assets connected to transnational actors.
b) For much of the reporting period, LEAs experienced challenges in mounting ML prosecutions for foreign predicate offences and proving *mens rea*, a key risk factor for Singapore. By extension, this also makes it difficult to link assets to such criminal conduct and prevent their dissipation, especially when funds are quickly moved or passed through Singapore's financial system. Still, while this poses challenges in identifying assets, there are case studies (*e.g. 3B$* case) showing Singapore can identify significant assets linked to foreign predicate offences.
c) Considering Singapore's status as a wealth management destination, successful attempts to trace criminal assets through complex structures and trusts could not be adequately demonstrated. In the review period, there has been only one case of seizure of assets held in trusts (SGD 256 million or USD 196 million in assets), which was initiated on the basis of STRO's analysis.
d) Limited targeting of ML involving professional intermediaries and local directors weakens asset tracing efforts (as was observed also in respect of one high-profile case). These actors may receive a portion of criminal proceeds in exchange for facilitating laundering or providing access to payment accounts. By failing to focus on identifying these illicit gains and the proceeds laundered, authorities miss opportunities to pursue recovery of assets laundered systematically (including those directly linked to the predicate offences) and across several cases and different crime types.

502. Singapore's main ML threat is fraud and, as detailed in IO.7, many of these investigations end up being categorised as standalone ML. In these cases, assets are identified and investigated as a matter of course. Conversely, there is a lack of comprehensive data quantifying the number of predicate crime cases where competent authorities pursue the recovery of criminal assets. Thus, it is challenging to assess how frequently and how well LEAs routinely identify and investigate assets for potential confiscation stemming from non-ML cases. This is occurring in some instances, as shown by Table 8.1 below.

503. Supported by SOPs, the focus of LEAs is primarily to identify and seize in the investigative stage. Beyond typical investigative techniques, Singapore also uses concealed income analysis (CIA) to examine the totality of an accused's hidden or undisclosed assets, liabilities and expenses. This is done with a view

to finding wealth that is disproportionate to known legitimate income which can be confiscated. This analysis allows LEAs to come to a better understanding of the quantum of criminal proceeds of the individual(s) under investigation. In these instances, courts can order the seizure and confiscation against the defendant, which extends to property that is not shown to be directly linked to an offence and is disproportionate to the defendant's known sources of income when the defendant cannot explain a legitimate source of wealth to the satisfaction of the Court. While Singapore has shown some very limited success using CIA by seizing SGD 20.9 million (USD 16 million) through 173 analyses, this intensive analysis is used infrequently when compared to the 11 000 ML investigations as well as the unknown but much higher number of predicate investigations. There are missed opportunities to identify additional criminal assets.

504. In conclusion, LEAs proactively identify and trace criminal property drawing on a strong legislative framework and operational powers, but few ML investigations uncover significant criminal property. Challenges for the identification of assets include a higher focus on money mule-related fraud over complex ML networks, proving *mens rea*, pursuing assets tied to foreign predicate offences, and the pursuit of assets through complex structures and limited targeting of professional intermediaries.

Box 8.2. Identification and tracing of assets

3B$ case[34]

SPF conducted an 18-month investigation tracing the networks and holdings of the suspects and their associates, their criminal activities and their assets. A joint workgroup comprising SPF, STRO and AGC was formed. SPF worked with STRO to identify instances of foreign nationals submitting forged documents to banks to substantiate their importation of funds into Singapore. Pre-raid preparations included collaborations with banks via MAS and digital forensics, including in-house virtual asset tracing and support from a private sector expert.

Authorities identified assets linked to 27 persons of interest. SPF arrested 10 foreign nationals and issued prohibition orders on assets tied to 17 others who had left Singapore before the investigation began. Over SGD 3 billion (USD 2.2 billion) in assets were seized or issued with prohibition orders, including bank funds (over SGD 1.45 billion/USD 1 billion), cash (over SGD 76 million/USD 56.2 million), cryptocurrencies (over SGD 38 million/USD 28.1 million), real estate, vehicles, luxury bags, luxury watches, jewellery, alcohol, and other high-value collectibles.

Use of CIA

MOM investigated Person A, a town council conservancy manager suspected of collecting kickbacks from foreign workers between 2016 and 2020. Upon further investigations, MOM seized SGD 326 305 (USD 241 465) in cash from Person A's home and alerted CAD, prompting concurrent financial investigations and a CIA. These revealed that Person A had accumulated about SGD 1.4 million (USD 1 million) in wealth despite declaring only SGD 588 000 (USD 435 120), leaving over SGD 706 000 (USD 522 440) of unexplained wealth. Although no ML offences were established due to the cash-based nature of transactions and lack of admissible evidence, MOM recommended 61 charges for collecting kickbacks. Person A was sentenced in November 2024 to 24 weeks' imprisonment and ordered to return SGD 395 440 (USD 293 000) to 57 migrant workers. Confiscation proceedings for the remaining unexplained wealth of SGD 311 119 (USD 230 000) are ongoing.

[34] See Box 7.1

8.3. Freezing and/or seizing criminal property and property of corresponding value

505. LEAs use a range of legal powers to seize and prevent the dissipation of criminal property, supported by WoG strategies and SOPs specific to each agency. The primary tool used is Section 35(1) of CPC, which allows LEAs to freeze and seize suspected criminal property without a court order. Seized property must be reported to the court either upon conclusion of the investigation or within one year, whichever comes first. Additional powers under Sections 18 and 21 of the CDSA enable restraint orders to prevent asset disposal, while Section 19, CDSA allows ex parte orders prohibiting dealing with realisable property. CPIB and CNB have additional seizure powers under PCA and MDA, respectively. Examples of these provisional measures are provided in Box 8.3

8.3.1. Active pursuit of provisional measures resulting from financial investigations

506. LEAs make active use of provisional measures to secure assets identified as a result of financial investigations, including in complex cases. Overall, authorities recorded seizures in a nearly 20 000 cases, concerning values of SGD 6.3 billion[35] (USD 4.7 billion). As shown in Table 8.1, seizure results are significant in value. However, only 5% of these cases (962) involved ML-related seizures, while accounting for 92% of the total seizure amounts. Conversely, the remaining 95% non-ML cases yielded more modest values, contributing to 8% of the total seized amounts. This follows on from the analysis of Singapore's investigation and prosecution of ML (see IO.7), which shows how Singapore's LEAs investigate very significant numbers of smaller cases. The few ML-related cases (typically involving foreign predicate offences) are high-value cases and generate most of the seizure amounts, while the majority of domestic predicate cases are more numerous and average out to be lower in value, and unaccompanied by ML investigations. For example, the 2023 *3B$ case,* in effect a combination of cases given the extensive networks and large numbers of subjects and funds involved, accounts for 47% of total seizures.

Table 8.1. Amount Seized (in SGD Million)

Seizure	2020	2021	2022	2023	2024	Total (%)	% ML seizures	% non-ML seizures
Foreign predicate offences (including tax crime)	100.1	836.1	289	3 532.60	320	5 077.8 (79.5%)	100	0
Domestic predicate offences (including CEF)	139.8	505.2	217.9	154.1	291.7	1 308.7 (20.5%)	45.2	54.8
Total number of cases (including tax crimes, but excluding CEF) (2)	4 287	4 411	3 338	4 108	3 627	19 771	5	95
# cases (ML seizures, excluding CEF)	209	242	178	191	142	962	n/a	n/a
# cases (non-ML, usually domestic predicates)	4 078	4 169	3 160	3 917	3 485	18 809	n/a	n/a
Total seizure amounts (including tax crime and CEF)	**239.9**	**1 341.3**	**506.8**	**3 686.7**	**611.7**	**6 386.4 (100%)** [1]	**92**	**8**

Note: (1) the total is the sum of lines 1 and 2.

507. Singapore has seized a wide variety of assets constituting criminal property including real estate, cash, vehicles, vessels, luxury items such as watches and handbags, precious stones and metals, securities, virtual assets, casino chips, and club memberships. Funds in bank accounts and real estate represent the largest asset categories by value seized.

508. Singapore's risk and context makes it essential to use international co-operation effectively to pursue asset recovery, particularly in the early phases of investigations. Singapore actively applies provisional measures, including stop-payment mechanisms, for example through INTERPOL's I-GRIP, the Egmont Group, ARIN-AP, and the rapid-response powers of ASC, which operates 24/7 to trace and freeze cross-border criminal proceeds. LEAs made a limited number of MLA requests in relation to provisional measures when considering the volume of ML investigations they conduct. However, as discussed further in IO.2, LEAs often use informal channels to trace assets and seek the imposition of provisional measures, followed by formal MLA requests when needed. While initial outreach often succeeds in restraining proceeds abroad, which is positive, subsequent MLA requests rarely follow to build on this progress. This is typically due to the absence of assets available for seizure, confiscation or repatriation. Singapore has also demonstrated responsiveness to foreign requests, executing urgent measures within seven days or by the requested deadline, and handling the majority of cases within 60 days.

509. Seizures of proceeds and instrumentalities are aligned with risks to a reasonable extent and concentrate in a few predicate offence types (Table 8.2). Over 61% of seizures relate to organised crime, mainly driven by the 3B$ case in 2023 (involving fraud, and forgery). ML seizures in respect of some high-risk predicates such as corruption, tax crimes, TBML and drugs (a notable ML threat according to the NRA) are modest and result from the lower number of ML cases investigated for these predicate crimes in comparison to fraud. There were no TF seizures during the reporting period, which aligns with risks. The ASC has seized SGD 590 million (USD 436.6 million) in proceeds related to CEF, which is in line with risks only to some extent (see 3.4.2). While seizures are high in real terms, this is not in keeping with the significance and increase in fraud-related cases.

Table 8.2. Seizures per predicate offence (in SGD Millions)

Predicate offence	2020	2021	2022	2023	2024	Total (%)	% ML seizures	% non-ML seizures
Organised crime	0	13.3	254.7	3 378.5	272.2	3 918.7 (61.4%)	100%	0
Fraud (excluding domestic CEF)	58.7	895.1	38.3	7.3	20.5	1 019.9 (16%)	99.6%	0.4
Domestic CEF	57.6	102	146.6	100.3	182.8	589.3 (9.2%)	100%	0
Corruption	14.7	2.4	12.4	150.9	12.8	193.2 (3%)	93%	7
Tax (including Tax ML and tax crimes)	54.6	14.5	14.4	25.5	34.4	143.4 (2.2%)	25.6%	74.4
TBML	0	0.7	0	0.6	0	1.3 (0%)	100%	0
Drug-related offences	1.9	1.5	1.3	1.4	1.6	7.7 (0.1%)	85.7%	14.3
Others (such as robbery, theft, remote gambling)	51.4	310.8	42	22.9	87.1	514.2 (8.1%)	0%	100
Total seizures	**239.9**	**1 341.3**	**506.8**	**3 686.7**	**611.7**	**6 386.4**	**92%**	**8%**

8.3.2. Expeditious measures

510. As shown in Box 8.3, Singapore can act swiftly to freeze assets, mainly through S35 CPC powers and coordinating with international counterparts. Case studies show that LEAs can suspend transactions in a timely manner by freezing assets moved to or through Singapore, and FIs/VASPs sometimes apply temporary suspensions ("credit freezes") proactively, reporting them to LEAs afterwards via STRs. However,

the systematic use of such suspension measures is unclear, and no statistics exist on how often SPF exercises this power or on the frequency of requests made by STRO (such as from other countries seeking suspension). Singapore would benefit from a more coordinated response to the temporary suspension activities of FIs and VASPs, including by affirming them after the fact as CPC S35 suspensions. This would also guard against unintended consequences on genuine accountholders. This is because seizure powers pursuant to S35 CPC can apply for up to one year, at which time LEAs need to apply to the Courts for continued seizure of the assets (or release of the seized assets before the one-year mark). The Courts will generally grant shorter renewals for continued seizure of the assets. A maximum duration of one year for such freezes is not consistent with a truly provisional and expeditious measure intended to buy time for more intensive LEA action. Moreover, suspensions in Singapore are essentially restraints that can last a year (or more after a court review), so the length of time that passes without court review is considered somewhat problematic. This is a minor issue dealt in the TC analysis (see R.4).

Box 8.3. Provisional measures[36]

Recovery of funds by Singapore through various informal channels and MLA

In July 2024, a company that was a victim of a BEC scam lodged a complaint with the SPF stating that it had been tricked into sending USD 42.3 million to a fraudulent bank account in Timor-Leste. Some of the funds were also found to be further transferred to bank accounts in Indonesia. SPF sought assistance from authorities in Timor-Leste and Indonesia to provisionally freeze the said illicit proceeds in their countries. By leveraging on INTERPOL I-GRIP's mechanism, ARIN-AP, LEA to LEA, FIU to FIU and MLA channels, Timor-Leste repatriated USD 39.3 million to Singapore. Steps are being taken for the remaining USD 2 million to be repatriated from Timor-Leste and Indonesia.

511. In conclusion, LEAs actively use provisional measures, primarily through S35 CPC, to secure assets and prevent dissipation, including in complex, high-value cases. Overall, a small number of ML cases (including the 3B$ case) generate the overwhelming majority of seized assets. Cases involving seizures from predicate offence investigations account for 95% of all instances of seizures, but a low average value. Seizures from ML cases generally involve foreign predicate offences, with domestic predicate cases representing only 11% of ML-related seizures by value. Seizures are aligned with risks to a reasonable extent, and authorities should enhance efforts to better address the severity of the CEF threat while more actively seeking opportunities for seizure related to some higher risk predicates, such as drug crimes.

8.4. Managing frozen or seized property to preserve its value

512. Asset management is a strength in Singapore's asset recovery regime. There is no central asset management office. Rather, each LEA is responsible for overseeing the upkeep and value preservation of the seized assets, guided by the 2024 'Whole-of-Government (WoG) Guidelines on Asset Management' which was introduced in furtherance of the NARS. This document ensures consistent and effective asset management across all LEAs, incorporating the objective of value preservation into all procedures. The Guidelines are operationalised by LEAs through SOPs that offer flexibility to accommodate various asset classes ranging from vessels to fine art and exotic animals, while ensuring accountability and transparency. Recognising the rise of virtual assets in criminal activity, Singapore also introduced the WoG Guidelines on Management of Crypto-assets, which standardise procedures to swiftly secure and – where appropriate – liquidate seized virtual assets to preserve their (potentially volatile) value. This decentralised approach to

[36] See also Box 2.4.

asset management does not pose effectiveness issues and does not undermine effective resource allocation within LEAs.

513. Moreover, in practice, Singapore has demonstrated a proactive and structured approach in managing frozen or seized criminal properties to preserve their value, including through timely pre-confiscation sale or disposal where appropriate. This highlights LEA's emphasis on maximising returns for the state, legitimate owners, or victims of crime as appropriate. This is also apparent from Singapore's mature approach to managing atypical assets. For instance, in a tax evasion case involving scrap gold, IRAS quickly disposed of 27 kg of seized gold via public auction to mitigate the volatility of gold prices, recovering SGD 2.3 million (USD 1.7 million) which was then used to offset outstanding taxes. In the 3B$ case, SPF managed an unprecedented volume of luxury goods including purses and cars by contracting professional asset managers and secure storage facilities, ensuring both evidentiary integrity and value preservation. Authorities have also safely managed one seized oil tanker, which was later auctioned off.

8.5. Confiscating and enforcing confiscation orders

514. Singapore confiscates the proceeds of both domestic and foreign predicates primarily through the use of domestic powers, and to a limited degree, uses international co-operation where assets are located abroad. Singapore has confiscated large amounts of criminal property leveraging on various legislative provisions to confiscate criminal assets (CDSA, CPC, OCA, PCA, and MDA) and through various approaches (NCBC, conviction-based confiscation (CBC) for ML offences, and unexplained wealth confiscations). Overall, seizures lead to confiscation to a good extent, but the minor shortcomings for seizures (discussed in 8.3) flow through to final confiscation outcomes. There are some weaknesses in seizure and subsequent confiscation in respect of predicate offences related to fraud, corruption, and TBML.

8.5.1. Criminal property and property of corresponding value located domestically

515. During the reporting period, Singapore confiscated SGD 3.9 billion (USD 2.9 billion) from ML and predicate offences which reflects a good (61%) seizure to confiscation ratio (including criminal tax recoveries). Excluding the top five asset recovery cases, the seizure/confiscation ratio is lower, at only 40%. However, in keeping with the trend seen with seizure figures, most confiscations were achieved in a small number of ML cases involving foreign predicate offences. In 93% of cases, the confiscation involved small values (approximately SGD 38 000 or USD 28 120 on average), linked to predicate offences investigations (see Table 8.3).

Table 8.3. Confiscations (in SGD millions)

Predicate offence	2020	2021	2022	2023	2024	Total (%)	% ML conf.	% non-ML conf.
Foreign predicate (including tax crimes)	32.1	43.3	25	3 262.7	105.7	3 468.8 (89.4%)	100%	0
Domestic predicate (excluding CEF)	31.1	302.3	24.8	25.9	25.4	409.5 (10.6%)	4.7%	95.3
Total number of confiscation cases (including tax crimes and excluding CEF)	2 090	2 108	2 514	2852	1 304	10 868	7.2%	92.8
# of ML cases (excluding CEF)	179	182	162	172	90	785	n/a	n/a
# of non-ML cases	1 911	1 926	2 352	2 680	1 214	10 083	n/a	n/a
Total Confiscations (including tax crimes and excluding CEF)	**63.2**	**345.5**	**50.1**	**3 288.8**	**131**	**3 878.6**	**90%**	**10%**

Note: SGD 590 million or USD 436.6 million of seized funds from scams / domestic CEF are excluded from this table, as Singapore does not track the amount confiscated, given that the seized funds may not be directly co-related to the crimes committed in the same year. The number of domestic CEF cases leading to confiscation is not available.

516. Singapore confiscates a wide array of assets, both proceeds and instrumentalities, including residential and non-residential property, cash and bank accounts, shares and companies' assets, vehicles and luxury goods, drugs, illicit wildlife products and virtual assets. Real estate and bank accounts are the most frequent confiscated assets in ML cases, while virtual assets, securities and bank accounts represent the biggest share of confiscated assets in non-ML cases.

517. Authorities rely on a range of measures to recover assets. Approximately 33% (around SGD 1.3 billion or USD 1 billion) of confiscation results from conviction-based confiscation (CBC), and 67% (approx. SGD 2.6 billion or USD 1.9 billion) from non-conviction-based (NCBC) proceedings (these figures exclude criminal tax recoveries). For example, 72% of all confiscated assets result from NCBC proceedings in the 3B$ case. As indicated in IO.7, a large majority of ML convictions are cases where the accused pleaded guilty (including through plea deals), and consequently, confiscation results in these cases are often achieved through plea deals followed by court orders (which are still counted among CBC figures). These involve situations where the accused agree to withdraw their claim to the assets (such as in the 3B$ case). SGD 7.9 million (USD 5.8 million) was confiscated during the reporting period through CIA. Singapore has also recovered approximately SGD 87 million (USD 64.3 million) in tax (from criminal cases) across 433 cases and an additional SGD 81 million (USD 60 million) through penalties and fines from criminal cases. There are also instances of default confiscations of unclaimed funds where sums are forfeited to the State. Overall, when they are issued by Courts, confiscation orders are enforced (and as outlined below, property returned to the victims/forfeited to the state as appropriate). There is no evidence of unfulfilled court orders or amounts 'ordered' for confiscation which are not actually "taken in" or realised by the State. This is positive and ensures that criminals are permanently deprived of ill-gotten assets.

518. Singapore has shown it is able to prioritise the pursuit of complex and cross-border cases with a significant amount of criminal assets involved, including related to high-risk predicates, in some circumstances. LEAs successfully achieved confiscation of more than 90% of the seized assets within a year in the *3B$ case* as some involved pleas and there were little/no challenges, and within 2-4 years in the other two larger cases. This is reasonable given the cross-border nature of the case and the need for international collaboration, involvement of complex ownership structures, and multiple predicate offences. Notwithstanding the considerations laid out in section 3.4.4, these three largest confiscations by value (Table 8.3 and 8.4) demonstrate the effectiveness of Singapore's confiscation regime and show that authorities are capable of securing high-value confiscations when such cases arise.

Table 8.4. High-value confiscation cases

Case	Amount Seized (SGD/Year)	Amount Confiscated (SGD/Year)	Remarks
3B$ case	~ 3 billion (2023)/ USD 2.2 billion	~ 2.8 billion/ USD 2 billion (2024)	Assets related to 2 out of 27 individuals are still pending the conclusion of proceedings under Singapore's laws. A significant portion of proceeds were confiscated through NCBC and CBC.
Case S	~ 233.7 million/ USD 173 million (2021)	~ 233.4 million /USD 172.7 million (2023-24)	The case pertains to a regulatory offence under the Securities and Futures Act for operating without a capital market services license and potential fraudulent activity. ML investigations relating to the fraudulent activity are ongoing. 99% of assets seized through the financial investigation were confiscated.
Case E	~ 144.3 million/ USD 106.7 million (2020)	~ 55.2 million/ USD 40.8 million (2021-23)	A case of investment fraud in which 38% of assets seized have been confiscated thus far. Proceedings are ongoing.

519. Overall confiscations align with risks to a reasonable extent (Table 8.5). There is a reasonable correlation between the value of confiscation and the main proceeds-generating crimes. Singapore primarily confiscates assets in relation to a low number of organised crime cases (owing to the *3B$ case*), fraud and tax crime. Almost all organised crime proceeds seized were confiscated, while there is room to improve the confiscation rate for corruption, TBML and fraud (for which only 10% of seized assets are confiscated). The absence of TF confiscations is in line with the risk and context of Singapore.

Table 8.5. Confiscations per predicate offence (in SGD Million)

Predicate offence	2020	2021	2022	2023	2024	Total (%)	% ML conf.	% non-ML conf.
Organised crime	0	4.4	0	3 253.9	101.8	3 360.1 (86.6%)	100	0
Fraud (excluding domestic CEF)	38.2	91.1	25.3	6.3	3.8	164.7 (4.2%)	66.3	33.7
Corruption	1.1	0.7	0.2	2.4	0.1	4.5 (0.1%)	68.9	31.1
Tax (including Tax ML and tax crimes)	17.9	14.5	14.4	23.0	17.5	87.3 (2.3%)	0	100
TBML	0	0	0	0	0	0 (0%)	0	0
Drug-related offences	0.2	0.1	0.4	0.4	0.2	1.3 (0%)	90.7	9.3
Others (such as Robbery, theft, remote gambling)	5.7	232	12.3	5.4	4.5	259.9 (6.7%)	0	100
Total confiscations	**63.2**	**345.5**	**50.1**	**3 288.8**	**131**	**3 878.6**	**90**	**10**

Note: SGD 590 million (452 million) of seized funds from domestic CEF are excluded from this table as Singapore does not track the amount confiscated in this respect. The funds are ultimately restituted to identifiable victims or forfeiture to the State following the completion of the criminal justice process.

8.5.2. Criminal property and property of corresponding value located abroad

520. Case examples and discussions with the authorities show LEAs are aware of the need to pursue assets abroad and proactively seek assistance from foreign counterparts to this end, both through formal and informal channels. As a matter of practice, LEAs commence domestic ML investigations into cases triggered by foreign counterparts with a view to identifying a possible nexus to Singapore. Where applicable, SPF also proactively engages its foreign counterparts to alert them to the presence of criminal proceeds and conducts joint investigations when such a nexus is established as necessary. Authorities also routinely use informal channels to improve confiscation outcomes (especially in cases with a foreign nexus) and actively follow-up on requests (over 900 informal requests have been made through ARIN-AP, Egmont, INTERPOL and other channels, and SGD 102 million (USD 75.5 million) has been seized as a result of informal co-operation. SOPs instruct LEAs to use informal networks to obtain early indications of cross-border elements in an investigation (such as bank account details, BO data, or criminal records). Where appropriate, LEAs are required to seek both informal and formal assistance concurrently. This approach narrows down the scope of subsequent MLA requests that may be issued in case foreign counterparts provide positive responses or viable leads. Case studies (see IO.2) and discussions with the authorities indicate that informal co-operation has helped speed up MLA and ease co-operation overall.

521. Singapore is credited for utilising informal channels to support confiscations, but there is still scope to improve the pursuit of formal co-operation, since MLAs are required in some instances to pursue assets located abroad and are seldom used. Despite the good results that can be obtained through informal co-operation, MLA is often necessary at the later stages of assistance (e.g. to finalise confiscation or enforce an order for assets located abroad). Over five years, Singapore sent 110 MLA requests for the freezing, seizing confiscation and enforcement of confiscation orders pertaining to criminal property (Table 8.6). Singapore sought the recovery of SGD 144 million or USD 106.5 million (and 3 properties) (USD 106.5 million) and actually secured the recovery of SGD 52 million (USD 38.5 million) and 3 properties (mainly in 2024). 51% of MLA requests were executed without any assets found/repatriated by the

requested state. It is also notable that Singapore did not seek enforcement of any of its own confiscation orders abroad. This indicates that more could be done to pursue assets located outside Singapore, especially considering the country's risk and context as a transit hub and the outward flow of funds from fraud victims in Singapore.

522. MLA requests are infrequent considering the volume of predicate and ML investigations (11 189 in the reporting period). MLA requests related to asset recovery were made in fewer than 1% of ML investigations, including many with transnational elements and involving high-value cases. This is modest when considered against Singapore's risk and context. While not every ML investigation would necessarily warrant an MLA request, there is scope to increase alignment of the use of MLA requests with Singapore's risks, considering that – as stated above – a formal request is often needed to conclude a case, such as when confiscations progress to the final stages of judicial procedures and/or repatriation is sought.

523. In turn, Singapore receives a significant number of asset recovery requests from counterparts concerning an estimated SGD 1.1 billion or USD 814 million (such as bank accounts and properties). Singapore generally responds proactively to these requests. As discussed further in IO.2, the scope of assistance provided is somewhat hindered by procedural issues, and only five in 26 foreign confiscation orders led to the repatriation of assets. This indicates that there may be a an even stronger need to identify and investigate ML related to foreign predicates in Singapore, and that Singapore may be able to do even more to pursue foreign-linked proceeds within its own borders directly.

Table 8.6. Outgoing/Incoming MLA requests (Asset Recovery) (SGD million)

	2020	2021	2022	2023	2024	Total
Total Outgoing # MLAs	24	18	17	12	39	110
Assets sought for recovery	SGD 10.7m + 2 properties	SGD 23.2m + 1 property	SGD 32.8m	SGD 89.3m	--	SGD 144.5m + 3 properties
Total Incoming MLAs	14	23	11	13	12	73
Assets sought for recovery	SGD 22.7m + 35 bank accounts + properties	SGD 7m + 55 bank accounts + 3 properties + virtual asset accounts + others	SGD 107.6m + 7 bank accounts + 1 property + others (e.g., stocks)	SGD 152.6m + 29 bank accounts + 1 property + virtual asset accounts + others	SGD 824.3m + 12 bank accounts + 2 properties, + others (virtual asset account and gold bars)	SGD 1.11b + 138 bank accounts + 7 properties + others

524. In conclusion, Singapore achieves good results converting seizures into confiscations, confiscating close to SGD 3.9 billion (USD 2.9 billion), mainly from ML and some predicate offences. The vast majority of asset recovery is secured from high-profile cases, involving an array of assets and through a combination of CBC and NCBC. There is a good seizure/confiscation ratio (61%), which varies according to certain predicate offences. Overall confiscations align with risks to a reasonable extent, with room to improve confiscation in respect of corruption, TBML and fraud. While Singapore understands the value of pursuing assets located abroad, there is scope to improve the use of formal international co-operation.

Box 8.4. Confiscations

3B$ Case (NCBC)

Over 90% of the assets seized from the 10 main persons of interests (approximately SGD 944 million) or USD 698.6 million) were forfeited to the State. Their remaining assets were returned due to evidentiary challenges in proving criminal origin. SPF seized and issued prohibition of disposal orders on assets amounting to about SGD 2 billion (USD 1.4 billion) linked to 17 foreign nationals who had left Singapore. 15 of them agreed to forfeit about SGD 1.85 billion (USD 1.4 billion) worth of assets, or 98.6% of their seized and prohibited assets, to the State. Court orders were made pursuant to Section 370(2)(d) of the CPC for the forfeiture of assets, in the absence of convictions (i.e. NCBC). The assets of the two remaining absconded persons are being dealt with in accordance with the new absconded persons provisions in the Anti-Money Laundering and Other Matters Act 2024, and Sections 370(3A) and 372(1) of the CPC. To preserve asset value, a dedicated SPF team was formed to manage the storage, upkeep, and maintenance of the wide range of seized items, leveraging expertise and specialised services from industry partners.

Tax fraud case

IRAS was alerted to a tax fraud scheme involving abuse of the government-run Productivity and Innovation Credit (PIC) scheme. Investigations by IRAS revealed that the director of a company had orchestrated a scheme to inflate sales and fraudulently claim higher PIC cash payouts.

IRAS uncovered a network of claimants and, considering the presence of ML indicators, referred the case to SPF(CAD) to open a PFI. CAD charged the director with ML for abetting fraudulent claims. In lieu of confiscation, tax assessments were raised to recover the fraudulent PIC cash payouts and bonuses obtained SGD 5.7 million. Unable to pay the full amount, he served an additional 31.5 months in prison.

8.6. Returning confiscated property to victims

525. Singapore prioritises the return of assets to victims and rightful owners when they are identifiable and forfeits criminal assets to the State when they are not (which also serves to cover costs of asset preservation). Restitution is a process carried out post-confiscation and not a separate form of asset recovery that precludes confiscation in Singapore. Authorities have taken many proactive steps to implement a victim-cantered approach, such as: seeking court-ordered compensation; adopting early seizure and value-preservation practices to maximise funds available for restitution; and engaging in upstream harm prevention, particularly in CEF cases. Where necessary, Singapore proactively reaches out to foreign partners to return recovered assets to other jurisdictions, which it achieves especially through informal channels. Box 8.5 demonstrates the effectiveness of rapid cross-border collaboration in preventing asset dissipation and securing victim restitution, both in Singapore and abroad.

526. Singapore returned approximately SGD 403 million (USD 298 million) in confiscated assets to victims during the reporting period, or about 10% of the SGD 4 billion (USD 2.96 billion) confiscated in the same period. This includes SGD 115.9 million (USD 85.8 million) of restitution in ML cases, with about 90% linked to foreign predicates (primarily fraud and corruption) and SGD 291.6 million (USD 215.7 million) of restitution in associated predicate offence cases, largely stemming from domestic predicate offences such as illegal gambling, robbery, and fraud. This outcome is largely in line with Singapore's risk profile as an IFI, with most confiscated assets stemming from ML cases involving foreign predicates and unknown victims.

Box 8.5. Asset Repatriation

1 MDB (Malaysia)

Since the high-profile embezzlement of the 1MDB investment fund in Malaysia (starting in 2015), SPF and AGC have obtained orders from Singapore courts to release about SGD 124 million (USD 91.7 million) in seized assets and return these to Malaysia. In the review period, SGD 92.1 million (USD 68.1 million) in assets have been repatriated, and Singaporean authorities are engaging with their Malaysian counterparts to secure the repatriation of the remaining amount.

Scam victims

In April 2024, swift co-ordination between Singapore and authorities in foreign jurisdictions led to the successful recovery of SGD 370 000 (USD 273 800) in scam proceeds and their repatriation to the victim in Singapore. After a bank in Singapore detected suspicious transfers involving an older victim's account to a flagged account in the foreign jurisdiction, ASC promptly alerted its counterpart. Further investigation revealed additional losses from a second bank, which were also traced to the same foreign account. With strong co-operation between banks, LEAs, and international partners, including proactive community engagement by Singapore's police, the funds were frozen and returned to Singapore.

8.7. Identifying and confiscating falsely or undeclared currency/BNIs or those related to ML/TF or predicate offences

8.7.1. Identifying and seizing non-declared or falsely declared cross border movements of currency and BNI

527. Singapore has recently strengthened its institutional and operational framework to identify and seize non-declared or falsely declared cross border movements of currency and BNI. Some gaps have been observed with the detection of CBCRR cases, with 439 violations detected over five years, out of 220 834 declarations and 576 million border crossings (travellers). Singapore has sought to remedy gaps with detection from 2024, but the effectiveness of these recent measures cannot be fully determined at this time. Authorities are aware of the risks related to cross-border transportation of cash/BNI and have made some seizures, although the number of seizures is low considering Singapore's status as an IFI and transit/transportation hub. There has only been one confiscation in relation to ML.

528. Singapore's declaration system, which was fully digitised since 2024, requires any person moving cash in and out of the country in excess of SGD 20 000 to (approx. USD 14 000) to make an online declaration. These declarations are automatically ingested into STRO's IT systems. ICA and SPF/CAD utilise various means to detect false/under-declarations, including conducting risk profiling and targeting of passengers at checkpoints for passengers from jurisdictions identified by Singapore as high-risk countries for CBCRR breaches. LEAs also consult STRO's and SPF's databases for relevant STR, CTR and CMR information filed by casinos, money changers and remittance services. LEAs also leverage on foreign sources and search criminal backgrounds, screen against intelligence databases and review advance passenger information from airlines. Crucially, however, ICA lacks advanced screening machines that can specifically detect cash by scanning postal articles, cargo, shipments, and luggage moving through checkpoints. This creates a vulnerability, particularly considering Singapore's position as a

transit/transportation hub. ICA would benefit from the use of new technologies to enhance its cash detection capabilities for both travellers and cargo.

529. Singapore's NRA does not identify bulk cash smuggling as a significant risk. Singapore has one of the highest levels of financial inclusion in the world and is mainly a cashless society, meaning that substantial amounts of cash would be more out of place in Singapore than elsewhere. However, cash-based ML has proven persistent even in highly banked jurisdictions, and among some of Singapore's closest neighbouring countries. The NRA acknowledges there is a risk associated with money mules transporting cash in/out of the country.

530. Notwithstanding, some limitations were observed in the risk-profiling system and detection practices, which undermines LEA's ability to identify potential breaches of CBCRR in a timely and effective manner. For example, the risk profiling system did not regularly target persons carrying cash. There have been cases in which ICA found out post facto about false or non-declarations, with some passenger found traveling through Singapore with cash over the reporting threshold (see example in Box 8.6). Authorities attribute these lapses to the absence of electronic submission mechanism prior to 2024.

531. Singapore has since 2024 taken steps to improve detection of CBCRR breaches and better adapt to observed typologies, including geographical risks. For example, in early 2025, authorities conducted additional checks on passengers from a neighbouring country prone to CEF activities to better understand ML/TF/predicate offence risks associated with large cash inflows. Moreover, CAD now shares CBCRR breaches detected during ML or predicate offence investigations with ICA on a quarterly basis. These are combined with other data points to improve ICA's risk profiling and identification of CBCRR breaches. ICA officers have received dedicated training to spot suspicious traveller behaviour. Since 2025, ICA enforces CBCRR breaches above the declaration threshold without ML/TF suspicion, while complex cases are escalated to CAD's FIG for detailed financial investigation. While positive, it is too early to determine whether these measures will lessen the number of undetected instances of CBCRR violations and mitigate the risk of cross-border cash smuggling.

Box 8.6. Breach in CBCRR declaration

Cross-border BEC case (2020)

A Western health products company was defrauded into transferring EUR 6.6 million to a Singapore corporate account for fake Personal Protective Equipment purchases. Swift action by SPF and seven banks led to freezing over EUR 6.4 million the same day. Investigations revealed the Singapore company's director knowingly facilitated laundering for a foreign fraud syndicate. Over SGD 10.2 million (USD 7.5 million) was moved through multiple accounts. He submitted two CMRs (SGD 1 million/USD 740 000 each) but later admitted under-declaring cash amounts hand-carried out of Singapore. Investigators matched CMRs, withdrawals, and travel records to trace fund flows. The director was convicted of seven ML counts and two CBCRR breaches. He received 8 years and 8 months' imprisonment. He is currently appealing the conviction

Detection of undeclared amount (2025)

ICA officers intercepted a man from Country X at a ferry terminal with undeclared cash amounting to SGD 26 260 (USD 20 000). CAD investigations revealed his involvement in advertising illegal online gambling websites based out of Country Y. Evidence from his phone showed draft and final advertisement materials used on social media. He admitted the cash was payment from gambling operators to fund further advertising. CAD found no links to ML, TF, or predicate offences upon inquiring in SPF and STRO databases. Information was shared with Country Y authorities and INTERPOL. He was

charged 10 days later under Sections 60 and 54 of the CDSA and convicted in March to 3 months and 2 weeks' jail. The full cash amount was forfeited under Section 364 CPC. After serving his sentence, he was deported and barred from re-entering Singapore.

8.7.2. Confiscation of currency or BNI related to ML/TF or predicate offences

532. The authorities have shown they can confiscate currency in case of CBCRR breaches where they consider there is a link to ML/TF or predicate offences, but there has only been one confiscation in relation to ML despite 439 instances of false or non-declaration.

533. In the review period, incoming passengers submitted a majority of CBCRR declarations (the majority of travel in/out of Singapore occurs by land over the border with Malaysia), which is foreseeable given Singapore's role as a transit/transportation hub. A small number of passengers submit CBCRR when compared to the overall traffic flow (0.115% of incoming passengers and 0.05% of outgoing passengers), as seen in Table 8.7.

534. While 439 instances of false or non-declarations were detected (mainly at air checkpoints), only 7% of the SGD 30.4 million (USD 22.5 million) in undeclared or falsely declared cash detected was confiscated. Further, 13.7% of the SGD 16.1 million (USD 12 million) seized from investigations was confiscated. All false or non-declaration amounts linked to ML/TF or predicate offences were fully confiscated, but this accounts for only one case with a prosecution ongoing for another case detected in 2025 and some BNIs have also been seized and no breaches detected through mail/cargo.

535. Detection of violations and amounts seized and confiscated are low, largely due to the abovementioned weaknesses in risk-profiling and detection (the low number of CBCRR breaches detected in 2020 to 2022 can be attributed to drop in passenger travel due to Covid-19). Singapore is likely not detecting a sizeable proportion of non/false declarations, considering evidence of prior missed cases and the high number of passengers crossing the land border with Malaysia, which Singapore considers are principally daily commuters (economic workers) that travel to/from both countries. As reported in its 2025 Mutual Evaluation, Malaysia has detected EUR 16.58 billion worth of cash/BNI (SGD 25 billion or USD 18.5 billion), and an assessment by Malaysia's FIU shows the Singapore dollar is the most common currency declared entering Malaysia (notwithstanding that there is no breakdown of the source countries and the foreign currencies of the EUR 16.58 billion worth of cash/BNI that might have entered Malaysia through other countries with much longer land borders with Malaysia such as Thailand, Brunei and Indonesia).

536. Singapore attributes a majority of CBCRR breaches to first time offenders who are not linked to criminality and who had misunderstood, lacked awareness of or mistakenly reported on the CBCRR obligation (e.g. due to language barriers). These reporting obligations are implemented in virtually every country in the world, and such a massive proportion of significant cash carrying travellers (438/439) having simply misunderstood the obligation while making a false or non-declaration does not stand to reason. This inability to link such significant volumes of cash entering the country through travellers making false or mis-declarations shows weaknesses in the process for fully investigating these travellers (especially in a largely non-cash society).

Table 8.7. False/non declarations and sanctions

	2020	2021	2022	2023	2024	Total
Passenger traffic	42 189 542	5 923 363	104 880 094	192 845 557	230 398 931	576 237 487
incoming	21 118 566	2 838 084	52 344 484	96 026 060	114 850 300	287 177 494
outgoing	21 070 976	3 085 279	52 535 610	96 819 497	115 548 631	289 059 993
Total # CMRs	19 785	6 432	37 180	71 964	85 473	220 834
incoming	12 695	3 267	22 954	43 762	53 417	136 095 (62%)
outgoing	7 090	3 165	14 226	28 202	32 056	84 739 (38%)
Number of false and non-declaration cases detected	28	14	46	120	231	439
CBNI detected (Million SGD)	4.0	0.8	2.9	10.3	12.4	30.4
Value of CBNI seized for further investigations (Million SGD)	3.2	0.5	0.7	6.9	4.8	16.1
CBNI confiscated (Million SGD)/number of cases	1.1 (2)	-	-	1 (8)	0.1 (7)	2.2 (17)
Amount of Court fines (in SGD)/number of cases	39 000 (3)	5 000 (1)	14 000 (2)	96 500 (15)	53 000 (11)	207 500 (32)
Number of travelers issued composition notices	18	7	32	59	155	271
Amount of composition collected (in SGD)	27 000	16 000	41 000	102 000	645 000	831 000

Note: the value of declarations is not tracked.

8.7.3. Sanctions

537. Singapore has a range of sanctions available to enforce the CBCRR regime, which are calibrated to the degree of culpability of the offender (see R.32): a warning for minor infractions (if detected CBNI is lower than SGD 25 000 or USD 18 500 and not linked to ML/TF or associated predicate offences), a composition sum (i.e. financial penalty in lieu of prosecution) for detected CBNI below SGD 100 000 or USD 74 000, court fines, imprisonment for ML/TF offences and/or confiscation (a larger percentage of the detected infraction is confiscated for larger false or non-declared amounts). The composition framework only applies for first time offenders with detected physical cash/BNI below SGD 100 000 or USD 74 000 and which is unrelated to ML/TF or predicate offences.

538. When dealing with false or non-declarations, LEAs seize the cash pending an investigation to ascertain whether the funds are linked to ML, TF or associated predicate offences. If they are, a prosecution for breaches to the CBCRR regime is pursued, leading to confiscation calibrated to the amount of the breach or if the traveller cannot reasonably explain provenance of the funds. 100% of the value is confiscated if a ML/TF or associated predicate offence is found or the passenger exhibits a high level of culpability, in addition to imprisonment.

539. There are some challenges which could undermine the application of the abovementioned sanctions framework. As discussed in IO.7, Singapore's competent authorities acknowledge that investigators and prosecutors face a persistent challenge linking funds to offences that takes place overseas. This is more pronounced when dealing with cash because of the lack of clear trail linking it to a specific source or offence. As a result, investigators generally rely on intelligence inputs, antecedents and case history of the passenger to determine if ML /TF or associated predicate offence has occurred, and this explains the low number of cases.

540. Of the two cases linked to ML/TF or associate predicate offence, one is still in the prosecution stage and the other case resulted in a conviction within which all CBNI amounts that were detected were fully

confiscated (and the culprit handed a prison sentence) (see Box 8.7). These sanctions appear effective, but it is challenging to draw systematic conclusions about the effectiveness of sanctions from one case.

541. The remainder of cases are dealt with through a composition scheme, which is not fully dissuasive. SGD 179 500 or USD 132 830 in court fines were meted out (an average of SGD 660 or USD 485 per instance) and a composition amount of SGD 831 000 or USD 614 940 (an average of SGD 3 000/USD 2 220 per composition) was collected from passengers, see Table 8.7). Singapore explains the low amounts by pointing to the fact that 98% of infractions for non-declared amounts involved first-time offenders not known to be linked to ML, TF, or predicate offences. However, money mules, being disposable enablers of ML, would never be sent to smuggle cash if they had already been found to have made a false or non-declaration. In cases of false or non-declaration, the passenger would have had knowledge of the declaration requirement and thus a certain level of knowledge and culpability can be inferred. The number of false declarations detected is an unknown percent of the 439 cases.

542. In conclusion, Singapore has a solid legal framework for CBCRR, though there is scope for improvement in risk-profiling to enhance the detection of breaches. The amounts declared and violations detected reflect Singapore's risk profile or context to some extent. This is notable given its largely cashless domestic economy, high traveller volumes, significant numbers of non-resident Singaporeans, its role as a major transit and transportation hub, and when compared to its closest neighbour. Most offenders are not filing or falsely file CBCRRs are reportedly first-time offenders, and Singapore cannot link the vast majority (438/439) of offenders to criminality. Money mules, too, are usually first-time offenders. This indicates that there are likely issues in follow-up investigations. Singapore recognises these gaps and has enhanced its CBCRR in 2024, though it is too early to assess its effectiveness. When offenders are linked to ML, TF or predicate offences, the sanctions meted out are proportionate and dissuasive. When they are not, the sanctions meted out are not.

Box 8.7. CBCRR violations

Inbound violation (2023, Changi Airport)

ICA flagged an arriving passenger for suspicious behaviour and after alerts from his luggage screening. He made two CBCRR declarations for SGD 505 500 and SGD 1.96 million (respectively USD 375 000 and 1.4 million) but was carrying SGD 1.98 million (USD 1.4 million). SPFCAD seized the cash, detained the passenger, and upon investigations found that he had previously falsely declared SGD 1 million (or USD 740 000). Checks showed no criminal links, that he worked for a money-changing firm, acted as a cash courier, and that funds were legitimate. He was convicted under Section 60 of CDSA and Section 108B of the PC for conspiring to move undeclared cash in excess of the threshold without a full and accurate report. The court imposed a confiscation order of SGD 400 000 or USD 296 000 and a fine of SGD 30 000 or USD 22 000, (about 26% of the undeclared funds). SPF shared case details with his home country, though the follow-up remains unknown.

Outbound violation

A person attempted to leave Changi airport in 2023 without making a CBCRR declaration on the movement of SGD 508 925 (USD 376 604), aided by two accomplices who split the cash amount. The three individuals were profiled by ICA for checks which revealed that cash was not declared, and CAD seized the cash. Further investigations by CAD showed that the main culprit had companies in Singapore from which the seized cash originated, but no sign of criminality was involved. The main culprit was convicted of a CBCRR offence under S60(2) CDSA. He was sentenced to a SGD 10 000 fine or USD 7 400 (SGD 5 000 each for the accomplices, or USD 3 700) and the full amount seized was forfeited to the State under S364 CPC due to the high degree of culpability of the offender who showed intent to conceal the cash to avoid detection by the authorities.

9 Terrorist financing investigations and prosecutions

The relevant Immediate Outcomes considered and assessed in this chapter is IO.9 The Recommendations relevant for the assessment of effectiveness under this chapter are R. 5, 30, 31 and 39 and elements of R. 1, 2, 15, 32, 37 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) The identification and investigation of TF is carried out by three agencies (ISD, CFTB and STRO) which co-ordinate closely and cooperatively, and financial intelligence is actively utilised in TF investigations. Investigative techniques are sound; however, there are opportunities for broader investigation of potential organisational TF and concealed income.

b) Singapore has opened 126 TF investigations into 213 natural and legal persons over the past five years. From these investigations, they have prosecuted six cases of TF over the reporting period using the same typology which involves individuals sending small amounts of their salary overseas to support global terrorist activities. While this is largely in line with Singapore's risk and context, there is an absence of CFT activity in relation to funds transiting through Singapore via the banking sector or DPTSPs.

c) A small proportion of investigated cases are brought to prosecution. Five prosecutions were resolved through guilty pleas and one case concluded with a conviction after a trial. The AGC will prosecute TF offences in cases where they determine the evidential threshold to be conclusively met. This high evidential threshold has likely led to some cases not being prosecuted. Where prosecutions are secured, sanctions are proportionate and dissuasive.

d) Singapore has strategic, policy and operational committees in place which utilise information from TF investigations to inform national CT efforts, contribute to TF threat assessments and the ML/TF NRA, as well as providing policy guidance.

e) It is not evident that Singapore uses alternative measures where securing a TF conviction is not practical.

Recommended Actions (RAs)

Singapore should:

a) Implement measures, such as the use of concealed income analysis, to identify potential TF activity and organisational TF in alignment with Singapore's risk and context, in particular TF transiting Singapore through the use of Singapore's banks, and DPTSPs.
b) Conduct a review of internal thresholds guiding prosecution decisions.
c) Enhance policies and procedures to ensure that there is a broader suite of tools used to disrupt TF, including other criminal justice measures, where it is not practicable to secure a TF conviction.

Overall Conclusions on IO.9

Singapore has strong national co-ordination settings, legal framework, national policies, and personnel to co-ordinate and apply mechanisms for successfully investigating and prosecuting TF in line with risks. Courts have demonstrated that, where cases come before them, proportionate, effective and dissuasive sanctions are applied to natural persons and exist for legal persons. However, Singapore has investigated cases in large numbers with a small fraction of relatively minor cases proceeding to prosecution, and almost all being resolved by guilty plea. The approach to TF prosecutions is conservative but this is in the context of a low threshold for initiating TF investigations in Singapore. In investigations, authorities are able to undertake financial investigations, and Singapore has demonstrated collaboration between domestic agencies responsible for financial intelligence, CT and CFT investigations and prosecutions, and with their global counterparts through formal and informal channels.

Singapore's authorities are aware of TF threats and vulnerabilities, and the results of their TF NRAs have been broadly disseminated. Whilst authorities have sought to mitigate the risks posed by abuse of legal persons and sought to understand the extent of any exploitation of their financial centre by reference to global feedback, further measures can be taken to investigate organised TF and concealed income noting Singapore's global significance as a financial and trading centre and centre for company formation.

Singapore undertakes preventive measures including immigration controls and incorporates rehabilitation and de-radicalisation to counter recidivism. These are actions to prevent terrorism and terrorist financiers, and not alternative measures when a TF conviction was not practicable.

Singapore is rated as having a Substantial level of effectiveness for IO.9.

Immediate Outcome 9

9.1. TF activity identified and investigated

9.1.1. Identification and investigation of TF activity

543. Terrorist financing is criminalised under Singapore's Terrorism (Suppression of Financing) Act 2002 (TSOFA) which also provides for asset confiscation.

544. As noted in IO.1, Singaporean agencies and private sector representatives demonstrated a reasonably sound understanding of TF risk that aligned with the findings of the TF NRAs. Overall, Singapore's NRAs conclude that the TF risk in Singapore is medium-low. Singapore's key TF threats are primarily related to regional terrorist organisations, and radicalised individuals supporting terrorist activities in jurisdictions distant from Singapore, including:

a) terrorist groups, such as the Islamic State of Iraq and Syria (ISIS), Al-Qaeda (AQ), and Jemaah Islamiyah (JI);
b) potential spillovers from the ongoing Israel-Hamas conflict and tensions in the Middle East; and
c) radicalised individuals who are sympathetic towards the cause of these terrorist groups, particularly ISIS.

545. Singapore's identified vulnerabilities reflect its status as an IFC and its geographical proximity to countries with active terrorist organisations. Given the predominant typology of assets raised in Singapore and send abroad or assets transiting Singapore, banks, PSPs with international remittance and DPTSPs pose the greatest risk for exploitation.

546. From their investigations, case studies and other data, Singapore has identified the main typology for TF in their jurisdiction involves provision of financial support to overseas terrorist groups or causes, or affiliated persons, by self-radicalised individuals or terrorist sympathisers based in Singapore. The typology is unsophisticated; the sums involved are small and sourced from individuals' own legitimate salaries or savings which are generally transferred via licensed money remittance services.

547. In both its 2020 and 2024 TF NRAs, Singapore noted its status as a transit hub as relevant to its TF risk and context: "our status as an international financial, business, and transport hub, coupled with robust connectivity, a substantial number of transient visitors, and geographical proximity to countries harbouring active terrorist groups, heightens our vulnerability to TF threats." Notably, the majority of respondents to Singapore's TF risk perception survey (totalling 41 jurisdictions)[37] did not observe a TF nexus with Singapore as a transit hub. Nevertheless, this remains an important aspect of Singapore's context. The TF risk perception survey contributed to Singapore's 2024 TF NRA which identifies Singapore-based individuals utilising their legitimate salaries to fund overseas terrorist groups as one of Singapore's primary sources of TF risk.

548. The identification and investigation of TF is carried out by three agencies (ISD, CFTB and STRO) which co-ordinate closely and cooperatively, using guidelines and SOPs which clearly delineate their respective roles and responsibilities.

549. The **Internal Security Department (ISD)** is Singapore's domestic security and intelligence agency and Singapore's lead agency for investigating terrorism cases. All terrorism investigations consider TF, and all officers in ISD's Counter-Terrorism (CT) Division are simultaneously involved in TF-related work, which includes identification of TF leads. ISD has sufficient resources. ISD has dedicated liaison officers located in countries with a regional TF nexus, supporting the exchange of information with foreign counterparts, and participates in various multilateral CFT and CT forums involving regional intelligence and security agencies. As well as all ISD officers incorporating a TF component into terrorism investigation, ISD has a dedicated team of officers in the TF investigation section of the CT Division. These officers focus on the identification of credible TF leads through preliminary financial examinations in parallel with their counter-terrorism investigations, including liaising with both domestic and foreign partners on potential TF leads. They use a broad array of information and techniques to identify potential TF including the use of Singapore's information/databases, technical investigation techniques and intelligence information. Upon detection of

[37] Other key high TF risk jurisdictions are defined as non-FATF members in Singapore's immediate Southeast Asian region with active terrorists and terrorist groups.

any potential TF elements, ISD refers information to CAD/CFTB for deeper parallel TF investigations. Referrals from ISD account for approximately 60% of TF investigations for CFTB.

550. The **Counter-Financing of Terrorism Branch (CFTB)** is a dedicated branch within SPF/CAD with the core responsibility for conducting TF investigations, following disseminations of financial intelligence from STRO and referrals from ISD through their investigation of Terrorism matters. CFTB serves as Singapore's lead CFT investigation and enforcement agency. CFTB is sufficiently resourced to investigate Singapore's TF threats with officers who are experienced in conducting complex financial investigations. This includes the use of a variety of techniques to identify and investigate TF including the use of financial intelligence, the use of domestic law enforcement tools and undertaking international co-operation. As SPF officers, CFTB officers may exercise powers under the Criminal Procedure Code 2010 to order the production of any document or thing for TF investigations. Through POET, a digital interface between local LEAs and banks, CFTB is able to expeditiously (within 24 hours) access and retrieve banking and financial information for TF investigations. CFTB officers engage with AGC early in TF investigations to obtain guidance in relation to admissible evidence gathering and exploration of leads to achieve positive conviction rates.

551. **STRO** has a dedicated team of analysts reviewing and analysing potential TF STRs and enhancing financial information with other sources of information to produce TF-related financial intelligence bundles. STRO prioritises TF-related bundles and promptly disseminates financial intelligence bundles to both CFTB and ISD upon detection of suspicious TF-related transactions. This dual dissemination enables triangulation of analyses and collaboration between all three agencies as to the course of investigation. STRO makes available automatic dissemination and self-screening to both ISD and CFTB ensuring that they have prompt access to financial information. During 2020-2024, STRO received 1 034 T/TF STRs (1% of total STRs). STRO has not kept statistics for the entire assessment period so it is unclear how many financial intelligence bundles have been disseminated during this entire time period (see IO.6) but, from 2023-24 statistics STRO disseminated 35 financial intelligence packages to CFTB and ISD. Of these 35 packages, four were used to initiate investigations while ten (10) supported ongoing investigations. 48 of the 126 TF investigations in Singapore 2020-2024 were the result of financial intelligence, showing Singapore's dedication to using financial intelligence to combat TF. This demonstrates a good use of financial intelligence to initiate and support investigations.

Table 9.1. Terrorist Financing Investigation Initiators

Initiator	2020	2021	2022	2023	2024	Total
Generated from a domestic terrorism investigation	6	13	11	10	10	50
Financial intelligence	10	5	9	10	14	48
Foreign referral (via ISD)	5	10	1	3	3	22
Foreign referral (via CAD)	4	0	0	0	2	6
Total	**25**	**28**	**21**	**23**	**29**	**126**

Box 9.1. T/TF STR-initiated TF investigation into donations to Al-Qaeda-linked fundraiser

In 2021, STRO concurrently referred T/TF financial intelligence to CFTB and ISD on a Singaporean, Person H, for making two payment transfers to Person I of Country A, for TF and terrorism investigations respectively. CFTB provided information on Person H and the monetary transfers to Country A's FIU and relevant law enforcement authorities through STRO; and concurrently requested for their assistance to provide all available information on Person I. Country A's FIU provided adverse information which helped to confirm Person I as an Al-Qaeda-linked fund raiser, who was arrested in Country A in 2020 for attempting to aid Al-Qaeda.

Based on the actionable financial intelligence from STRO, CFTB conducted a deeper parallel TF investigation to assess if there was a prima facie offence made out under TSOFA. Concurrently, ISD conducted a parallel terrorism investigation, supported by various sources of information such as confidential sources and social media analysis to assess if Person H posed a security threat.

CFTB also interviewed Person H, who confirmed that she had sent the two payments to Person I as a form of charity relief. Person H claimed to be unaware of Person I's background or if she had harboured any undesirable ideologies. In line with the extensive nature of TF investigations by CFTB, further checks were conducted on Person H, which revealed that she had also donated to various other Muslim charities not known to be linked to terrorist entities.

CFTB did not recommend tendering any TF charges against Person H upon the conclusion of its TF investigations and ISD's terrorism investigations, as there was no information or conclusive court-admissible evidence to prove beyond reasonable doubt that Person H knew or reasonably believed of Person I's involvement with Al-Qaeda. Person H continues to be closely monitored by the security agencies. The information provided by STRO also enriched ISD's database intelligence on a third person, Person J (father of Person H's who was already under monitoring by ISD), and Person I.

9.1.2. Investigations identifying the specific role of terrorist financier

552. Singapore initiated 126 TF investigations on 213 natural and legal persons during the reporting period and, at the time of the onsite, had 26 active TF investigations (see table 9.3). While this number may seem high compared to Singapore's assessed risk profile, it reflects a proactive and comprehensive approach to national security. Given the seriousness of TF offences and Singapore's commitment to investigating all intelligence that could relate to TF, this level of activity demonstrates a strong and reasonable stance in safeguarding against potential threats

553. In terms of the role of the TF financier, investigations opened in Singapore since 2020 show that the subject has been the financier for a variety of terrorist organisations. Case studies outlined that the role of the TF financier had been identified along with identification of terrorist financiers in terrorism offences. TF investigations are in line with the risks identified by Singapore in their NRA.

554. Whilst Singapore has identified existing and emerging vulnerabilities, has taken steps to screen potential use of legal persons for TF and has also sought an international perspective and feedback on their exposure to TF exploitation, there is little evidence that Singapore has undertaken proactive investigation to identify organised TF and concealed income. There is also very limited identification and investigation into funds transiting Singapore, for example through across banks and DPTSPs, which pose a medium high risk in the 2024 TF risk assessment.

Table 9.2. Breakdown of TF Investigations by TF Fund Flow Type

	2020	2021	2022	2023	2024
Total No. of TF Investigations	25	28	21	23	29
Type 1: Global TF funds transiting through Singapore for global terrorism activities	0	0	0	0	1
Type 2: Global TF Funds supporting domestic terrorism activities	0	1	0	0	2
Type 3: Domestic TF funds supporting global terrorism activities (possible links to UNSC-designated entities/individuals)	16 (4)	23 (11)	6 (1)	4 (1)	10 (2)
Type 4: Domestic TF funds supporting domestic terrorism activities	0	0	0	0	0
Type 5: Cases involving fund flows through licensed intermediary money remittances disbursing funds to beneficiary institutions (e.g., FIs) in foreign jurisdictions	3	1	4	10	9
Type 6: No funds flow observed	6	3	11	9	7

555. Overall, Singaporean authorities are adept at identifying and investigating TF in line with their understanding of risks. TF investigations are systematically opened when there is a terrorism investigation, financial intelligence and other investigative tools are leveraged, and international information is used appropriately. Singapore's three responsible agencies are able to share intelligence, evidence and information and have the specialised skills to undertake complex financial analysis and investigation. However, there are opportunities to enhance financial investigations to broaden the scope for potential identification of organisational terrorist financing and concealed income.

9.2. Prosecuting and convicting different types of TF

556. Prosecution of TF (and terrorism) offences in Singapore is the responsibility of the AGC, who is well-resourced with competent prosecutors for the volume of TF cases who have demonstrated an ability to prosecute TF cases. AGC works closely with CFTB to ensure that there is sufficient and credible court-admissible evidence before prosecuting individuals involved in TF. This ensures that, by the time charges are tendered in court, there is sufficient admissible evidence to make out the TF offences against the individuals concerned, thereby maximising the chances of successful TF prosecutions and convictions.

Table 9.3. Prosecutions and Convictions of TF

	2020	2021	2022	2023	2024	Total
Number of TF Investigations Opened	**25**	**28**	**21**	**23**	**29**	126
Number of Natural and Legal Persons Investigated for TF	57	62	26	30	38	213
Number of Ongoing Investigations				5	21	
Number of Natural Persons Prosecutions	4	1	1			6
Number of Natural Persons Convictions	4	1	1			6

557. Since 2020, Singapore has prosecuted six natural persons for TF. Whilst this is a low number considering that 213 natural and legal persons were the subject of a TF investigation since 2020 it is due to the low threshold for opening TF cases given the national security implications of T/TF. AGC has a robust internal threshold for bringing a TF prosecution and Singapore has secured a conviction in all six cases, including extra-territorial cases, with five convictions from guilty pleas and one conviction after a full trial where the subject contested the offence before the courts. The facts of a small number of cases were reviewed and the decision to prosecute or not seemed reasonable in those cases. An overwhelming number of cases are resolved through a guilty plea (five out of six). Singapore's approach to bringing prosecutions is viewed as conservative as there likely are some cases where Singapore's AGC has decided that there is insufficient *mens rea* to proceed where they may have succeeded in court. This approach results in fewer potential criminals facing criminal justice.

558. All of Singapore's prosecutions and convictions involve individuals sending small amounts of their salary overseas to support global terrorist activities. The typology for TF in each of these cases is essentially the same but the methods used were slightly different. Each case involved small amounts of money (generally SGD 20 to 100 or USD 15-74) transmitted by individuals residing in Singapore (either Singaporeans or resident workers), from their salaries via legitimate channels (PSPs), to overseas terrorist actors, entities, or sympathisers.

Box 9.2. Case Study: Mens Rea in prosecuting TF

In December 2021, Person A (male Country Z national) was charged in Singapore for providing monies (SGD 891.98) to Entity A and another "charity" campaign in Country S "having reasonable grounds to believe" that the monies would, in part, benefit members of Entity B, a terrorist group in Country S. The money was provided through a remittance service in October 2014.

During TF investigations, Person A consistently took the position that he had no knowledge and did not "know" that the monies he had donated would benefit the terrorist entity (i.e. Entity B).

Given Person A's denials, and bearing in mind the objective-subjective standard for "reasonable grounds to believe", CAD/CFTB worked closely with AGC and conducted investigations focused on demonstrating that Person A possessed the requisite mens rea by establishing the following:

- Person A originally supported the goals of ISIS to establish an Islamic caliphate in Syria. Around mid-2019, Person A changed his allegiance to support Entity B.
- Person A made multiple social media accounts and pages to spread his own views (which involved violence and war). He created multiple social media accounts using temporary email addresses and phone numbers to evade deletion by the social media company.
- Person A bought kitchen knives, pen knives, foldable knives to be "ready for jihad" if religious clashes broke out. He had not conceived any specific plans at the time of his arrest, nor had he intended specific consequences for his actions.
- Person A followed the social media posts of Person B, which publicised (1) that Entity A's hospital purportedly provided medical treatment to all persons in the area; and (2) a purported charity campaign contributing to homebuilding efforts in Country S.
- Person A knew (1) the area the hospital was located in, and (2) the area where the homebuilding efforts were located, were controlled by Entity B and its fighters.

AGC successfully persuaded the court that Person A had "reasonable grounds to believe" that the monies would benefit members of Entity B. Person A ultimately pled guilty to the charges and was convicted on five counts under section 4(1)(b) TSOFA and sentenced to 32 months' imprisonment.

Box 9.3. Case Study: TF trial to sentencing

This is the only trial under TSOFA during the assessment period from 2020 to 2024. The accused (Person A) is a Singaporean who, on 31 October 2014, remitted moneys amounting to SGD 450, through a money remittance service, to an individual in Country X for his publication of Islamic State in Iraq and Syria ("ISIS") propaganda.

Person A did this knowing that the moneys would benefit the ISIS by, amongst other things, garnering more support for ISIS and raising awareness for ISIS. Person A repeatedly stated throughout the trial that he did not recognise Singapore law.

After hearing submissions from AGC, the court convicted Person A. Even though Person A had donated only SGD 450, the court considered the fact that Person A was not remorseful for committing the offence. The court sentenced Person A to a sentence of 33 months' imprisonment.

Table 9.4. Typology of TF Convictions in Singapore

Person	Source of Funds	Typology			
	Salary	Use of PSP	Social Media Appeal for Funding	Foreign Charitable Appeals	Front NPOs
Person A	X	X			X
Person B	X	X			X
Person C	X	X	X		
Person D	X	X			X
Person E	X	X	X		
Person F	X	X		X	

559. Singapore has not yet prosecuted any cases of other TF typologies, such as funds transiting Singapore, that have been highlighted in the TF NRA. As identified above, the TF methods that have been detected in Singapore are fairly unsophisticated and conventional. Singapore is yet to prosecute different types of TF activity. This approach does not fully account for Singapore's risk profile.

560. Overall, Singapore brings few of its TF investigations for prosecution (less than 5%). Whilst the AGC's internal threshold is effective in converting prosecutions to conviction, with a 100% success rate, which leads to the conclusion that the robustness of evidential threshold applied internally by the AGC prior to going to court is impacting on the number of prosecutions that are undertaken. TF activity prosecuted and convicted is relatively unsophisticated, and only partially reflective of Singapore's risk and context.

9.3. Effectiveness, proportionality and dissuasiveness of sanctions

561. Singapore introduced amendments to enhance the sanctions under the TSOFA in 2018.The maximum penalties for natural persons under the TSOFA are a term of imprisonment up to 10 years or a fine of up to SGD 500 000 (USD 370 000), or both. This is comparable to the maximum penalties for other serious offences in Singapore such as corruption, drug trafficking, money laundering, cheating, and human trafficking. Legal persons or entities found to be facilitating TF may be subject to a fine not exceeding the higher of SGD 1 million (USD 740 000) or twice the value of the property involved, whichever is higher.

562. There have been six convictions in the assessed period and all convicted persons received a term of imprisonment upon sentencing, as can be seen in the table below. The Singaporean courts apply general

deterrence principles when sentencing TF offenders which results in substantially longer jail terms for offending involving very small sums contrasted with sentencing for much higher value for offences not involving TF.

Table 9.5. Sanctions Applied

	Amount of TF	Prison Term
Person A	SGD 140	18 months
Person B	SGD 130	24 months
Person C	SGD 450	33 months
Person D	SGD 1 216.73	45 months
Person E	SGD 1 026	46 months
Person F	SGD 891.98	32 months

563. Any foreign persons convicted of terrorist financing offence are deported back to their home jurisdiction once their sentence has been served and the relevant authorities in the home jurisdiction are informed of Singapore's actions.

564. Singapore widely publicises all TF convictions and the corresponding sentences imposed to send a clear message to the public about the consequences of participating in TF.

565. All persons convicted of TF offences and/or detained under the Internal Security Act are designated in the public-facing First Schedule of the TSOFA. A gazette is published (i.e. names published in the First Schedule of the TSOFA) after the issuance of an Order of Detention under the Internal Security Act or conviction under TSOFA, to effect the designation. Consequently, FIs, DNFBPs, and NPOs are prohibited from having financial dealings with these persons and their associates without permission from Singapore's authorities.

566. Singapore's legal framework provides for proportionate and dissuasive sanctions for natural and legal persons involved in TF activity. The small sample of convictions for individuals reflect a good level of intended deterrence in the sentences imposed. Effectiveness and the deterrent (dissuasive) impact upon legal persons is unable to be measured without examples of convictions to consider.

9.4. National counter-terrorism strategies and activities

9.4.1. Formulating national counter-terrorism strategies and activities

567. As a small, connected law enforcement circle, there is almost complete overlap in Singapore with respect to agencies or teams dealing with CFT and CT. This brings cohesion between CTF efforts, including investigations, prosecutions and convictions, and the formulation of national counter-terrorism strategies.

568. The Security Policy Review Committee (SPRC) is the Ministerial-level Committee that reviews national security policies, including CT and CFT policies. Singapore's TF NRA and National Strategy for Countering the Financing of Terrorism (NSCFT) complement Singapore's larger National CT Strategy.

569. The AML/CFT SC is co-chaired by the PSs of the MHA, MOF and MAS, with membership of senior representatives from the security and intelligence, law enforcement, financial intelligence and regulatory agencies, and sectoral supervisors. The common membership of the SC and the SPRC, in particular the role of MHA and STRO in each, contributes to TF risks and CFT strategies being aligned with CT strategies with information from investigations being used to augment Singapore national CT efforts.

570. The inaugural 2020 TF NRA and 2022 NSCFT were reviewed and endorsed by the AML/CFT SC before publication on the MHA, MOF and MAS websites. Both the refreshed TF NRA and NSCFT were similarly reviewed and endorsed by the AML/CFT SC before publication on the MHA, MOF and MAS websites on 1 July 2024.

9.4.2. Sharing and using information and intelligence to support national counter-terrorism purposes and activities

571. Integration across CFT and CT activity at the operational level occurs through the ISD's CT Division, which is also involved in TF-related work (see core issue 9.2). While Singapore has provided evidence of information sharing, across competent authorities and with the private sector, on TF risks generally, there is less evidence that TF investigations and prosecutions are being used to build a deeper understanding of TF networks and organisations, albeit the context of the investigations were used for the NRA and TF threat assessments. In relation to international co-operation, Singapore has demonstrated strength through the sharing of results, where relevant, of its financial intelligence, investigations and prosecutions with international counterparts, through formal and informal channels, and by actively participating and presenting at international fora.

Table 9.6. Singapore's International CFT Information Exchange

	2020	2021	2022	2023	2024
Total T/TF information exchanges with foreign counterparts	1 224	1 467	1 595	2 579	2 353
1a. No. of incoming T/TF Information exchanges (UNSCR 1267-designated individuals / entities)	NA	675 (8)	808 (3)	1 430 (2)	1 481 (13)
1b. No. of outgoing T/TF Information exchanges (UNSCR 1267-designated individuals / entities)	NA	792 (17)	787 (5)	1 149 (2)	872 (59)
2. Total TF Information exchanges with foreign counterparts	18	42	26	129	121
2a. No. of incoming TF Information exchanges (Related to legal persons)	9 (0)	18 (0)	20 (0)	47 (0)	33 (3)
2b. No. of outgoing TF Information exchanges (Related to legal persons)	9 (4)	24 (1)	6 (0)	82 (0)	88 (10)

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

572. Singapore makes limited use of alternative criminal justice and regulatory measures to disrupt TF activity where securing a TF conviction is not practical.

573. Most examples of alternative measures provided by Singapore related to border control measures to prevent terrorists from entering Singapore, deporting foreigners suspected or convicted of TF offences once their sentence is served and implementing counter radicalisation programs rather than disrupting TF activity where a TF prosecution is not practicable.

574. Singapore has used its Internal Security Act (ISA) for preventive detention or restriction of individuals suspected to be involved in TF and terrorism activities if the individual is assessed to present an imminent national security threat to Singapore. Such detentions or restrictions are subject to yearly review by an Advisory Board, chaired by a Supreme Court Judge.

Table 9.7. Number of persons subjected to detention or restriction under the ISA

	2020	2021	2022	2023	2024
# of Persons	5	4	5	2	8

10 Terrorist financing preventive measures and financial sanctions

The relevant Immediate Outcomes considered and assessed in this chapter is IO.10. The Recommendations relevant for the assessment of effectiveness under this chapter are R. 1, 4, 6 and 8 and elements of R.14, 15, 16, 26, 30, 31, 32, 35, 37, 38 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Singapore's framework for proposing designations for TF TFS is capably led by the IMC-TD and appropriately governed by TSOFA.

b) The TSOFA is drafted such that TFS obligation enters into force automatically and immediately following changes to designation. However, there are multiple intermediaries between an alert from the UNSC on changes in listings and dissemination by Singaporean authorities to reporting entities. This has the potential to cause multiple potential points of failure to communicate designations and has caused delays in implementation.

c) During the assessed period, Singapore froze a net value of SGD 1.3 million (USD 962 000) of assets listed under Singapore's domestic TFS regime (i.e. UNSCR 1373), but no assets have been identified or frozen under UNSCR 1267 which does not appear to be in keeping with the risks faced by Singapore.

d) Singapore uses a strong programme of guidance and outreach to mitigate its medium-low risk of TF abuse of NPOs within the FATF definition. The approach is focused, proportionate and not unduly disruptive to the legitimate activities of NPOs in Singapore.

e) FIs and VASPs in Singapore demonstrated a sound understanding of their obligations in relation to TF TFS, including to freeze assets without delay. Understanding of TF TFS obligations across DNFBPs was varied, with scope for improvement across virtually all DNFBPs.

f) Singapore's FI, VASP and DNFBP supervisors do not have appropriate supervisory coverage for TF TFS obligations. FIs and VASPs are subject to a very significant number of controls-based supervisory activities that rectify compliance deficiencies, but it is unknown to what extent they covered TF TFS controls-related deficiencies. There were limited intensive supervisory activities that did. Where there were supervisory activities, a reasonably high TF TFS controls-related

deficiency rate was observed. Identified deficiencies are addressed with non-punitive remedial measures.

g) Despite these obligations being in place for a considerable time and extensive guidance having been issued, TF TFS related compliance deficiencies persist, but relatively weak enforcement action is evident.

Key Recommended Actions (KRAs)

Singapore should:

g) Ensure communication of TF TFS without delay using a more streamlined approach to reach all competent authorities and reporting entities.

h) Use a wider range of information and skill sets including BO information, concealed income analysis and complex network analysis to ensure the funds and assets of natural and legal persons subject to TF TFS pursuant to UNSCR 1267 are identified.

i) Ensure that funds and assets related to TF are immobilised, rather than only immobilising the individual when under investigation for TF offences.

Other Recommended Actions

Singapore should:

a) Ensure that a more appropriate level of supervisory coverage and intensity of TF TFS obligations.

b) Ensure supervisors have mechanisms to systemically address non-compliance with TF TFS and related obligations with proportionate and dissuasive sanctions.

Overall Conclusions on IO.10

Whilst Singapore has a robust legal framework to implement TFS, there are several steps in transmitting information to reporting entities when there are changes in listing. These steps have led to delays in dissemination of updates on TF TFS. FIs and VASPs demonstrated a sound understanding while DNFBPs demonstrated an uneven understanding of their obligations in relation to TF TFS. STRs on TF TFS issues have been increasing in response to concerted outreach and education campaigns by supervisors.

Singapore's NPO regulators, led by COC, collaborate well to provide strong outreach and support to the sector. Singapore mitigates the medium-low TF risk within the NPO sector without unduly disrupting or discouraging legitimate NPO activities.

Singapore produces guidance documents and has good quality outreach in relation to TF TFS. However, Singapore is not systemically identifying and addressing non-compliance with TF TFS through risk-based supervisory activities. FIs and VASPs are subject to a very significant number of controls-based supervisory activities that rectify compliance controls deficiencies, but it is unknown to what extent these relate to TF TFS. There were limited cases of more intensive supervisory examinations that covered TF TFS obligations. In cases of non-compliance,

supervisors are not applying strong measures with lighter, non-punitive sanctions (e.g. reprimands) being applied.

Singapore is rated as having a Moderate level of effectiveness for IO.10.

Immediate Outcome 10

10.1. Implementation of TF-related targeted financial sanctions without delay

575. The IMC-TD is the competent authority responsible for proposing designations to the 1267/1989 and 1988 Committees for designation, and for designations under UNSCR 1373. Singapore has made active use of terrorist designations pursuant to UNSCR 1373. All relevant agencies are included in the process of proposing designations and this domestic process is used effectively to address the domestic terrorism risk faced by Singapore.

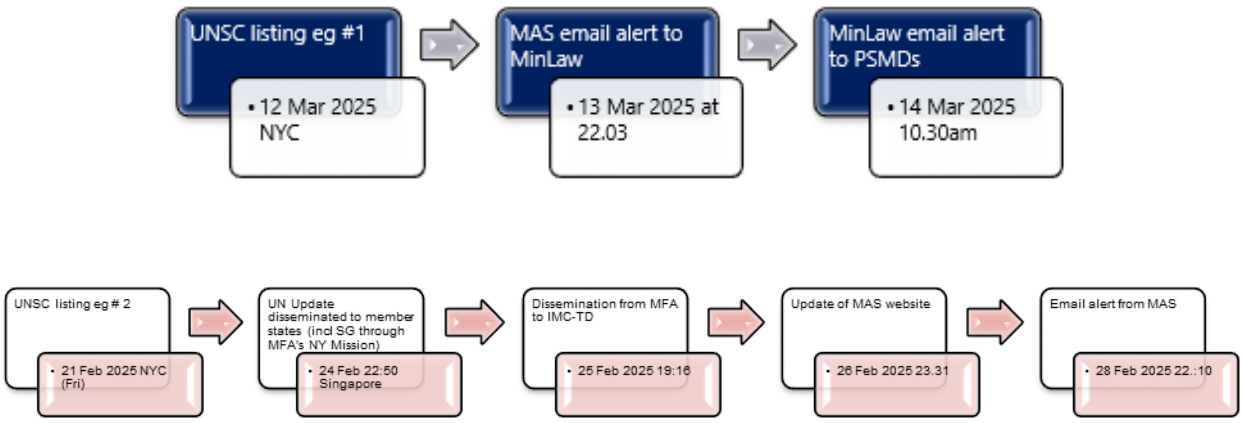
576. Singapore did not submit any designation proposals to the relevant UN Committees or co-sponsor any designations. No requests for co-designation pursuant to UNSCR 1267/1989 and 1988 were made or received by Singapore in the period under review. This is in line with Singapore's risk and context.

577. All UNSC 1267 designations are automatically included in the First Schedule of the TSOFA; however, to take into account the time difference between Singapore and New York, the law only takes effect in Singapore on the date immediately following the date of addition to the UN list. For domestic 1373 designations, the freezing obligation takes immediate effect after gazetting.

578. Singapore's mission at the UN relays listings and changes to the MFA, and these are then transmitted to all agencies and sector supervisors. Singapore's primary mechanism to disseminate information on changes to UNSC lists is via updating the MAS website (for publicly available information) and disseminating to FIs, VASPs and DNFBPs. Through checks during supervisory engagement, MAS has confirmed that all FIs and VASPs are subscribers to the relevant MAS website. Most DNFBP sectors had full subscription to the MAS website, but not all sector supervisors could confirm that the totality of sector their subscribed or used the MAS website. As such, for some sectors, dissemination beyond FIs and VASPs occurs through relevant sector supervisors email alerts to their sector, once they are notified of the designation.

579. MAS has a SOP in place that includes coverage for dissemination over the weekend and a 24-hour work pattern. However, challenges exist in disseminations to other sector supervisors and DNFBPs when the designation is on a Friday due to the time difference. Based on spot checks, there have been instances where Singapore has not disseminated updates on TF TFS without delay, i.e. within 24 hours. Some examples below:

Figure 10.1. Some instances of delays in implementation for Listings/De-listings[38]



580. There are a few intermediaries between a designation from the UNSC and dissemination by Singaporean authorities to reporting entities within the DNFBP sectors created potential points of failure to communicate designations and have caused delays in transmission beyond 24 hours in some instances. Singapore did also provide examples of disseminations to FI and VASP sectors which took place within the 24 hours.

581. Designations pursuant to UNSCR 1373 are initiated by the relevant IMC-TD agencies, and the proposal is then considered by the IMC-TD prior to the Minister for Home Affairs' approval. Once the designation is made, REs are informed via a gazette on the public-facing Singapore Statutes Online website, and email advisories/alerts by MAS and supervisory authorities of DNFBPs within 24 hours. The IMC-TD SOP sets out mechanisms for identifying targets for designation that is based on the designation criteria set out in UNSCR 1373. Under this SOP foreign countries may make requests to Singapore for persons/entities to be designated under UNSCR 1373. Singapore makes good use of domestic sanction legislation under UNSCR 1373 with the system used robustly. To date, Singapore has not received any in-coming designation requests from other countries.

582. The designation process is used as a tool once a person is convicted of TF under TSOFA or detained under the ISA if they are assessed to pose an imminent terrorist threat. Any agency that is part of the IMC-TD will propose a 1373 designation with case facts and evidence of criteria being fulfilled. JOG (as secretariat) will circulate proposal to all agencies for input and the proposal will be authorised by MHA. Whilst this process takes two weeks from receipt of proposal from the originating agency, the person is in custody and to that extent their assets are not accessible by them. Security agencies monitor any movement in their assets during this period. As at September 2024, 46 individuals have been designated and subjected to targeted financial sanctions under the TSOFA pursuant to UNSCR 1373.[39]

583. ISD periodically reviews individuals for delisting based on their rehabilitation progress and threat of relapse into T/TF activities. Listed individuals who are rehabilitated and assessed to no longer pose a threat will be recommended to the Minister for Home Affairs (through the IMC-TD) for delisting. A list of

[38] With respect to the delay in relaying the information to FIs, VASPs and DNFBPs in February 2025, Singapore noted that this was due to several glitches, e.g. MAS officers did not receive UN alerts despite having subscribed to the UN mailing list, delay in dissemination of updates by the UN to MFA.

[39] Approximately SGD 3.97.million (USD 2.9 million) worth of TF assets belonging to 16 individuals listed in the first schedule of the TSOFA, comprising different asset types, have been frozen. This figure represents funds that have been frozen across all time, earlier than 2019 and remain frozen.

persons will be disseminated to FIs, VASPs and DNFBPs on a confidential basis through which they would be subjected to continued supervision.

584. In the latest round of updates in September 2024, 20 individuals were delisted from the First Schedule of the TSOFA and placed on a list of persons disseminated to FIs, VASPs and DNFBPs on a confidential basis.

Box 10.1. Freezing of assets to prevent their use for T/TF purposes

Individual A, a licensed money changer working in Singapore, was arrested and detained under the ISA in May 2019. ISD was alerted to his activities by a foreign partner.

Terrorism investigations conducted by ISD found that he was a follower of an overseas radical preacher, Individual B. Individual B was believed to be part of a militant group in his country and had ties with an internationally designated terror group. He was also identified to be the mastermind of a major terror attack in his country. Investigation established that Individual A had visited Individual B overseas on multiple occasions and donated funds to Individual B and his group. Individual A also harboured a desire to undertake armed conflict overseas.

Upon the discovery of a possible TF element, ISD promptly referred the case to CFTB for deeper parallel TF investigations within three weeks of the commencement of its terrorism investigations. Through detailed deeper parallel TF investigations, CFTB was able to trace his funds and assets and determined that none of the funds/assets were linked to T/TF. Individual A was subsequently listed on the First Schedule of the TSOFA in May 2020 – assets and accounts amounting to SGD 1.9 million (as at end 2023) were frozen and he was prevented from making any further transactions to Individual B or in support of any terrorism-related causes.

10.2. Identification and deprivation of terrorist funds or other assets

585. During the assessed period, no assets have been identified or frozen under UNSCR 1267. Singapore has provided information on one false positive being reported by a FI in 2024 after the September 2024 update to the First Schedule of TSOFA. Given Singapore's status as an IFC the volume of transactions with assets under management around SGD 8.2 trillion (USD 6 trillion) and annual transaction values around SGD 98.2 trillion (USD 72.6 trillion), it is implausible that there are no positive matches and only one negative match. The lack of funds or assets identified under TF TFS is not in line with the risk and context of Singapore.

586. All reporting entities are required to identify funds or assets held by UNSC-designated individuals/entities, as well as those acting on their behalf or under their direction, and report directly to the SPF (S8 and 10 of TSOFA), as well as file an STR on the frozen assets. During the assessment period there were 11 STRs lodged by reporting entities on TF TFS under the UNSCR-regime related to Al-Qaida. In all 11 cases, the reporting entity had suspended the transaction, requested additional information from the customer and also filed an STR and informed the authorities accordingly. The STRs were promptly reviewed and referred by STRO to ISD and CFTB but following investigations, there was insufficient identifiers/information to take any further action. These instances highlight areas for improvement where LEAs could be using a wider range of information and skill sets to identify beneficial owners, or undertake complex network analysis where appropriate, to ensure the funds and assets of natural and legal persons subject to TF TFS are identified.

Table 10.1. Designations and Net Change in Assets Frozen Under Domestic Regime

	2019-20	2020-21	2021-22	2022-23	2023-24
Net change in aggregate value of assets frozen from previous year (SGD, rounded to nearest dollar)	+155 857	+588 118	+122 229	+193 789	-$1 809 079
Number of individuals added/removed from the 1st schedule	8 individuals added	4 individuals added	No change in number of individuals in First Schedule. [NB: the increased value of assets of the listed individuals is due to COVID-related government payouts to all Singaporeans.]		3 individuals added 20 individuals removed from 1st Schedule

587. During the assessment period, Singapore froze a net value of SGD 1.3 million (USD 962 000) of assets listed under Singapore's domestic TFS regime (i.e. UNSCR 1373). Singapore currently has frozen approximately SGD 3.97 million (USD 2.9 million) of assets belonging to 16 individuals listed in the first schedule of the TSOFA. Singapore has shown itself adept at identifying and freezing funds and other assets. The value and types of assets frozen under UNSCR 1373 are in line with Singapore's risk profile.

Table 10.2. Assets Frozen Under UNSCR 1373 at 31 December 2024 by Asset Type

Type of Asset	Value of Assets (SGD, rounded to nearest dollar)
CPF (social security scheme)	793 606
Bank Account Balance	233 776
Property	1 709 888
Investment	926 000
Insurance	303 664
Total	**3 966 934**

588. ISD is the competent authority with responsibility for oversight on frozen assets. ISD is also responsible for any applications for exemptions from freezing. During the assessed period, an average of 240 exemption orders were processed annually. Within ISD there is a team responsible for the rehabilitation of persons designated under TSOFA who continue to monitor and engage with the person and their family as part of their re-integration process. This process is observed to be effective.

589. Individuals under investigation by ISD are provisionally detained as a national security measure. Whilst a person is detained by ISD they are physically prevented from accessing any funds or assets and communication with others is tightly controlled. Their funds and assets, however, remain unencumbered, meaning that those acting on their behalf or at their direction could still have access to the funds/assets while the individual under investigation is provisionally detained. Competent authorities acknowledge that funds and assets could be accessed by third persons, including those acting on behalf of or at the direction of financiers, but there are no known instances of this happening. Should an instance happen, it would be investigated by ISD. Notwithstanding that, this is a significant shortcoming.

10.3. Targeted application of focused and proportionate mitigation measures to at-risk non-profit organisations

590. The NPO sector in Singapore comprises charities, a number of companies limited by guarantee (CLG) and societies, as well as mosques, madrasahs and Wakaf Masyarakat Singapura (WMS), a community wakaf. The Singapore TF NRAs 2020 and 2024 conclude that NPOs pose a medium-low risk of TF abuse.

591. There are four regulatory bodies in Singapore responsible for the supervision for the NPO sector, COC, ACRA, MUIS and ROS. These bodies collaborate well, with COC taking the lead in engagement matters.

592. In line with its risk and context, Singapore uses a strong programme of guidance and outreach to mitigate risk of TF abuse of those in the NPO sector that fit within the FATF definition. The approach is focused, proportionate and not unduly disruptive to the legitimate activities of NPOs in Singapore.

Table 10.3. Breakdown of the number of NPOs by regulator (as of 31 December 2023)

NPO regulator	COC	ACRA	MUIS			ROS	Total
Type of NPO	Charities	CLGs (NPO)*	Mosque	Madrasah	WMS	Societies (NPO)*	2 659
Number of NPOs	2 398	122	70	6	1	62*	

Note: Comprise CLGs and societies that fall within the FATF definition of NPO, but not registered as a charity under the Charities Act 1994 (Charities Act)

593. As of 31 December 2023, there are 2 659 entities falling within the FATF definition of NPO of which approximately 200 have been identified as the high-risk subset. During the assessment period, there were no cases of NPOs in Singapore being misused for TF. Factors taken into account in determining vulnerability of NPOs in the charity sector are:

a) involvement in overseas operations and activities;
b) awareness of risks of abuse for TF;
c) implementation of due diligence measures;
d) implementation of monitoring mechanisms to maintain and promote accountability and transparency; and,
e) use of regulated financial channels.

594. The identified high-risk subset could be categorised as one that is providing humanitarian aid and religious groups based in high-risk jurisdictions, conflict zones or neighbouring jurisdictions.

595. The NPO sector in Singapore is domestically focused, and within the NPO sector, the charity sector (under the purview of the COC) with relatively higher exposure to overseas activities is assessed to be more vulnerable to TF abuse with a medium-low vulnerability. The remaining NPOs under ACRA, MUIS and ROS are assessed to be of low vulnerability of TF abuse.

596. Singapore adopts a risk-based approach to regulating and monitoring the NPO sector, in which higher-risk NPOs are subjected to focused measures such as additional disclosure requirements, screening and targeted outreach.

597. All NPOs are subjected to baseline regulatory requirements to promote accountability and integrity in the administration and management of NPOs, which include the need to apply for registration and file annual submissions. NPOs are also required to notify their regulators of any changes in information related to their entities, such as changes in the constitution, place of operation and composition of their key office bearers. In addition, the accounts of NPOs are required to be audited or independently examined in accordance with the statutory requirements under the relevant legislation to promote credibility of the financial information presented by the NPOs. Regulators also conduct background screening on all key office bearers of NPOs, including against the list of designated/sanctioned individuals pursuant to TF.

598. Singapore's monitoring and oversight of NPOs is risk-based, focusing on activities that have factors creating vulnerability of TF abuse in NPOs. Primarily this relates to activities by charities that are fundraising to spend, remit or disburse funds to locations outside Singapore. Charities fundraising for foreign charitable purposes are required to apply for a Fundraising for Foreign Charitable Purposes (FRFCP) permit, disclose

information regarding the quantum and countries where such funds are applied, as part of their annual submissions.

599. The administration of the FRFCP is risk-based, with greater scrutiny placed on applications which involve foreign beneficiaries, partners and/or foreign NPOs located in high-risk jurisdictions and conflict zones/regions. All persons or entities raising monies for any foreign charitable purpose, must apply for FRFCP permits. Approximately 70 permits per year are approved once the COC has completed due diligence on beneficiaries utilising relevant competent authorities. During the assessed period only one application was refused, due to deficiencies in the documentation submitted.

Box 10.2. Case Study: Targeted measures for the protection of charities that may be deemed at higher risk of TF

In November 2023, MHA alerted COC to a fund-raising appeal conducted by a registered charity ("Charity A") to provide humanitarian relief to the affected victims of an ongoing conflict in the Middle East, through an overseas partner entity. MHA highlighted that the social media post of Charity A contained information that appeared to suggest that part of the donations from the appeal would be used to support a foreign party to the conflict. The COC found that Charity A had failed to apply for FRFCP permit prior the fund-raising appeal.

In response to inquiries from MHA and COC, Charity A removed all social media posts related to the appeal. Charity A agreed to work with the COC to rectify its non-compliance before resuming further disbursement of donations. In due course, an appropriate FRFCP permit was issued to Charity A to continue its fundraising activities.

600. The COC adopts a pro-active approach in uplifting the capabilities of charities to mitigate the risks of TF abuse and has dedicated additional resources to provide guidance and targeted outreach, particularly, for identified higher-risk charities.

601. Guidance materials are produced in a co-operative manner with formal partnerships established via MOUs, whilst collaboration with other partners is established through goodwill arrangements.

602. Partnerships and collaboration in place with other sectors such as lawyers and accountants to enable the guidance materials to be targeted and relevant. Material produced is innovative and timely including the use of webinars and YouTube to ensure they are targeted at as wide an audience as possible. Panel discussions take place with experts to discuss best practice, again aimed at reaching a wide audience.

Box 10.3. COC guidance to higher-risk charities

In December 2024, COC designated a small group of charities for a pilot scheme to encourage charitable giving towards foreign charitable causes beyond Singapore. Tax deductions are granted for qualifying overseas cash donations that have been made through these designated charities towards emergency humanitarian assistance.

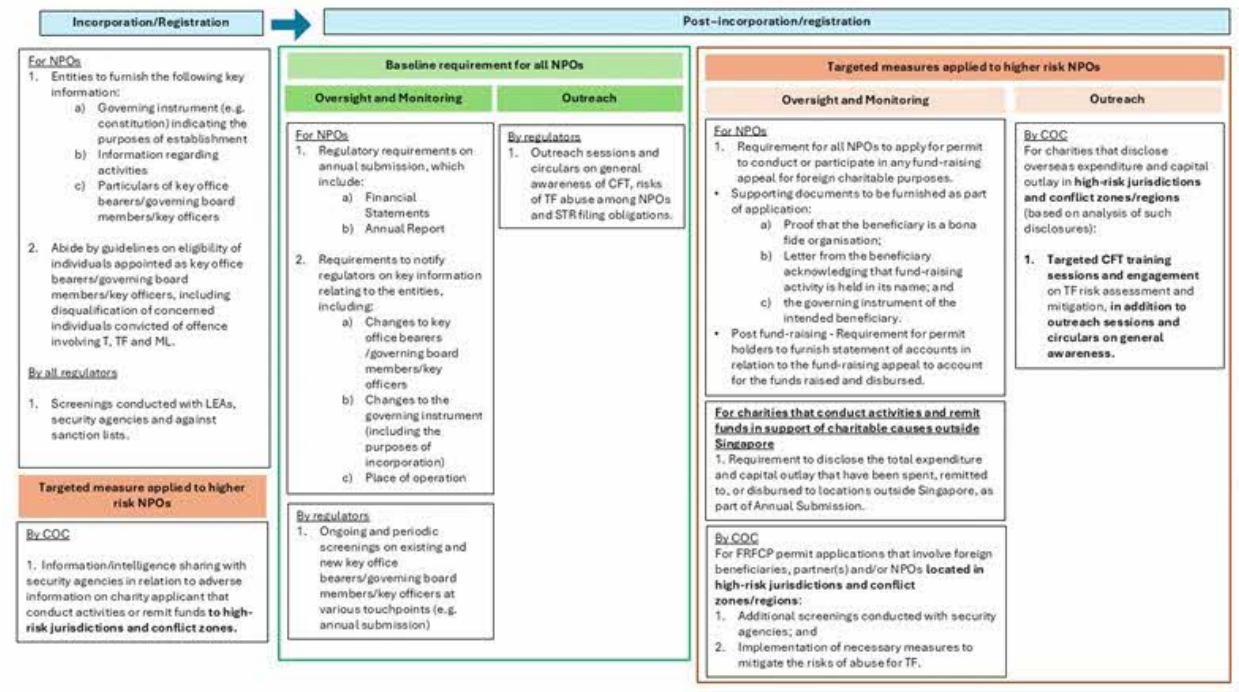
Given the increased inherent risks of operating in disaster-stricken and/or conflict regions, these designated charities were required to furnish documented policies and procedures to demonstrate that they have implemented mitigating measures against illicit fund flows. During the assessment process, the COC guided charities on areas of improvement in their policies and procedures to better safeguard their organisations against the risks of TF abuse, through targeted engagement.

603. MUIS conducts periodic updates for Mosque Management Board (MMB) and school leaders on mosques and madrasahs financial policies and procedures, including matters relating to TF risks and abuse. MMBs attend such trainings regularly at the start of each term of appointment and during re-appointments.

604. ROS has published a Code of Governance for Registered Societies that provides best practices to societies in carrying out their duties, managing society funds and properties, and a Guidance Note - Protecting Your Society against Money Laundering & Terrorist Financing (AML/CFT Guidance Note for Societies) on its website since June 2015. Annually, ROS also issues email advisories to the societies about AML/CFT resources and encourages the societies to circulate such information to its members, staff, and volunteers to create awareness.

605. The diagram, below outlines the risk-based approach, providing an overview of the baseline statutory requirements that apply to all NPOs and the additional measures that are targeted at higher-risk NPOs.

Figure 10.2. Oversight and Monitoring of NPOs



Box 10.4. COC's Terrorist Financing Risk Mitigation Toolkit for Charities (2023)

In February 2023, the COC launched a Terrorist Financing Risk Mitigation Toolkit for Charities (the Toolkit), which comprises a step-by-step risk assessment framework and recommended mitigating measures, to guide charities in identifying TF risks, assessing the level of risks, prioritising and mitigating the identified risks in a systematic manner.

The Toolkit was co-developed with charities and industry professionals, where the COC engaged the higher risk charities through focus group discussions. These charities were guided by a team of consultants to complete a mock risk assessment based on the draft Toolkit and they also provided feedback to enhance the utility of the Toolkit. The COC adopted some of the feedback from the participants, one of which is the inclusion of checklists in the Toolkit to provide additional guidance on the key considerations that charities should take note of when conducting their risk assessments.

Following the launch of the Toolkit, the COC rolled out training sessions that were targeted at higher risk charities, in particular the religious charities that conduct and support overseas activities and charitable causes, and charities that facilitate humanitarian and disaster relief work, in high-risk jurisdictions and/or near conflict zones.

606. COC conducts annual Safer Giving campaigns targeting the donor community, including material on verifying the beneficiary and purpose of donations educating the public on TF risks and how to donate safely to NPOs.

607. NPOs with high, medium and low risk profiles indicated that they had limited concerns about Singapore's regulations being overly onerous or preventing them from conducting legitimate charitable activities. NPOs provided positive feedback on the outreach of the COC and the collaborative approach employed by regulators. There was, however, some concern in relation to the delay for FRFCP permits where funds were needed urgently for foreign charitable purposes (e.g. in natural disaster events).

10.4. FIs, VASPs and DNFBPs understanding of and compliance with obligations

10.4.1. FIs and VASPs

608. FIs and VASPs met by the Assessment Team in Singapore demonstrated a sound understanding of their obligations in relation to TF TFS, including to freeze assets without delay. FIs and VASPs actively screen for designated individuals and entities and freeze immediately where required. FIs and VASPs have developed their understanding through guidance, tools and outreach/engagement events.

Box 10.5. Case Study: Virtual Asset donation to campaign of terror group

On 30 August 2023, Company A, a DPTSP, detected a cryptocurrency transfer of more than USD 4 000 by a Singaporean account holder (Person T) to a wallet associated with donation campaigns to a terror group designated by many countries. The wallet allegedly belonged to a foreign national who was being investigated by a foreign counter-terrorism agency (Agency X) for TF offences. Foreign Agency X had, through an Administrative Order dated 30 June 2021, sanctioned and seized the wallet.

These transactions were flagged by a blockchain analysis firm engaged by Company A to monitor third-party transactions on their platform. Company A immediately suspended the transaction on the same day and filed an STR the following day, on 31 August 2023.

609. MAS and MinLaw have provided extensive guidance products to all FIs and VASPs. The reporting entities were readily able to provide details on the guidance and how they implemented it into their systems. This demonstrates that the reporting entities understand and, in general, comply with their obligations.

610. All FIs and VASPs are subscribed to MAS' webpage, which provides updates on 1267 and successor resolution designations. In addition to subscribing to the MAS webpage and using it as a source of reference, FI and VASPs also rely on updates directly from the UN website of consolidated lists and/or are subscribed to various commercial databases to enable them to perform screening against updates to the relevant UNSCR lists. All FIs and VASPs indicated that they are subscribed to mailing lists by their supervisor that provides them with updates on national designations. The AT cannot conclude that those acting on behalf of or at the direction of designated persons and entities are being captured by screening practices.

611. Outreach has been conducted by the supervisors, and this are in line with the risk and context of Singapore. These outreach sessions, including as webinars to provide accessibility, are aimed at supporting the reporting entities in understanding their obligations in relation to TFS. Outreach has increased greatly in the last two years.

Table 10.4. Outreach Sessions (Including but not limited to TF TFS)

FI/VASP	2020	2021	2022	2023	2024
Banks	11	5	10	17	25
DPTSPs	9	2	12	13	24
PSPs with CBMT services	7	1	12	13	24
Other FIs	73	17	113	176	297

612. Overall, the number of STRs in relation to TF TFS have increased across the sectors which would suggest that the outreach efforts that are taking place are making a positive impact.

10.4.2. DNFBPs

613. DNFBPs in Singapore demonstrated an uneven understanding of their obligations in relation to TF TFS, including to freeze assets without delay. Some DNFBPs actively screen for designated individuals and entities and freeze immediately where required, while others, which became apparent during interviews with entities at the onsite, were unsure of their obligations and what to do if there was a positive match.

614. All DNFBP sectors have been provided with sector-specific guidance, but the degree of familiarity with the guidance varied from entity-to-entity. Singapore has been gradually conducting more outreach activities, which DNFBPs viewed as positively contributing to their awareness.

Table 10.5. Outreach Sessions (Including but not limited to TF TFS)

DNFBP	2020	2021	2022	2023	2024
Casinos	2	0	2	0	6
EAs/Developers	11	4	3	11	2
PSMDs	21	38	24	21	27
Law Firms	10	8	11	16	27

DNFBP	2020	2021	2022	2023	2024
CSPs	3	6	4	4	9
Accountants	2	2	3	2	5
Moneylenders	2	2	0	3	10
Pawnbrokers	3	2	4	3	9

615. Overall, the number of STRs in relation to TFS have increased across the sectors which would suggest that the outreach efforts that are taking place are making a positive impact. For example, following MinLaw's industry engagement session in May 2024 and regular outreach, authorities noted an increase in understanding of TF risk and TFS preventive measures amongst the PSMD sector (from 81% to 93%) and 9% increase for both the moneylending (from 87% to 96%) and pawn-broking sector (from 84% to 93%), as assessed through questionnaires administered prior to and after the outreach session. 99% of PSMDs, and 100% of pawnbrokers and moneylenders found the sessions useful.

616. In the period under review, all reporting entities combined to lodge 111 STRs (4% of total T/TF-related STRs filed) relating to TF TFS under UNSC sanctions regimes. When making such an STR submission, FIs, VASPs and DNFBPs will place a hold on these accounts/transactions. STRO has in place mechanisms to pick up such STRs through the STR form's structured fields that indicate whether measures have been taken in relation to the account/transaction. The mechanism for reporting a potential match through an STR is flawed as it does not always result in timely action. The process of reporting entities lodging STRs may involve a longer time than is ideal for TFS match confirmation. Further, it is not clear that in instances of unconfirmed matches by DNFBPs the assets are being frozen while veracity of the identify is confirmed.

10.5. Competent authorities monitoring and ensuring compliance with TF-related targeted financial sanctions

617. Singapore's framework for monitoring regulated entities' compliance with TFS is built into its broader supervisory settings. Supervisors monitor compliance with TF TFS as part of onsite and offsite supervisory activities on a rules-based approach, including by reviewing data submissions from reporting entities.

10.5.1. FIs and VASPs

618. As identified in IO.3, MAS supervises the implementation of TF TFS through supervisory activities that are initiated by three approaches: (1) controls-based, (2) FIRA-based or (3) risk surveillance-based.

619. Controls-based supervisory activities are targeted scope supervisory activities where MAS has become aware of a compliance issue through the review of internal/external audit reports, the review of STRs etc. In these cases, MAS promptly follows-up with the FI/VASP to rectify the issue.

Table 10.6. Number of Controls-based Supervisory Activities

Sector	2020	2021	2022	2023	2024	Total
Banks (155)	401	469	394	463	440	2167
DPTSPs (29)	0	6	9	23	20	58
PSPs with CBMT services (199)	20	25	22	67	89	223
Other FIs (2139)	386	339	296	314	219	1 554

620. Singapore places great reliance on controls-based supervisory activities – they represent approximately 95% of total supervisory activities. However, given the targeted and less formal nature of

these supervisory activities, there are no statistics on exactly what scope these supervisory activities covered. It is known that these activities took place, and if there was a compliance issue it was generally either rectified or escalated to a more intensive supervisory activity. There is no information to demonstrate how, and to what extent, these controls-based supervisory engagements incorporated TF TFS obligations. Some credit must be given to Singapore for the supervision of TF TFS requirements through these controls-based supervisory activities but because of the unknown scope, the assessment team must be conservative in taking these into account.

621. As outlined in IO3 Singapore also conducts full scope or more intrusive examinations through its other two supervisory approaches, FIRA-based or risk surveillance-based supervisory activities. These include vetting policies and procedures, reviewing sanctions screening activities, testing alerts, checking freezing/blocking requirements, overseeing transaction monitoring and reporting of matches.

Table 10.7. Number of Intensive Supervisory Activities (Including but not limited to TF TFS)

FI/VASP	2020	2021	2022	2023	2024	Total
Banks (155)	5	9	2	10	0	26
DPTSPs (29)	0	0	3	5	0	8
PSPs with CBMT services (199)	2	5	0	38	43	88
Other FIs (2139)	11	4	2	3	3	23

622. Over the course of the assessment period, there was limited known coverage of intensive supervisory activities related to TF TFS for FI and VASP sectors. Where there were intensive supervisory activities, there was a reasonably high deficiency rate with 56 TFS-related deficiencies (for the period 2020 to 2024) from those 141 examinations. The large majority of deficiencies were uncovered by MAS through its risk surveillance approach. The deficiencies mostly related to more specific AML/CFT control and process failures which include screening of clients against sanction lists.

Table 10.8. No of TF TFS-related Compliance Deficiencies (number of sanctions)

Year	FIs	DPTSPs	Casinos	EAs/Developers	PSMDs	LPEs	CSPs	PAEs	Money-lenders	Pawn-brokers	Total
2020	22(7)	0	2	0	0	0	0	0	0	0	24(7)
2021	15(1)	0	5(4)	0	0	0	1(1)	0	0	0	21(6)
2022	8(1)	0	0	0	0	0	1(1)	0	0	0	9(2)
2023	5	0	3(2)	0	0	0	0	0	0	0	8(2)
2024	5(1)	1	1	6(1)	1	0	7(7)	0	0	0	21(9)
Total	55(10)	1	11(6)	6(1)	1	0	9(9)	0	0	0	83(26)

623. In response to this level of deficiency, MAS conducted a series of thematic reviews in 2021 and 2022 to assess reporting entities' TF risk understanding and examine the effectiveness of their CFT-related controls. Following which, MAS published a guidance paper ("Strengthening Financial Institutions' CFT Controls") in May 2023, to set out MAS' key observations and supervisory expectations of CFT controls. In addition, MAS also conducted thematic examinations on FIs' (including banks) name screening processes in 2021 and issued an information paper to FIs on "Strengthening AML/CFT Name Screening Practices" in April 2022.

624. Supervisors have largely addressed detections of TF TFS-related deficiencies (83 in the period under review) through lighter, non-punitive remedial measures (e.g. reprimands), though punitive sanctions (e.g.

fines or suspension or revocation of licenses) have also been meted in 10 cases involving more serious offences, including non-compliance with TF TFS-related obligations. This is reflective of Singapore's lighter approach preferring remedial measures to sanctions (see IO.3 and IO.4).

625. Overall, Singapore's FI and VASP supervisors do not have appropriate supervisory coverage for TF TFS obligations but identify a reasonably significant amount of non-compliance regardless. Supervisors are addressing deficiencies generally with non-punitive remedial measures.

10.5.2. DNFBPs

626. As identified in IO.4, all DNFBP supervisors implement risk-based supervision to ensure DNFBPs are complying with their AML/CFT requirements. SC/IAC's guidance on supervisory coverage indicates that all high risk DNFBPs (around 90%) and medium-high risk DNFBPs (around 70%) should be subject to a supervisory activity over a period of two to four years – 90% were in the case of high risk and 70% were in the case of medium-high risk. Where examinations are undertaken by supervisors, they generally include an element on TF TFS. As noted above and in IO.3/IO.4, there are deficiencies in the risk-basis of the approaches adopted by MAS and MinLaw, and gaps in the supervisory coverage of MAS, URA and CEA. When conducting supervisory activities, supervisors generally seek confirmation that the reporting entity has registered with MAS and have other commercial software to be alerted to changes in TF TFS. Supervisors were not able to confirm that DNFBPs had ready means to ensure compliance with TF TFS.

Table 10.9. Number of Supervisory Activities (including but not limited to TF TFS)

DNFBP	2020	2021	2022	2023	2024
Casinos (2)	6	2	2	4	2
EAs/Developers (1243)	12	24	2	3	33
PSMDs (1967)	218	136	209	241	191
Lawyers (7400)/LPEs (1161)[40]	50	50	50	52	24
CSPs (2883)	109	379	367	300	417
Accountants (4465)	32	55	14	10	10
Pawnbrokers (241)	61	60	60	60	60

627. Supervisors are addressing deficiencies generally with remedial measures although there are other stronger measures available to them. Overall, despite obligations having been in place for decades, a sophisticated audience of reporting entities, and comprehensive guidance, compliance deficiencies persist, but relatively weak enforcement action is evident.

Box 10.6. DNFBP STR filing at sanctions hit

In 2023, a PSMD filed an STR as its internal screening, post-transaction, detected that a customer (Person A) was designated under the 1st schedule of the TSOFA. In this case the PSMD did not screen the customer prior to the transaction, and as such did not identify the match or refuse the transaction. After the transaction, the PSMD lodged an STR. MinLaw deemed this to an appropriate response as the entity recorded the customer's particulars; and conducting post-transaction screening in line with its internal procedures.

[40] Lawyers are covered through LPE examinations as lawyers can only practice through LPEs.

11 Proliferation financing financial sanctions

The relevant Immediate Outcome considered and assessed in this chapter is IO.11. The Recommendations relevant for the assessment of effectiveness under this chapter are R. 7 and elements of R.1, 2 and 15.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Singapore has a strong legal framework for PF TFS obligations, with the AML/CFT SC providing co-ordination and policy leadership allowing Singapore to convene quickly to discuss PF issues and co-ordinate as needed.

b) Singapore's 2024 PF NRA identifies its PF TFS risks. The threats, vulnerabilities and risks have largely been appropriately identified but it could be strengthened with more granular data, specific to Singapore's context. General and high-level mitigation measures are set out in the PF NRA report and Singapore's CPF Strategy. These measures are general, not proportional to risk and largely already being conducted as part of Singapore's CPF regime. Singapore's PF NRA highlights higher risk areas that have no or negligible mitigation measures identified.

c) The communication mechanisms and obligations for PF TFS are identical to what is described under IO.10 for TF TFS. There have been some instances over the assessment period where processes were not able to react without delay.

d) Singapore's FIs and VASPs broadly have a good understanding of their obligations to comply with PF TFS, and most subscribe to commercial sanctions-screening software. DNFBPs demonstrated an uneven understanding of obligations and lacked insights into complex PF TFS evasion techniques. The AT cannot conclude that those acting on behalf of or at the direction of designated persons and entities are being captured by screening practices.

e) Reporting entities submit large numbers of PF-related STRs (around 1 900 STRs during the assessment period), of which 732 STRs were confirmed to relate to the DPRK. Over 1100 PF-related STRs have been disseminated as Fin-IRs to competent authorities.

f) Singapore's AGC successfully prosecuted 22 natural persons and eight legal persons for PF-related/proliferation-related breaches of Singapore's UN (Sanctions – DPRK) Regulations and other export control regulations. No natural or legal persons have been prosecuted for PF TFS breaches. SGD 22.3 million (USD 16.2 million) has been frozen in one case during the reporting period. No assets have been identified or frozen in other cases during the reporting period, which does not accord with Singapore's risk and context.

g) Representation offices of foreign flag States operating in Singapore which the AT met during the onsite have a very low awareness of their PF TFS obligations. The main mitigation measures imposed on these representation offices of foreign flag States are the requirement to comply with Singapore's UN DPRK Regulations and Singapore authorities' outreach to them; however, the entities appear not to be complying with their obligations, and the outreach has been very recent.

h) Singapore's FI, VASP and DNFBP supervisors do not have appropriate supervisory coverage for PF TFS obligations. FIs and VASPs are subject to a very significant number of controls-based supervisory activities, but it is unknown to what extent they covered PF TFS. There were limited intensive supervisory activities that did. Where there were supervisory activities, a reasonably high deficiency rate was observed. Identified deficiencies are generally addressed by lighter remedial measures and sanctions.

i) Penalties for breaches or failure to comply with CPF-related obligations are relatively low and cannot be considered proportionate and dissuasive in all cases.

Key Recommended Actions (KRAs)

Singapore should:

j) Improve supervisory coverage and intensity, and engagement specific to PF TFS for higher risk sectors, particularly VASPs and CSPs.

k) Deepen context-specific understanding of PF TFS evasion risks and implement further risk and context-specific risk mitigation measures.

l) Increase PF TFS engagement with representation offices of foreign flag States to increase awareness of obligations and the risks associated with DPRK-related financial flows and complex PF TFS sanctions evasion techniques.

Other Recommended Actions

Singapore should:

a) Increase the systematic use of PF-related financial intelligence by LEAs to initiate enforcement activities that prevent designated persons and entities from operating or executing financial transactions related to proliferation in Singapore's financial system.

b) Enhance enforcement action, including the issuance of proportionate and dissuasive penalties, to address non-compliance with PF TFS obligations, including for the failure to take reasonable measures to detect the evasion of PF TFS, where appropriate.

Overall Conclusions on IO.11

AML/CFT SC, IAC and RTIG are the primary AML/CFT/CPF policy co-operation mechanisms in Singapore, and the IMC-EC leads Singapore's counter-proliferation and export controls regime and plays an active role in Singapore's PF (including PF TFS) risk mitigation. All mechanisms can convene quickly to co-ordinate and discuss PF issues, and develop policy as needed. Singapore's ban on trade with the DPRK in 2017 has had a positive impact on its overall risk exposure to the DPRK but the risk to Singapore

remains higher due to its context and the nature of its economy. Operational co-ordination among MAS, Singapore Customs, LEAs and other relevant authorities is strong when needed.

Singapore's PF NRA appropriately identifies the headline threats, vulnerabilities and risks but there is insufficient detail and nuance on the level of exposure that Singapore has to PF. Mitigation measures set out in Singapore's CPF Strategy are general, not proportional to risk and largely already being conducted as part of Singapore's CPF regime. Singapore's PF NRA highlights higher risk areas that see no or negligeable mitigation measures.

Singapore's FIs and VASPs broadly have a good understanding of their obligations to comply with PF TFS, and most subscribe to commercial sanctions-screening software. DNFBPs demonstrated a mixed understanding of PF TFS obligations, and representation offices of foreign flag States operating in Singapore have a very low level of understanding of their obligations. Reporting entities have filed a very significant number of PF-related STRs with STRO. Singapore has successfully prosecuted 22 natural persons and eight legal persons for PF-related/proliferation-related breaches of Singapore's UN (Sanctions – DPRK) Regulations and other export control regulations. Assets amounting to SGD 22.3 million (USD 16.2 million) have been frozen in one case within the reporting period. No assets have been identified or frozen in other cases within the reporting period. This does not accord with Singapore's risk and context.

Singapore has undertaken outreach activities to assist most at-risk reporting entities understand their obligations and the risk mitigation measures they should put in place. FIs and VASPs are subject to a very significant number of controls-based supervisory activities that rectify compliance controls deficiencies, but it is unknown to what extent these relate to PF TFS. There were limited cases of more intensive supervisory examinations that covered PF TFS obligations. In cases of non-compliance, supervisors are not applying strong measures with lighter, non-punitive sanctions (e.g. reprimands) being applied.

Singapore is rated as having a Moderate level of effectiveness for IO.11.

Immediate Outcome 11

11.1. Competent authorities' co-operation and co-ordination to combat PF

628. Singapore's legal framework for PF TFS has largely remained the same since the previous ME. Singapore uses the same approach to monitor and ensure that FIs, DNFBPs, and VASPs comply with their obligations related to PF TFS as it does for TF TFS (see IO.10). Singapore has maintained the relevant Regulations (applicable to FIs, DNFBPs, VASPs and all other persons) relating to the DPRK. While outside the reporting period for the ME, Singapore imposed a complete ban on trade with the DPRK in 2017. This trade ban (which goes beyond the DPRK UNSCRs) covers trade with the DPRK, any person in the DPRK and any DPRK national. The DPRK trade ban has lessened Singapore's FIs', VASPs' and DNFBPs' exposure to the DPRK but Singapore remains as having a relatively high level of PF risk.

629. In 2024, Singapore published a PF NRA with an associated CPF Strategy. Singapore has a number of contextual factors and attributes which make it one of the jurisdictions most vulnerable to PF: its geographical position, and its status as an IFC, and a hub for trade, transport, maritime and virtual assets.

11.1.1. Co-operation and co-ordination to develop and implement policy

630. The AML/CFT SC is the main co-operation and co-ordination body for the development and implementation of AML/CFT/CPF policy in Singapore, alongside their subsidiary committees, IAC and RTIG. Specifically for PF, these committees work closely with the IMC-EC, the key policy and operational co-ordination mechanism for the implementation of the UNSCRs pertaining to PF. The IMC-EC, through the Permanent Mission of the Republic of Singapore to the United Nations in New York, is also Singapore's focal point for sanctions-related engagements with the UNSC, including the relevant UNSC Panels of Experts.

631. The AML/CFT SC is the principal CPF policy lead, with the IMC-EC responsible for Singapore's export controls framework. The IMC-EC is chaired by the MFA and comprises the AGC, CAD, MPA, MINDEF, MHA, MinLaw, MTI, MAS and Singapore Customs. The IMC-EC has met annually to plan and discuss key strategic issues for the year ahead, and in practice, also meets more regularly on an ad hoc basis to discuss specific issues (including policy issues and cases); for instance, it had 21 ad hoc meetings in 2024 and 12 in the first half of 2025.

632. CPF policy issues are discussed through the same mechanisms as AML and CFT policy issues, and robust co-operation and co-ordination methods are one of Singapore's key strengths (see IO.1). For CPF, Singapore has co-ordinated well in relation to the 2024 PF NRA with respect to emerging sanctions risks and in the development of its CPF Strategy. The RTIG has discussed PF once per year, on average, particularly in relation to the misuse of legal persons and virtual assets, which have been identified as key PF threats in Singapore's PF NRA. PF has also been discussed at the ACIP and identified as one of three priority areas under COSMIC which facilitates private-to-private information sharing among six major commercial banks in Singapore. COSMIC enables these FIs to securely share information on customers that exhibit multiple red flags which may indicate possible PF concerns. Singapore has explained that it had limited changes in its CPF policies relating to the DPRK during the reporting period as it has given largely compliant effect to TFS in relevant UNSCRs through its domestic legislation and has imposed the DPRK trade ban in 2017. In 2021, key policy decisions were taken to cover PF under COSMIC, and for sector supervisors to explicitly require FIs, VASPs and DNFBPs to conduct PF risk assessments and apply appropriate risk mitigation measures (despite these already being covered by existing AML requirements). The mechanisms described above have shown an ability to convene quickly and co-ordinate as needed to discuss PF issues and develop and implement policy as needed.

11.1.2. Co-operation and, where appropriate, co-ordination for operational purposes

633. The IMC-EC and AC3N are the key CPF co-ordination bodies for operational purposes. The IMC-EC co-ordinates interagency follow-ups (including enforcement action by law enforcement) when Singapore receives information or intelligence from foreign counterparts relating to the proliferation of WMD and its associated financing. When the IMC-EC comes across information that relates to CPF policy issues and PF risks, it can refer the information to the IAC or RTIG respectively.

634. Over the reporting period, the IMC-EC has met on a number of occasions to discuss proliferation and PF issues. The AC3N may also deal with non-export control PF cases surfaced by AC3N agencies, and it (or its predecessor, ISTRA) has considered PF cases throughout the reporting period. SGD 33.4 million (USD 24.7 million) of assets (to-date) have been frozen in Singapore, with SGD 22.3 million (USD 16.2million) in the reporting period (see Box 11.2), demonstrating operational co-ordination among MAS, Customs, LEAs and relevant authorities when needed.

635. As evidenced by Table 11.3, Singapore authorities have increasingly prioritised regular engagements with private sector stakeholders to enhance their awareness and compliance, including non-

reporting entities such as those from the maritime sector. MPA and MAS have only recently begun engaging representation offices of foreign flag States in Singapore to raise their awareness of and compliance with their obligations.

636. Overall, as with AML/CFT, co-operation and co-ordination for operational and policy issues related to PF in Singapore is a strength.

11.2. Understanding and mitigating the risk of breach, non-implementation or evasion of PF-related targeted financial sanctions

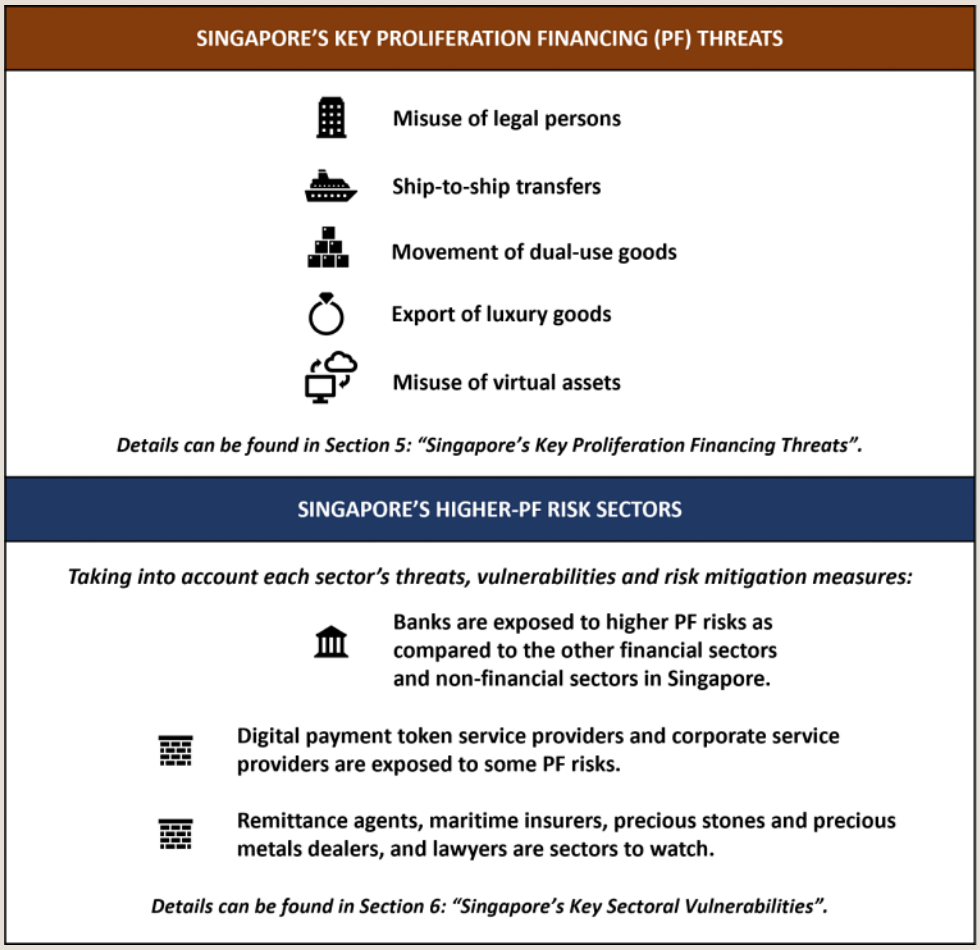
637. PF risks are monitored through the RTIG, overseen by the AML/CFT SC. Singapore recently published its first PF NRA report and an accompanying National CPF Strategy in 2024. Singapore's PF NRA built on existing guidance and industry engagements, and covered the risks of breaches, non-implementation and evasion of all sanctions imposed on the DPRK and Iran, including activity-based sanctions (i.e. broader than the scope of the FATF Standards). The NRA process involved all relevant competent authorities, including ACRA, AGC, CAD, MFA, MHA, MinLaw, MAS and Customs, overseen by the RTIG. The ACIP was also consulted, with a specific CPF Working Group gathering feedback from financial and non-financial sectors.

638. Singapore's PF NRA assessed risks based on threats, vulnerabilities (with reference to possible exploitation) and consequences. Key data included PF investigations, proliferation investigations, PF-related and sanctions evasion-related STRs, PF-related intelligence, PF-related requests for formal and informal international co-operation and international typologies (including those from the UNSC Panel of Experts). Singapore conducted sectoral vulnerability assessments, factoring in CPF controls and industry feedback, and consulted international partners. The NRA was shared with private sector stakeholders through existing supervisor communication mechanisms, including alerts, circulars and industry outreach.

639. Singapore's PF NRA methodology is reasonable. Although the PF NRA does not use the same terminology as the ML and TF NRAs, Singapore explained that the terms used in the PF NRA (i.e. "Higher PF risks", "Some PF risks" and "Sector to watch" as set out in Box 11.1 below) correspond to "High", "Medium-High" and "Medium-Low" in the ML and TF NRAs respectively. Singapore explained that a different approach was taken to better support industry's focus on the substance of the PF NRA since assessing PF risks is a relatively new obligation. Singapore is credited with trying to support the private sector's implementation of a new obligation but these differences in terminology make it less likely for the private sector to be able to implement a risk-based approach and the language used did not appear reflective of the risk situation (e.g. labelling a sector as "exposed to some PF risks" sends a different signal from labelling it as "Medium-High risk"). Singapore has conveyed that based on industry engagements post-publication of the PF NRA, there was no indication that the private sector had misunderstood the PF NRA findings including the risk ratings or how each sector stands relative to other sectors.

640. While the PF threats, vulnerabilities and risk areas set out below have been appropriately identified, further granularity and context-specific insights are needed to strengthen the assessment. This is particularly the case for capturing nuanced risk scenarios and applying these to Singapore's context rather than relying on international typologies. As noted in IO.1, Singapore's PF risk identification and assessment process also does not bring any proportionality to the risks identified.

Box 11.1. Summary of Key Findings from Singapore's PF NRA (2024)



641. There is misalignment in Singapore's PF NRA that downplays Singapore's PF risk exposure. For example, DPTSPs are considered "exposed to some PF risks" when the misuse of virtual assets has been identified as a key PF threat. CSPs are also considered "exposed to some PF risks" while the misuse of legal persons has been identified as another key PF threat. Overall, Singapore's assessment of PF risk lacks alignment and the language used downplays the country's exposure to PF risk. Interviews with Singapore's competent authorities indicated that there is an uneven understanding of the risks of potential breaches, non-implementation or evasion of PF TFS obligations, with key RTIG agencies (like MAS and CAD) and MFA having a stronger understanding.

642. There is no mechanism or part of Singapore's risk identification and assessment process that identifies, assesses and attempts to understand lower PF threats, vulnerabilities and risks. Singapore's one-page CPF Strategy was released in 2024 within the PF NRA report and comprises five generic actions that are largely already being undertaken: (1) maintain strong national and international co-operation, (2) remain alert to evolving PF risks, (3) keep regulatory instruments up-to-date and compliant with relevant UNSCRs, (4) engage industry to raise and strengthen industry's PF risk awareness and understanding, and (5) monitor for compliance and take proportionate and effective enforcement action. Singapore's strategies and actions to be undertaken (as set out in the CPF Strategy) are high-level, lack specificity and are already underway. Further, they do not appear to directly address the threats, vulnerabilities or risks that have been

identified as part of the PF NRA process. Lastly, while there is proportionality to the risks identified, there is no proportionality to the risk mitigation responses in the CPF Strategy. These actions do not adequately or specifically mitigate Singapore's risks, threats, or vulnerabilities, and are not measurable quantitatively or time bound. Singapore mainly monitors and reviews its CPF efforts via the AML/CFT SC, IAC and RTIG interagency co-ordination mechanisms.

643. During the reporting period, Singapore has issued a range of CPF guidance materials across AML/CFT-obliged sectors. However, there are key context-specific threats and vulnerabilities that are not included in the guidance materials. Aside from outreach by Singapore authorities, there are limited mitigation measures applicable to the Singaporean entities that export luxury goods and those that provide goods or services to the maritime industry, including to representation offices of foreign flag States operating in Singapore offering flags of convenience (e.g. Liberia and the Republic of the Marshall Islands), where outreach was conducted very recently. As detailed below, Singapore relies heavily on its trade ban with the DPRK as a mitigation measure without specific attention to PF issues. For example, while misuse of legal persons is a key PF threat identified by Singapore, there is negligible evidence of targeted mitigation measures undertaken in relation to CSPs on PF, for example in relation to verification of BO information that might obfuscate identities of designated persons (see IO.5).

644. Given Singapore's status as a hub for trade, transport and maritime, Singapore Customs has in place measures to monitor and enforce the DPRK trade ban. The MPA also has in place systems and controls to ensure that Singapore does not register ships that are owned by UNSC-designated persons, and that Singapore-registered ships comply with Singapore's regulations. Further, MPA has in place controls to ensure that UNSC-designated ships and those ships owned or controlled by the DPRK are not able to call at Singapore's port. As stated above, Singapore recently engaged the representation offices of foreign flag States. There is scope for Singapore to further engage these offices as the representation offices that the AT met in Singapore demonstrated a negligible understanding of the PF TFS obligations. Given that the changes to incorporate PF into the scope of the FATF Recommendations occurred in 2020, the scale of Singapore's vulnerability and the findings of the PF NRA, it is unclear why these industries were not prioritised throughout the reporting period.

11.3. Implementation of PF-related targeted financial sanctions without delay

645. Singapore has a sound legal framework for the implementation of PF-related TFS, with the IMC-EC overseeing this implementation. PF TFS have automatic effect in Singapore with no need for further transposition into the relevant Regulations; however, the law takes effect the next day after addition to the UNSC TFS list (to account for the time difference between New York and Singapore). The MAS and UN DPRK Regulations apply to any person in Singapore and any Singapore citizen outside Singapore, including FIs, VASPs and DNFBPs. This includes TCSPs, legal persons, shipping companies, companies that provide shipping registration and/or administration services outside Singapore and representation offices of foreign flag States in Singapore. The powers, communication mechanisms and obligations are identical to what is described under IO.10. There are minor gaps in relation to exemptions (see R.7); however, Singapore has a solid framework to implement PF TFS.

646. The Regulations are available publicly on multiple Singapore websites. Where there is a change in the Regulations or any UNSC TFS list, an alert will be sent to FIs, VASPs and DNFBPs that are subscribed to the MAS website. Many entities also subscribe directly to commercial sanctions information service providers. Subscription to the website is checked as part of supervisory engagements. Some DNFBP sector supervisors also pass along these alerts, which, in some instances, can result in delay between receipt and onforwarding to regulated entities if the entity is not directly subscribed to the MAS website. As per IO.10,

communication of new listings, updates and de-listings did not always occur without delay during the reporting period.

647. PF TFS screening is conducted on potential or new customers (and their BOs) at the time of onboarding and before the provision of any services or undertaking of any transactions for the customer. Ongoing screening is also conducted on existing customers by FIs, VASPs and DNFBPs. Most reporting entities have appropriate screening systems and mechanisms in place although some deficiencies have been revealed in supervisory activities.

648. As noted above, there are entities operating within Singapore (outside of the traditional AML/CFT regime) that are exposed to higher proliferation and PF risks (e.g. representation offices of foreign flag States). The AT met such offices during the onsite and found very low levels of awareness of the PF TFS obligations. The AT could not conclude that these offices are complying with PF TFS obligations without delay.

649. At the time of the onsite visit, Singapore had not proposed nor co-sponsored any proposals for designation pursuant to UNSCR 1718, and its successor resolutions. This is consistent with the global approach to UNSCR 1718.

11.4. Identification of assets and funds held by designated persons/entities/those acting on their behalf and prohibitions

11.4.1. Identifying funds or assets held by designated persons/entities/persons acting on their behalf or at their direction

650. All reporting entities are required to identify funds or assets held by UNSC-designated individuals/entities, as well as those acting on their behalf or under their direction, report to MAS (for freezing pursuant to the FSM DPRK Regulations) or the SPF (for freezing pursuant to the UN DPRK Regulations), as well as file an STR on the frozen assets. This requirement is outlined in guidance to reporting entities. During the reporting period, as of July 2025, FIs in Singapore have frozen assets in one case totalling SGD 22.3 million/USD 16.2 million (in 2019), pursuant to UNSCR 1718 and its successor resolutions.

651. Reporting entities met during the onsite emphasised the importance of PF sanctions screening and STR reporting in complying with their AML/CFT/CPF obligations. However, based on discussions during the onsite visit, aside from FIs/VASPs, their understanding appears to be focused on the requirement of detecting positive matches against sanctioned individuals and entities through screening, with significantly less consideration given to the analysis of complex sanctions evasion techniques and the implementation of risk-based mitigation measures. The AT is concerned that in Singapore's PF context, reliance on screening software may not result in the identification of persons acting on behalf of or at the direction of DPRK-related designated persons and entities. As seen in Table 11.2, PF-related/proliferation-related prosecutions relating to the UN (Sanctions – DPRK) Regulations and other export control regulations, there were incidences where law enforcement discovered activities in connection with Singapore's DPRK trade ban and or designated persons.

652. Singapore makes BO information accessible to competent authorities through its central ACRA registry and through CDD conducted by reporting entities. As identified in IO.5, there are deficiencies in measures to ensure the accuracy of BO information. The lack of access to accurate BO information for legal persons and arrangements undermines the implementation of PF TFS in Singapore, particularly given that one of Singapore's key PF threats relates to the misuse of legal persons.

653. Over the reporting period, Singapore received around 1900 STRs related to PF, with 732 related to the DPRK. These are high numbers of STRs relating to the DPRK. Singapore was able to confirm that of these 732 STRs, 165 STRs related to UNSC DPRK sanctions.

Table 11.1. PF-related STRs (which include STRs filed in connection with UNSC sanctions against the DPRK and PF-related sanctions imposed by any other country)

	2020	2021	2022	2023	2024	Total
Banks	222	269	121	275	249	1 136
DPTSPs	4	5	4	71	266	350
Remittance agents	1	3	15	28	22	69
Insurers	33	33	34	53	61	214
CSPs	1	3	1	7	4	16
Lawyers/LPEs	0	4	2	0	0	6
Other sectors	21	13	8	45	27	114
Total	282	330	185	479	629	1 905

Note: Statistics are based on STRO's profiling of STRs filed i.e. reporting entities may have filed on other suspicions.

654. Singapore provided information dissemination statistics for 2023-24 - there were five UNSC sanctions proliferation/PF-related financial intelligence packages disseminated to relevant competent authorities in 2023.[41] Each of these related to entities involved in an investigation under the UN (Sanctions – DPRK) Regulations.

655. From 2020 to 1H 2025, Singapore's AGC successfully prosecuted 22 natural persons and eight legal persons for PF-related/proliferation-related breaches of Singapore's laws. Nineteen of these prosecutions proceeded under the UN (Sanctions – DPRK) Regulations, with the remainder prosecuted under the DPRK trade ban control offences. No natural or legal person has been prosecuted for PF TFS breaches. Please see Table 11.2 for the 30 prosecutions, which provide an insight into the PF exposure of Singapore. It is also notable that the sanctions applied to those prosecuted range from 8 days to 12 months' imprisonment and fines ranging from SGD 3 500 to SGD 311 000. These sanctions are not in line with the gravity of offences and are not appropriately dissuasive. The assessment team saw very limited evidence that the cases below attracted supervisory penalties although the YTE case had accompanying MAS intervention (via the imposition of a financial sanction on an FI) to the prosecution.

Table 11.2. PF-related/proliferation-related prosecutions related to UN (Sanctions – DPRK) Regulations and other export control regulations

	Case / Year Convicted	Description	Penalty
1	Li Hyon (T-Specialist International (S) Pte Ltd / SCN Singapore Pte Ltd) / **2020**	Li Hyon, on his father's instructions, placed orders for prohibited luxury items with T-Specialist and SCN, checked on shipment status and facilitated payments for goods. 4 counts of abetment by conspiracy to supply designated luxury items under the UN (Sanctions –DPRK) Regulations	**4 weeks' imprisonment**
2	Sherly Muliawan (T-Specialist International (S) Pte Ltd) / **2020**	Shipping manager and purchaser in T-Specialist - failed to inform Police about the prohibited supply of prohibited luxury items to the DPRK. 5 counts of failing to provide the Police with information about prohibited transactions under the UN (Sanctions –DPRK) Regulations	**Fine of SGD 10 000**

[41] In 2023-24, there were 34 proliferation/PF-related financial intelligence packages related to a wider range of PF-related concerns such as cases involving OFAC and other unilateral sanctions.

	Case / Year Convicted	Description	Penalty
3	Lam Hon Lan (SCN Singapore Pte Ltd) / **2020**	Secretary in SCN - failed to inform Police about the prohibited supply of prohibited luxury items to the DPRK. 3 counts of failing to provide the Police with information about prohibited transactions under the UN (Sanctions – DPRK) Regulations.	**Fine of SGD 6 000**
4	Lim Cheng Hwee (SINSMS Pte Ltd) / **2020**	Supplied prohibited luxury items (i.e., wine and spirits) to the DPRK through SINSMS. 3 counts of abetment by conspiracy to supply designated luxury items under the UN (Sanctions –DPRK) Regulations (4 other similar charges, and 2 charges of abetment by intentional aiding in commercial trade with the DPRK under the Regulation of Imports and Exports Regulations were taken into consideration for the purpose of sentencing).	**2 months' imprisonment**
5	Hong Leng Ooi (SINSMS Pte Ltd) / **2020**	Wife of Lim Cheng Hwee -assisted with administrative operations of SINSMS. Failed to inform Police about the prohibited supply of prohibited luxury items to the DPRK. 2 counts of failing to provide the Police within formation about prohibited transactions under the UN (Sanctions – DPRK) Regulations	**Fine of SGD 4 000**
6	SINSMS Pte Ltd / **2020**	Supplied prohibited luxury items (i.e., wine and spirits) to the DPRK. 3 counts of supplying designated luxury items under the UN (Sanctions –DPRK) Regulations (4 other similar charges, and 2 charges of engaging in commercial trade with the DPRK under the Regulation of Imports and Exports Regulations were taken into consideration for the purpose of sentencing).	**Fine of SGD 30 000**
7	Tan Wee Beng (Wee Tiong Pte Ltd) (WTPL) / **2021**	Managing director and shareholder of WTPL, who had carried on business with entities linked to the DPRK, including selling sugar and other goods to two DPRK persons. Trading ceased before the embargo on trade with the DPRK was put in place. However, Tan Wee Beng falsified invoices to conceal the fact of trading from banks out of concern that banks would terminate the banking relationship. 7 counts of falsification of accounts under the Penal Code.	**Fine of SGD 210 000; in default, 7 months' imprisonment**
8	Bong Hui Ping (WTPL) / **2021**	Shipping manager of WTPL and main staff assisting Tan Wee Beng with DPRK business. Intentionally aided Tan Wee Beng to falsify invoices submitted to the ban. 7counts of abetting Tan Wee Beng's offences under the Penal Code.	**Fine of SGD 59 000; in default, 14 weeks' imprisonment**
9	Chong Hock Yen / **2022**	Supplied prohibited luxury items (i.e., perfumes, cosmetics, watches and musical instruments) to the DPRK through the three companies listed in this page. 8 counts of abetment by conspiracy to supply designated luxury items under the UN (Sanctions –DPRK) Regulations (35 other similar charges were taken into consideration for the purpose of sentencing).	**6 weeks' imprisonment**
10	SCN Singapore Pte Ltd / **2022**	Supplied prohibited luxury items (i.e., perfumes, cosmetics, watches and musical instruments) to the DPRK. 6 counts of supplying designated luxury items under the UN (Sanctions – DPRK) Regulations (33 other similar charges were taken into consideration for the purpose of sentencing).	**Fine of SGD 311 000**
11	Laurich International Pte Ltd / **2022**	Supplied prohibited luxury items (i.e., perfumes, cosmetics, watches and musical instruments) to the DPRK. 1 count of supplying designated luxury items under the UN (Sanctions – DPRK) Regulations.	**Fine of SGD 30 000**
12	Sindok Trading Pte Ltd / **2022**	Supplied prohibited luxury items (i.e., perfumes, cosmetics, watches and musical instruments) to the DPRK. 1 count of supplying designated luxury items under the UN (Sanctions – DPRK) Regulations (2 other similar charges were taken into consideration for the purpose of sentencing)	**Fine of SGD 23 000**
13	Phua Sze Hee (Pokka) / **2022**	Supplied prohibited goods (i.e., Pokka strawberry milk) to the DPRK. 4 counts of abetment of exporting prohibited goods to the DPRK under the Regulation of Imports and Exports Regulations (24 other similar charges were taken into consideration for the purpose of sentencing).	**5 weeks' imprisonment**
14	Manfred Low Cheng Jing (Yuk Tung Energy Pte Ltd) (YTE) / **2022**	The accused was a director and shareholder of YTE. YTE had been allegedly involved in a ship-to-ship transfer of gasoil to a DPRK-flagged vessel. The accused disposed of his iMac computer, which contained bank documents, payment vouchers and claims. The disposal frustrated CAD's ability to fully investigate YTE's alleged contravention of the UN DPRK Regulations. 1 count of intentionally obstructing the course of justice under the Penal Code (a similar charge was taken into consideration for the purpose of sentencing).	**15 weeks' imprisonment**
15	Vladlen Amtchentsev (Velmur Management Pte Ltd) / **2022**	Following receipt of intelligence that Velmur had allegedly facilitated business activities on behalf of a UNSC-sanctioned DPRK entity, CAD commenced an investigation into potential breaches of the UN DPRK Regulations. Due to the lack of evidence, Singapore eventually proceeded on ancillary charges of forgery as Vladlen had forged statements of financial institutions to create a misimpression that he had deposited monies in the said accounts. 2 counts of forgery under the Penal Code (1 other similar charge under the Penal Code and 2 charges under the Companies Act were taken into consideration for the purpose of sentencing)	**4 weeks' imprisonment**
16	Tay Kiong Chiak (A-Linkz Marketing Pte Ltd) / **2022**	Supplied prohibited goods (i.e., Pokka premium milk coffee and Pokka strawberry milk) to the DPRK. 1 count of exporting prohibited goods to the DPRK under the Regulation of Imports and Exports Regulations (2 other similar charges were taken into consideration for the purpose of sentencing).	**12 days' imprisonment**

	Case / Year Convicted	Description	Penalty
17	Sim Swee Wah (Hock Seng Food Pte Ltd) / **2022**	Supplied prohibited goods (i.e., various food and beverage products belonging to brands under the Hosen Group) to the DPRK. 1 count of exporting prohibited goods to the DPRK under the Regulation of Imports and Exports Regulations (2 other similar charges was taken into consideration for the purpose of sentencing).	**8 days' imprisonment**
18	Benny Tan Chun Kiat (MT Sea Tanker II) / **2023**	In relation to an investigation into MT Sea Tanker II allegedly engaging in ship-to-ship transfers with DPRK-flagged vessels, MPA requested for documents from Sea Hub Tankers, including MT Sea Tanker II's official logbook, oil record book, charter party agreement(s) and bill(s) of lading. The accused and accomplices rewrote the records and discarded documents to create a false narrative about the movement and cargo activity of MT Sea Tanker II, which frustrated CAD's ability to fully investigate Sea Hub Tankers' alleged contravention of the UN DPRK Regulations. 1 count of abetment by conspiracy to intentionally obstruct the course of justice under the Penal Code (1 other similar charge was taken into consideration for the purpose of sentencing)	**6 months' imprisonment**
19	Ong Chou Hong (Sea Hub Tankers Pte Ltd) / **2023**	In addition to the above, Ong and another accomplice, Jeremy Koh disposed of the computer CPU on MT Sea Tanker II containing information relating to MT Sea Tanker II's activities. Ong was traced to a previous offence of obstructing the course of justice in 2019. 2 counts of abetment by conspiracy to intentionally obstruct the course of justice under the Penal Code (1 other similar charge was taken into consideration for the purpose of sentencing)	**9 months' imprisonment**
20	Koh Renfeng Jeremy (MT Sea Tanker II) / **2023**	Similar to the above, Koh and Ong disposed of the computer CPU on MT Sea Tanker II containing information relating to MT Sea Tanker II's activities. 2 counts of abetment by conspiracy to intentionally obstruct the course of justice under the Penal Code (1 other similar count was taken into consideration for the purpose of sentencing)	**6 months' imprisonment**
21	Loh Mun Sang (Rejo Beverages Pte Ltd) / **2023**	Sole directing mind of Rejo - supplied prohibited luxury items (i.e., wine and spirits) to the DPRK via Rejo. 4 counts of abetment by intentional aiding to supply designated luxury items under the UN (Sanctions – DPRK) Regulations (13 other similar charges were taken into consideration for the purpose of sentencing)	**6 weeks' imprisonment**
22	Rejo Beverages Pte Ltd / **2023**	Supplied prohibited luxury items (i.e., wine and spirits) to the DPRK. 4 counts of supplying designated luxury items under the UN (Sanctions – DPRK) Regulations (13 other similar charges were taken into consideration for the purpose of sentencing)	**Fine of SGD 160 000**
23	Koh Kuan Jiu (Xu Kuanrou) (Muller and Partner (Singapore) Private Limited) / **2023**	General manager of Muller - provided freight forwarding services to a company, Eluva International Pte Ltd, which shipped prohibited luxury items (i.e., spirits) to the DPRK. 2 counts of abetment by intentional aiding to supply designated luxury items under the UN (Sanctions – DPRK) Regulations	**Fine of SGD 7 000; in default, 6 weeks' imprisonment**
24	123 Holdings Pte Ltd / **2023**	Supplied prohibited luxury items (i.e., spirits) to the DPRK. 2 counts of supplying designated luxury items under the UN (Sanctions – DPRK) Regulations (3 other similar charges were taken into consideration for the purpose of sentencing)	**Fine of SGD 60 000**
25	123 Duty Free Pte Ltd / **2023**	Supplied prohibited goods (i.e., Pokka assorted drinks) to the DPRK. 2 counts of exporting prohibited goods to the DPRK under the Regulation of Imports and Exports Regulations (3 other similar charges were taken into consideration for the purpose of sentencing)	**Fine of SGD 30 000**
26	Wang Jung Chung (123 Holdings Pte Ltd/123 Duty Free Pte Ltd) / **2023**	Joint director of 123 Holdings (together with siblings) and sole director for 123 Duty Free - supplied prohibited luxury items (i.e., spirits) and prohibited goods (i.e., Pokka assorted drinks) to the DPRK. 2 counts of abetment by intentional aiding to supply designated luxury items under the UN (Sanctions – DPRK) Regulations (3 other similar charges were taken into consideration for the purpose of sentencing). 2 counts of abetment by intentional aiding to export prohibited goods to the DPRK under the Regulation of Imports and Exports Regulations (3 other similar charges were taken into consideration for the purpose of sentencing)	**8 weeks' imprisonment**
27	See Swee Hian (123 Holdings Pte Ltd/123 Duty Free Pte Ltd) / **2023**	Export director employed by 123 Holdings who reported to Wang - supplied prohibited luxury items (i.e., spirits) and prohibited goods (i.e., Pokka assorted drinks) to the DPRK. 2 counts of abetment by intentional aiding to supply designated luxury items under the UN (Sanctions – DPRK) Regulations (3 other similar charges were taken into consideration for the purpose of sentencing). 2 counts of abetment by intentional aiding to export prohibited goods to the DPRK under the Regulation of Imports and Exports Regulations (3 other similar charges were taken into consideration for the purpose of sentencing)	**4 weeks' imprisonment**
28	Koh Poh Choo (Skyline Shipping Private Limited) / **2024**	General manager of Skyline - provided freight forwarding services to a company, Eluva International Pte Ltd, which shipped prohibited luxury items (i.e., spirits) to the DPRK. 1 count of abetment by intentional aiding to supply designated luxury items under the UN (Sanctions – DPRK) Regulations (3 other similar charges, and 2 charges of abetment by intentional aiding to export prohibited goods to the DPRK under the Regulation of Imports and Exports Regulations (3 other similar charges were taken into consideration for the purpose of sentencing)	**Fine of SGD 3 500**

	Case / Year Convicted	Description	Penalty
29	Low Eng Yeow Justin / **1H 2025**	Caused ISA Energy (Asia) to effect transfers of monies to Hin Leong Trading Pte Ltd for the purchase of refined petroleum products (RPP), knowing that the transfers would contribute to the transfer of RPP to persons in the DPRK. 3 counts of indirectly transferring financial assets that may contribute to a prohibited activity under the UN (Sanctions – DPRK) Regulations (6 other similar charges were taken into consideration for the purpose of sentencing)	**Global imprisonment term of 12 months and 3 weeks**
30	ISA Energy (Asia) Pte Ltd / **1H 2025**	Effected transfers of monies to Hin Leong Trading Pte Ltd for the purchase of RPP, knowing that the transfers would contribute to the transfer of RPP to persons in the DPRK. 3 counts of directly transferring financial assets that may contribute to a prohibited activity the UN (Sanctions – DPRK) Regulations (6 other similar charges were taken into consideration for the purpose of sentencing)	**Global fine of SGD 280 000**

656. Given the very high number of DPRK PF-related STRs filed in Singapore during the assessment period, and the PF-related/proliferation-related prosecutions of 22 natural persons and eight legal persons for involvement in or provision of luxury goods, it is unlikely that there were only funds in one case and no other assets to freeze. Singapore could make better use of financial intelligence and investigative capacity to better identify funds and assets in these cases.

11.4.2. Prohibiting financial transactions related to proliferation

657. FIs, VASPs and DNFBPs are required to freeze assets, and transactions related to designated persons or entities are prohibited. When MAS or other supervisors receive specific and credible intelligence via the IMC-EC or RTIG mechanism, or bilaterally from foreign counterparts, MAS will alert the relevant FIs/VASPs and ask them to review and report any relationship with the names cited in the intelligence so as to ascertain: (i) the exposure of and risks to Singapore's financial system; and (ii) whether there had been any breach of the FSM DPRK Regulations and AML/CFT requirements which FIs/VASPs have to comply with.

11.5. FIs, VASPs and DNFBPs understanding of and compliance with obligations

658. Singapore's FIs and VASPs have a good understanding of their obligations to comply with PF TFS. For the most part, the understanding is analogous to the understanding of compliance with TF TFS (see IO.10). DNFBPs demonstrated an uneven understanding of obligations, with some DNFBPs demonstrating active screening for designated individuals and entities and immediate freezing, while others were less sure of their obligations and what to do if a positive match was identified. DNFBPs demonstrated much less consideration given to the analysis of complex sanctions evasion techniques and the implementation of risk-based mitigation measures. It is also not clear that reporting entities' use of screening software is appropriately capturing transactions or assets that are conducted/held on behalf of or at the direction of persons or entities designated by the UNSC in relation to PF.

659. Singapore has prioritised outreach and awareness raising to assist reporting entities in their understanding of their PF TFS obligations. Over the reporting period, Singapore has conducted and issued a substantial number of CPF-related outreach events and guidance products. DNFBP sectors have been provided with sector-specific guidance, but the degree of understanding of the guidance varied across sectors and entities. Such outreach and awareness raising are largely in line with Singapore's PF risks; however, there is a lack of outreach for CSPs generally, a sector providing higher risk services. This is somewhat mitigated by ACRA's examinations of CSPs that consider CPF-related controls.

Table 11.3. CPF-related Outreach

	2020	2021	2022	2023	2024	Total
Banks	11	5	10	17	25	68
DPTSPs	9	2	12	13	24	60
PSPs with CBMT services	7	1	12	13	24	57
Insurers	6	1	8	13	23	51
CSPs	3	4	3	3	6	19
PSMDs	1	31	4	5	11	52
Lawyers/LPEs	4	6	3	5	10	28
Total	41	50	52	69	123	335

660. Most FIs, VASPs and larger DNFBPs rely on commercial software to screen against TFS lists and conduct ongoing and real-time screening of client lists and transactions. Smaller entities reported good engagement by their sector supervisor to assist them with their obligations. In particular, MinLaw had developed a standalone screening database for the PSMD sector to assist them with the obligations. These entities are aware of their obligations to report to their supervisor and authorities, and to terminate relationships, and know where to seek further guidance and information as needed.

661. Customers are screened at onboarding and periodically against lists at a pre-defined frequency that aligns with a customer's risk profile, when there are changes to the lists or when there are wire transfers involving a customer that has not otherwise established business relations (no threshold for domestic wire transfers and a threshold of at least SGD 1 500 or USD 1 110 for cross-border wire transfers). Checks are also conducted on customers and transactions where red flags may be present. For wire transfers, FIs and VASPs comply with prohibitions on conducting transactions with designated persons. Banks generally facilitate wire transfers through automated systems which do not process transfers if any fields trigger sanctions screening hits. VASPs generally use blockchain analytics tools to screen the beneficiary and originator to verify that they are not on sanctions lists, and to detect any exposure to wallet addresses with a sanctions nexus at onboarding and on an ongoing basis. PSPs have a variety of different processes to comply with this requirement.

662. Singapore has received a large number of PF-related STRs over the reporting period demonstrating reporting entities' awareness of PF-related risks and CPF obligations. However, the lack of STRs from lawyers, PSMDs, DPTSPs (up to 2022) and CSPs does not accord with Singapore's risk profile. This may be reflective of an uneven understanding of TFS obligations. It is noticeable that there have been around 1 900 PF related STRs, but limited funds or other assets frozen or false positives registered during the assessment period, indicating a possible disconnect between reporting and freezing actions.

11.6. Competent authorities monitoring and ensuring compliance with PF-related targeted financial sanctions

11.6.1. FIs and VASPs

663. The approach to monitoring and ensuring PF TFS compliance mirrors the approach for TF TFS (see IO.10). The review of reporting entities' compliance with PF TFS obligations is integrated into the overall scope of supervisory activities. As identified in IO.3, MAS supervises and monitors FIs' and VASPs' implementation of PF TFS through supervisory activities that are initiated by three approaches: (1) controls-based, (2) FIRA-based or (3) risk surveillance-based.

664. Controls-based supervisory engagements are targeted scope supervisory activities where MAS has become aware of a compliance issue through the review of internal/external audit reports, the review of STRs, etc. In these cases, MAS promptly follows up with the FI/VASP to rectify the issue.

Table 11.4. Number of Controls-based Supervisory Activities

Sector	2020	2021	2022	2023	2024	Total
Banks (155)	408	484	394	473	446	2205
DPTSPs (29)	0	6	12	26	22	66
PSPs with CBMT services (199)	21	25	21	67	89	223
Insurers (105)	33	39	44	50	59	236

Note: See Table 11.5 below for supervisory examinations related to CSPs, PSMDs and Lawyers/LPEs

665. Singapore places great reliance on controls-based supervisory activities – they represent approximately 95% of total supervisory activities. However, given the targeted and less formal nature of these supervisory activities, there are no statistics on exactly what scope these supervisory activities covered. It is known that these activities took place, and if there was a compliance issue it was generally either rectified or escalated to a more intensive supervisory activity. There is no information to demonstrate how, and to what extent, these controls-based supervisory engagements incorporated PF TFS obligations. Some credit must be given to Singapore for the supervision of PF TFS requirements through these controls-based supervisory activities but because of the unknown scope, the assessment team must be conservative in taking these into account.

666. As outlined in IO3 Singapore also conducts full scope or more intrusive examinations through its other two supervisory approaches, FIRA-based or risk surveillance-based. These include vetting policies and procedures, reviewing sanctions screening activities, testing alerts, checking freezing/blocking requirements, overseeing transaction monitoring and reporting of matches. Considering the number of REs, and the risk and context of Singapore, few supervisory activities are known to scope in ensuring compliance with PF TFS.

Table 11.5. CPF-related Supervisory Activities

Sector	2020	2021	2022	2023	2024	Total
Banks (155)	5	9	2	10	0	26
DPTSPs (29)	0	0	3	5	0	8
PSPs with CBMT services (199)	2	5	0	38	43	88
Insurers (105)	1	0	0	0	0	1
CSPs (3093)	109	379	367	300	417	1572
PSMDs (1967)	218	136	209	241	191	995
Lawyers/LPEs (1161)	50	50	50	52	24	226
Total	385	579	631	646	675	2916

667. Over the course of the assessment period, there was limited known coverage of supervisory activities related to PF TFS for FI and VASP sectors. The number of supervisory examinations scoped to include PF TFS for PSMDs and lawyers/LPEs is quite significant when compared to more material and higher risk sectors. There does not seem to be a risk-based approach to ensuring compliance with PF TFS obligations.

Box 11.2. Case Study – Imposition of financial penalty for failure to maintain freeze on the funds of individuals acting on behalf of UNSC-designated entity

In response to intelligence from a foreign counterpart, in 2018, CAD investigated a Singapore based UNSC-designated YTE (Yuk Tung Energy, an oil trading and bunkering company). The company was involved in oil trading, bunkering, and marine engineering consultancy work. CAD seized a sum of approximately SGD 22.3 million (USD 16.2 million) in another company's bank account (PITSPL). YTE had paid PITSPL this amount after agreeing to purchase gasoil. In March 2021, Courts ordered the funds to be released back to PITSPL's account with Bank A. Bank A subsequently informed MAS that it had assessed that the funds were beneficially owned by YTE and were thus subject to the asset freezing provisions in the FSM DPRK Regulations.

In November 2020, MAS imposed a financial penalty of SGD 200 000 (USD 148 000) on Bank D for breaching the FSM DPRK Regulations by closing three accounts belonging to two individuals, MLCJ and ABY, and unfreezing and releasing the funds within to them - an amount of about SGD 9 000 (USD 6 660) was released to MLCJ and an amount of about SGD 30 000 (USD 22 200) was released to ABY. Given that MLCJ and ABY were the shareholders and directors of UNSC-designated YTE, they were assessed to be acting on behalf of YTE.

This penalty was applied almost two years after the YTE's oil transactions with DPRK were brought to Singapore's attention by another jurisdiction and the UNSC. The bank had voluntarily reported the lapse to MAS and has since enhanced and tightened its controls to prevent a recurrence.

In 2022, a Director of YTE pleaded guilty to obstruction of justice charges related to an illegal ship-to-ship gasoil transaction in 2018 between a YTE-owned vessel and a DPRK-registered vessel.

668. Where there were breaches of CPF requirements detected, remedial actions and sanctions were applied. However, these penalties are relatively low. 17 remedial measures and sanctions were imposed against banks, nine against CSPs, six against insurers and two against DPTSPs. Remedial measures and sanctions ranged from lighter actions such as a supervisory reminder, private reprimand or supervisory warning to stronger actions such as imposition of financial penalty, curtailment of business or revocation of licence. During this same period, MAS also took action against two FIs for breaches of the FSM DPRK Regulations (i.e. imposition of financial penalty and private reprimand). Penalties for failure to comply with PF-related obligations are relatively low when considering the breaches and are not proportionate and dissuasive in all cases. In addition to the actions taken for breaches, MAS regularly gets FIs/VASPs to take remedial actions to address findings identified in its supervisory engagements and examinations.

Box 11.3. Case Study – Singaporean persons trading with the DPRK

In 2020, MAS detected an STR network involving a Singapore citizen, JC, who, according to the UNSC Panel of Experts on the DPRK, allegedly shipped vodka to the DPRK. The entities of which JC was a shareholder, or a director were also allegedly involved. Based on the STRs filed, JC appeared to be attempting to circumvent a number of banks' controls by using an alias to facilitate the payments for the vodka purchases.

MAS escalated this case to ISTRA in November 2020 and followed up with the banks involved. MAS' follow-up did not uncover assets that the banks should have frozen pursuant to the FSM DPRK Regulations or any breach of the FSM DPRK Regulations or major weaknesses. There were instances

where some of the banks' name screening checks could be further enhanced (i.e. they should not just screen against sanctions lists but also against names identified within the UNSC Panel of Experts' reports), and MAS requested these banks to do so. Separately, Customs carried out an investigation into JC and his entities, and charges have since been brought against them for exporting prohibited items pursuant to the UN DPRK Regulations and the Regulation of Imports and Exports Regulations.

Annex A. Technical compliance[42]

This section provides detailed analysis of the level of compliance with the FATF 40 Recommendations in their numerical order. It does not include descriptive text on the country situation or risks and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report.

This technical compliance covers areas where the country has made legal, regulatory or operational framework changes since its last mutual evaluation (dated 2016) (or follow-up reports with technical compliance re-ratings (dated 2019) and areas where there has been a change in the FATF Standards for which the country has not previously been assessed. The reassessed areas are clearly identified under each heading.

For Recommendations not under review, pre-existing information from the country's most recent assessments is included. Such Recommendations are marked with a footnote cross-referencing the date and source of the information (i.e. the country's most recent mutual evaluation or follow-up reports with technical compliance re-ratings).

Recommendation 1 – Assessing risks and applying a risk-based approach[43]

In the 4th round MER, Singapore was rated Largely Compliant with R.1. Singapore was assessed to have used cross-government co-ordination mechanism to identify ML/TF risks and mitigate the identified risks, but gaps were noted in some high-risk areas such as in relation to transnational money laundering, illicit financial flows, international co-operation, and cash couriers. The previous MER did not assess compliance in relation to understanding and mitigating risks related to proliferation financing.

Countries' obligations and decisions

Assessment of ML/TF risks

Criterion 1.1 –

Singapore has identified and assessed its ML/TF risks through continual risk monitoring. To consolidate risk assessments over the years, Singapore published its updated ML and TF NRAs in June and July 2024 respectively.

Criterion 1.2 –

RTIG is the working level body to oversee the identification, assessment, and mitigation of ML/TF/PF risks. The RTIG reports to the AML/CFT SC on Singapore's key ML/TF/PF risks.

[42] In accordance with the 5th Round Methodology, Recommendations under review, which have been analysed for this mutual evaluation, are in green.

[43] Recommendation 1 is newly assessed due to changes to the FATF Standards for which Singapore has not previously been assessed.

Criterion 1.3 –

Since the first NRA in 2014, Singapore has published two TF NRAs in 2020 and 2024 respectively, while the updated ML NRA was published in 2024. Singapore also issued four thematic risk assessments all of which were published/updated in 2024. Although it was noted in the 4th round MER that the NRA would be updated regularly, there was no formal basis outlining the frequency of NRA updates and the 2024 NRAs also do not commit to any timeline for updates. Singapore's "dynamic approach" to keep its understanding of risk up to date through monitoring and discussion at the RTIG is noted, but such discussions did not result in any regular and comprehensive update on overview of its ML/TF risk landscape. The risk observations and findings from the dynamic risk monitoring are not consolidated into a clear and consistent communication until the NRAs published in 2024.

Criterion 1.4 –

All competent authorities are involved in and participate collectively in ML/TF risk identification and assessment efforts through the RTIG. The ML NRA, TF NRA and other thematic risk assessments are available on the websites of MHA (including CAD/SPF), MOF and MAS. Singapore engaged the private sectors through the ACIP, other relevant industry associations, platforms such as industry events, surveys and small group discussions to gather feedback on risk understanding, assessment and mitigation across the system.

Assessment of PF risks

Criterion 1.5 –

Sub-criterion 1.5(a) - Singapore identified and assessed its PF risks through the RTIG with inputs from relevant LEAs, sector supervisors and private sector under the ACIP. Singapore published its first PF NRA in October 2024. The PF NRA is built on existing PF-related guidelines and guidance produced by the relevant authorities.

Sub-criterion 1.5(b) - The RTIG is the main interagency body to co-ordinate actions to assess and mitigate PF risks at the WoG level.

Sub-criterion 1.5(c) - The first PF NRA was published in 2024 and there is no timeline for updates. Given that this is a new requirement, the risk assessment is considered up-to-date.

Sub-criterion 1.5(d) - The PF NRA is available on the websites of MHA (including CAD/SPF), MOF and MAS. Supervisors also disseminate the PF NRA and convey supervisory expectations on its relevance through circulars issued to the private sector as well as industry outreach sessions.

Measures to mitigate ML/TF risks

Criterion 1.6 –

The AML/CFT SC has guided agencies to establish dedicated workgroups (e.g. on tax ML and TBML cases) to enhance risk understanding and typologies in some higher risk areas and take co-ordinated mitigating actions. Sectors which are assessed to pose higher risk (e.g. DPTSPs) are subject to enhanced measures and more intensive supervisory oversight (for example, see c15.9(a)). Resources are allocated centrally to agencies by the Ministry of Finance (MOF). Agencies will assess if the risk mitigation measures (as guided by RTIG/IAC/SC) can be met by their current resources (e.g. redeploying resources from other functions), or if more resources may be needed, while concurrently starting work on the risk mitigation measures. If more resources are needed, requests for additional headcount can surfaced to IAC/SC for guidance and endorsement before they are submitted to MOF for approval. Such resource applications are considered on a case-by-case basis without systematic consideration of overall risk landscape. At isolated junctures, the SC/IAC have also reviewed the resource of AML/CFT agencies.

LEAs prioritise and allocate their resources towards pursuing the types of ML activities highlighted in the ML NRA as key threats. This includes specialised units and taskforces to focus on predicates and related ML (e.g. Anti-Scam Command to combat CEF and related ML), as outlined in the Law Enforcement Strategy to Combat Money Laundering. Singapore adopts an intelligence-led approach to TF investigations to ensure that resources are deployed to achieve maximum TF investigation and prosecution outcomes. The approach highlights triangulation between financial intelligence and security intelligence, and is aligned with its TF risk profile, particularly the threat that arises from self-radicalised individuals using legitimate income for TF. Targeted resources have also been allocated to equip officers with specialised training and enhance inter-agency collaboration in response to emerging risks, such as the rising TF threat in the virtual asset sector.

Criterion 1.7 –

Sub-criterion 1.7(a) - In Singapore, exemptions from certain AML/CFT/CPF requirements are applied only in limited circumstances where the ML/TF/PF risks have been proven to be low. There are no exemptions from the requirements for these persons/entities to file STRs (pursuant to section 45 of the CDSA) when they have reasonable grounds to suspect any property or transaction may constitute a predicate offence which they come across during the course of their business/employment.

Sub-criterion 1.7(b) - Singapore does not allow for exemption of financial activity from AML/CFT requirements on the basis that such activities were carried out on occasional or very limited basis such that there is a low ML/TF risk.

Criterion 1.8 –

Where higher risks have been identified and conveyed by the competent authorities, FIs and DNFBPs are required to ensure that this information is incorporated into their risk assessments and to take enhanced measures to manage and mitigate those risks. This is covered by 24 sector specific regulations and notices.

Criterion 1.9 –

FIs and DNFBPs may apply simplified measures when the assessment of low risk is supported by an adequate analysis of risks. The simplified measures must be commensurate with the level of risk, based on the risk factors identified by the FI or DNFBP, and guided by the risks identified in ML NRA, TF NRA and any other guidance from the authorities. Simplified CDD measures are prohibited in higher risk scenarios, or where there is a suspicion of ML/TF. This is covered by 24 sector specific regulations and notices.

Criterion 1.10 –

Sector supervisors, including SRBs, oversee the implementation of AML/CFT/CPF requirements (including obligations under R.1 to assess ML/TF/PF risks and the mitigation of these risks).

Measures to mitigate PF risks

Criterion 1.11 –

Sub-criterion 1.11(a) – As described under c.1.7, the exemptions described therein also applies to PF.

Sub-criterion 1.11 (b) and (c) - All FIs and DNFBPs were already subject to CPF requirements since PF (including the UN and FSM Act Regulations on DPRK) is an ML predicate offence under the CDSA. All FIs and DNFBPs are required to conduct a PF risk assessment and apply the appropriate risk mitigation measures for PF (which is already an existing requirement that is under the AML/CFT framework), including taking commensurate measures to manage and mitigate higher and lower risks respectively, while ensuring full implementation of the targeted financial sanctions required under R.7.

Sub-criterion 1.11 (d) - As described under c.1.10, the regulatory framework described therein also applies to PF risks.

Obligations of financial institutions and designated non-financial businesses and professions

Assessment of ML/TF risks

Criterion 1.12 –

FIs and DNFBPs are required to take appropriate steps to identify, assess and understand their ML/TF risks in relation to its customers, the countries or jurisdictions its customers are from or in, the countries or jurisdictions it has operations in, and the products, services, transactions, including digital token transactions, and delivery channels. This includes documenting risk assessments, considering all relevant risk factors before determining the level of overall risk and the appropriate type and extent of mitigation to be applied, keeping these assessments up to date, and having appropriate mechanisms to provide risk assessment information to competent authorities and SRBs. This is covered by 24 sector specific regulations and notices.

Measures to mitigate ML/TF risks

Criterion 1.13 –

FIs and DNFBPs are required to develop and implement policies, procedures and controls which are approved by senior management to effectively manage and mitigate the risks that have been identified or notified to it by the relevant authorities in Singapore, monitor the implementation of those policies, procedures and controls and enhance them if necessary, and perform enhanced measures where higher risks are identified to effectively manage and mitigate those higher risks. This is covered by 24 sector specific regulations and notices.

Criterion 1.14 –

Singapore permits FIs and DNFBPs to take simplified CDD measures where low risks have been identified. FIs and DNFBPs are not allowed to perform simplified CDD measures where there is ML/TF suspicion. This is covered by 24 sector specific regulations and notices.

Assessment of PF risks and measures to mitigate them

Criterion 1.15 –

All FIs and DNFBPs were already subject to CPF requirements. All FIs and DNFBPs are required to conduct PF risk assessments, and apply requirements (which are already existing requirements under the AML/CFT framework) to have policies, controls and procedures which are approved by senior management and consistent with national requirements and guidance from competent authorities and SRBs to manage and mitigate PF risks, monitor the implementation of these controls and enhance them if necessary, take commensurate measures to manage and mitigate the risks where higher PF risks are identified, and where the level of risks are lower, ensure that measures to manage and mitigate the risks are commensurate with the level of risk while ensuring full implementation of the targeted financial sanctions required under R.7.

> *Weighting and conclusion –* Singapore identifies and assesses its ML/TF/PF risks through continual risk monitoring at the WoG level. Singapore has framework in place to require FIs and DNFBPs to conduct risk assessments and implement measures commensurate with the identified risks. Singapore has very recently introduced a series of legislative and regulatory amendments for express reference to PF risk assessment and mitigation requirements. Minor gaps remain in the existing mechanisms to ensure a comprehensive and up-to-date risk understanding, and systematic consideration of overall risk landscape in allocating supervisory resources across supervisors for different sectors with varying risk levels.
>
> Recommendation 1 is rated **Largely Compliant.**

Recommendation 2 – National co-operation and co-ordination[44]

In the 4th round MER, Singapore was rated Compliant with R.2.

Criterion 2.1 –

Singapore published (i) the National Strategy for CFT on 1 July 2024; (ii) the National AML Strategy on 30 October 2024; and (iii) Singapore's 2024 PF NRA and CPF Strategy on 30 October 2024. While there is no defined interval for regular review of the policies, Singapore's AML/CFT policies and competent authorities' progress are regularly reviewed and monitored by the AML/CFT SC which meets three to four times a year.

Criterion 2.2 –

The AML/CFT SC, supported by the IAC and RTIG, drives and co-ordinates Singapore's national AML/CFT/CPF policies and activities. The IAC is comprised of Singapore's AML/CFT agencies, including policy makers, the financial intelligence unit, law enforcement authorities, supervisors, customs and tax authorities, intelligence services, and AGC. The IAC serves as the main body that facilitates AML/CFT/CPF policy co-ordination and implementation across agencies and track the progress made. The RTIG regularly updates the IAC and AML/CFT SC on Singapore's key ML/TF/PF threats and risk considerations and recommends mitigation steps. These committees facilitate domestic co-ordination and information exchange concerning AML/CFT/CPF policies.

Criterion 2.3 –

The AML/CFT SC's mandate includes responsibilities to oversee and co-ordinate the WoG approach to prevent and combat ML/TF/PF risks in Singapore; oversee the effective implementation of AML/CFT/CPF measures by the respective agencies; and identify and mitigate emerging ML/TF/PF risks.

Criterion 2.4 –

Singapore has established mechanisms (e.g. IAC, RTIG, AC3N, various inter-ministry committees, subject matter specific taskforces, etc.) to permit effective operational co-operation, co-ordination, and timely sharing of relevant information among competent authorities, both proactively and on request. For operational purposes related to AML/ CFT and CPF, AML/CFT agencies are empowered to share information for AML/CFT purposes via legislation or structured data exchange arrangements.

Criterion 2.5 –

National AML/CFT/CPF policies and requirements are developed taking into account all relevant laws including those relating to Data Protection and Privacy.

> *Weighting and conclusion –* All criteria are met.
>
> Recommendation 2 is rated **Compliant**.

Recommendation 3 – Money laundering offence [45]

In the 4th round MER, Singapore was rated Compliant on R.3.

Criterion 3.1 –

Singapore criminalises ML in line with the requirements of the Vienna and Palermo conventions (S50,51,53,54,55, CDSA). S 53 and 54, CDSA fully meets the physical and material requirements of both

[44] Recommendation 2 is newly assessed due to changes to the FATF Standards for which Singapore has not previously been assessed.

[45] Recommendation 3 is newly assessed as Singapore has made legal, regulatory or operational framework changes since its last mutual evaluation.

Conventions, namely: acquiring, possessing or using property, concealing or disguising any property that in whole or in part, directly or indirectly represents benefits of criminal conduct, and converting or transferring (moving) property or removing it from Singapore. The *means rea* element is covered by requiring the offender to know or have reasonable grounds to believe that property, in whole or in part, directly or indirectly, constitutes the benefits of criminal conduct (S53(2) and 54(2), CDSA). These provisions also create an offence of assisting another to retain benefits of drug dealing / criminal conduct by concealing, disguising, converting, transferring or removing someone else's criminal benefit.[46] For definition of property, see c 3.4.

Criterion 3.2 –

The CDSA applies a list approach to predicate offences, with drug dealing offences listed in the First Schedule, serious offences (such as counterfeiting, prostitution, etc.) listed in the Second Schedule, and other specified offences (such as foreign serious tax offences) in the Third Schedule. Overall, the list – which is regularly updated – comprises more than 600 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.

Criterion 3.3 –

Criterion 3.4 –

All ML offences extend to any type of "property", defined under section 2(1) of the CDSA as money and all other property, movable or immovable, including things in action and other intangible or incorporeal property. Sections 53 and 54, CDSA state that the ML offence extends 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 –

It is not necessary that a person be convicted of a predicate offence when proving that property is the proceeds of crime. Section 56(1-2-5-6) 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. To establish that a predicate offence (including ML) has occurred, 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 offence (Section 54) covers every act constituting a "serious offence" prescribed under the Second Schedule (such as bribery, corruption and tax evasion). Criminal conduct refers to any act that constitutes a 'serious offence' that is undertaken in Singapore or elsewhere (S2(1), CDSA). Moreover, a "*foreign serious offence*" is defined under section 2(1) as offences which would have constituted a serious offence had it occurred in Singapore.

[46] The CDSA was amended in 2024 to extend the ML offence to situations where persons act rashly or negligently (S501(A), 51(A), 53(3) and 54(3), CDSA). ML type offences (dealing with property of terrorists) can also be found in S6, TSOFA, and (assisting a person to carry out unlicensed moneylending) in S19(5)(b) of the Moneylenders Act.

Criterion 3.7 –

The CDSA (and therefore ML offence) applies to persons that commit the predicate offence (Sections 53(1) and 54(1) for drug dealing and criminal conduct respectively and confirmed by case law in *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).

The *mens rea* for ML offences (i.e. knowledge that the laundered property is the proceeds of crime) include negligence and rashness. Under sections 50(1A), 51(1A), 53(3) and 54(3) of the CDSA, an offender who laundered the benefits of drug dealing or benefits of criminal conduct is guilty of an offence even if he did so negligently or rashly in respect of the circumstances that the property represents/relates to the benefits of drug dealing or benefits from criminal conduct.

The requirement that the property be a benefit of drug dealing or a benefit from criminal conduct relates only to the offender's *mens rea* and not the *actus reus*. Sections 56(5) – 56(11) CDSA make it clear that for the purpose of proving an ML offence, it is not necessary to prove as a physical element of the offence that the property was in fact the benefits of drug dealing or benefits from criminal conduct.

Criterion 3.9 –

Proportionate and dissuasive criminal sanctions apply to natural persons convicted of ML. Sections 53(6) and 54(6) of the CDSA provide that natural persons are liable to a maximum imprisonment of 10 years, and/or a fine not exceeding 500 000 (approx. EUR 354 000 / USD 371 050) upon conviction. This is similar to – and in cases, goes beyond – other serious economic offences (e.g. cheating and dishonesty, forgery, falsification of accounts, corruption, bribery, etc.), though is under sanctions for drug trafficking offences (20-to-30-year imprisonment). Case law and sentencing guidelines establish that aggravating factors should also be considered and the sentence should be tailored to the severity of the crime based (See: *Public Prosecutor v Ngiam Kok Min* [DAC 18666/2012 and others], and the Information Note on General Sentencing Principes by the Sentencing Advisory Panel).

Criterion 3.10 –

Criminal liability and sanctions apply against legal persons. The maximum fine that may be imposed for legal persons for the commission of a ML offence is: SGD 1 million (USD 740 000) or twice the value of the property involved/benefit of drugs dealing/benefit of criminal conduct, whichever is higher (Sections 50(7), 51(7), 53(7), 54(7) and 55A(6) CDSA). Based on the circumstances of each case, sanctions can be tailored to the severity of the harm and the culpability of the legal person and can be supplemented by administrative sanctions (such as revocation of license, shutting down a company, S124-125 of the Insolvency, Restructuring and Dissolution Act). In practice, sanctions against legal persons do not preclude parallel civil or administrative proceedings against the legal persons in countries in which more than one form of liability is available. Sanctions against the legal persons are also without prejudice to the criminal liability of natural persons (S244, CPC; S39, IA, S80, CDSA). Sanctions for legal persons are considered proportionate and dissuasive.

Criterion 3.11 –

Singapore has appropriate ancillary offences for ML in place. This includes: 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 –* All criteria are Met.
>
> Recommendation 3 is rated **Compliant**.

Recommendation 4 – Confiscation and provisional measures[47]

In the 4th round MER, Singapore was rated Compliant on R.4.

General principles

Criterion 4.1 –

Sub-criterion 4.1(a) - has policies and operational frameworks that prioritise asset recovery in both the domestic and international contexts. Singapore published its first National Asset Recovery Strategy (NARS) in June 2024. The Strategy underscores the need to detect and deprive criminals of illicit assets through four pillars: detection, deprivation, deterrence, and delivery. It adopts a Whole-of-Government (WoG) approach to asset recovery, engaging LEAs, financial supervisors, and other stakeholders, while highlighting the importance of international co-operation and partnerships. NARS commits to regular legal reviews, prioritizing victims, and preserving assets. It also explores tax recovery and voluntary restitution as complementary tools. Asset recovery is further reinforced as a priority in Singapore's 2024 Law Enforcement Strategy to Combat Money Laundering. To support operational efforts, MHA and AGC have jointly developed and launched the WoG Guidelines on Asset Management and Crypto-Assets, providing LEAs with clearer guidance for effective asset recovery in this area.

Sub-criterion 4.1(b) - periodically reviews its asset recovery regime to ensure its effectiveness. This includes various legislative amendments, including: introducing non-conviction-based (NCB) measures in 2016 (S 51 of the OCA 2016, as amended); allowing competent authorities to dispose of seized property (S370 of the CPC, 2018, as amended); empowering Courts to deal with assets seized from absconded persons who refuse to co-operate with investigations by the LEAs (Sections 370 to 372 of the CPC, 2024, as amended); criminalising money mules in 2023 (S 50, 51, 53,54 and 55, CDSA). Moreover, Singapore introduced in 2020 a SOP guiding LEAs on the management of highly depreciative seized or confiscated assets and in May 2024, the WoG Guidelines on Asset Management and on Crypto-Assets.

Sub-criterion 4.1(c) - provides sufficient technical, human and financial resources to effectively pursue asset recovery. The SPF has doubled the human resources of its Financial Investigation Group (FIG) since 2015 (159 staff as at early 2025). Various LEAs have dedicated units for tracing and recovering assets (see R.30): Division III of the Asset Confiscation Branch (ACB in CAD), the Specialised Fraud investigation Branch (SFIB), and the Anti-Scam Command (ASC); and within CID, the Financial Investigation Branch and the Technology Crime Investigation Branch (TCIB) focusing on cyber-enabled crimes. This is in addition to the embedding of asset recovery functions in the job scope of all LEA investigators, guided by the WOG Guidelines on Asset Management and WOG Guidelines on Management of Cryptocurrencies. Singapore's competent authorities also leverage technology and data analytics to enhance the detection and tracing of criminal assets with a view to facilitating their recovery. All LEAs also have access to specialised resources (such as

[47] Recommendation 4 is newly assessed due to changes to the FATF Standards for which Singapore has not previously been assessed.

financial intelligence and direct access to STRO's database, WINGS X, see R.29) to gather financial intelligence and trace assets, and asset recovery is a core training element for all LEAs.

Sub-criterion 4.1(d) - has a framework in place to enable effective use of the asset recovery regime, consistent with R.2. Singapore adopts a WoG approach to asset recovery. Various platforms are in place through which competent authorities and the private sector can share information and identification of ML and predicate offence risks and cases and facilitate the investigation, forfeiture and confiscation of illicit property. These include: the AML/CFT SC, the IAC, the RTIG, AC3N and the ACIP (see R.2 for further detail).

Investigative measures

Criterion 4.2 –

Singapore has measures, including legislative measures, which enable their competent authorities to:

Sub-criterion 4.2(a) - identify, trace and evaluate criminal property and property of corresponding value, regardless of whether it is owned/held by third parties (see definition of property under R.3). The CPC and CDSA provide for a range of traditional investigative methods (e.g. obtaining documents from FIs, search and seizure, etc.) (S20 to 35(1), CPC, S40(1-5), CDSA, S72 OCA). CDSA enables authorised officers to apply to the court for production orders, which enables them to detect and trace properties and gather facts and circumstances of the cases (S36 and 37). LEAs also have court-granted powers to conduct search and seize in the context of TF investigations (S11(1), TSOFA). The evaluation of assets to be recovered is done by Courts, or failing that, by a Registrar (S6(4) and S7(4), CDSA). When a defendant is convicted of a drug dealing or serious offence set out in Schedule 2 of CDSA, Courts can issue a substitute confiscation order (S34(1-4)). This implies that LEAs and courts are able to identify, trace and evaluate property of corresponding value as well.

To identify and trace property, 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.), as well as STRO's databases. FIG's Asset Confiscation Branch is responsible for conducting Concealed Income Analyses (CIA) to identify unexplained wealth and property of equivalent value that can be subject to confiscation (see c 4.8). CFTB also works with the ISD with respect to TF investigations.

Sub-criterion 4.2(b) - take any other appropriate investigative measures (S 18, 20, S 22-23, S 32-34, S 35(1), CPC; S 12, 15, 36,37 CDSA) (see also R.31). See also resources available under 4.2(a).

Provisional measures

Criterion 4.3 –

Sub-criterion 4.3(a) - has measures, including legislative measures, which enable competent authorities to withhold consent or suspend a transaction suspected of being related to money laundering, a predicate offence, or terrorist financing. Part 4, S35 of the CPC provides LEAs (SPF, CPIB and CNB) with broad powers to seize or prohibit the disposal of or dealing in any property in respect to which an offence is suspected to have been committed without a court order (S35(1-2), CPC). These powers allow LEAs to promptly suspend transactions. Additionally, LEAs can also instruct FIs to refuse any dealing in respect of property held or suspected to be held in an account or safe deposits of the FI or VASP, as well as issue prohibition of disposal orders to DNFBPs to prohibit from dealing in or disposing of assets (S 35 (2b), CPC). SPF is also able to issue Restriction Orders for banks to temporarily restrict banking transactions in relation to scams (S4, Protection from Scams Act). Where STRO requires it or receives an international request from partners, it does not have powers to suspend transactions, as this power is bestowed upon LEAs such as SPF only (see c.40.12).

Sub-criterion 4.3(b) - Specifies the maximum duration of time these suspension powers apply. Seizures made under the powers vested by Part 4, S35, CPC (see 4.3a) are time-bound and subject to judicial review. Restriction Orders for scams – which often involve smaller amounts – are issued for an initial period of 30 days (S5, Protection from Scams Act). A police officer must specify a period of time within which a FI must suspend a transaction when exercising powers under S35(2b), CPC. The officer who seizes any property in the exercise of any power under Part 4, S 35, CPC must also make a report to the relevant Court at the earlier of the following time: when the law enforcement officer considers that the property is not relevant for the purposes of any investigation, inquiry, trial or other proceeding under any written law, or one year after the date of seizure of property (S370, CPC). The court may grant an order for continued seizure of property for a specified period of time. Considering that a suspension power is meant to be used for emergency and short purposes only and the courts can renew this power, the outer limit of a year appears too long.

Criterion 4.4 –

Singapore has measures, including legislative measures, to enable their competent authorities to expeditiously carry out provisional measures. This includes:

Sub-criterion 4.4(a) - freezing and seizing measures to prevent any dealing, transfer or disposal of criminal property and property of corresponding value. This is achieved through restraint and charging orders for property that may become subject to confiscation (S35(1), 35(4), 35(9)(1), S370, CPC; S22, PCA, S26 MDA, S18-21 CDSA). The powers under S 35(4) CPC can be exercised expeditiously by a police officer, and do not require any application to court.

Sub-criterion 4.4(b) – allowing the initial application to freeze or seize criminal property and property of corresponding value to be made *ex parte* or without prior notice. The powers bestowed upon police officers to use restraint and charging orders can be done without notice to the affected person (S35(1,4), CPC). Moreover, the Public Prosecutor can make an ex parte application for a restraint order against any realisable property (S 19(4)(a)-(b), CDSA). Realisable property is defined as any property held by the defendant and any property held by a person to whom the defendant has, directly or indirectly, made a gift. In respect of TF offences, the Public Prosecutor can make an ex parte application for a warrant to search for, seize or restrain the dealing with any property which the authorities have reasonable grounds to believe may be forfeited (S 11, TSOFA).

Sub-criterion 4.4(c) - ensuring that provisional measures do not have unreasonable or unduly restrictive conditions for effective action. Competent authorities can take immediate action to freeze or seize property without a court order (see c.4.4a) and can use a lower burden of proof based on 'reasonable grounds to believe' to prove that property constitutes benefits of drug dealing or criminal conduct (S 56(1-2), CDSA, see also c.3.5).

Criterion 4.5 –

Singapore enables competent authorities to freeze and seize criminal property and property of corresponding value without a court order when it is necessary to act as expeditiously as possible (S35(1,4), S370, CPC, S24(1), S26 MDA). The law enforcement officer who seizes property pursuant to S35 CPC must make a report of the seizure to the Court one year after the date of seizure or sooner to ask for continued seizure or the release of the seized property (S370(1), CPC). Individuals affected by the seizure can also challenge the action at any time and apply for the release of property in Court, which must be satisfied that doing so is necessary for the payment of basic expenses, to reimburse professional fees, etc. (S35(7-8), CPC).

Criterion 4.6 –

Singapore has measures, including legislative measures, that enable their competent authorities to take steps that will prevent or void actions that prejudice the country's ability to freeze, seize or confiscate criminal property and property of corresponding value. 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), CPC). Courts can also direct that seized property continue to be under custody of relevant law enforcement agency where the person entitled to the property cannot be ascertained or found (S372, CPC). A police officer may seize, or prohibit the disposal of or dealing in, any property to prevent its dissipation. To ensure Singapore is able recover property that is subject to confiscation, sections 15(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. With respect to TF offences, 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 (S, 29, TSOFA). A judge may also apply interim preservation rights (S28, TSOFA).

Confiscation

Criterion 4.7 –

Singapore has measures, including legislative measures, to enable the confiscation of criminal property and property of corresponding value after a person is convicted. Confiscation of benefits from criminal conduct is mandatory where a defendant is convicted of either one or more drug offence(s), or one or more serious offence(s), including ML, predicate offences and TF, and the court is satisfied that the defendant derived benefits from this criminal conduct (S6(1)-7(1) and S34-35, CDSA). 'Benefits' is defined broadly to include any property or interest in a property held by the defendant at any time, being property or interest disproportionate to the person's known sources of income and the holding of which cannot be explained to the satisfaction of the court, whether located in Singapore or abroad (S3(5), S10(1)-11(1), CDSA). Additional forfeiture and confiscation powers are set out in the legislation (S364, CPC, S27-28-29 MDA, S48 and 61, OCA, S64, CDSA. (For CBCRR offences see R.32). Under the CPC, the Courts may order the disposal of property during or at the conclusion of any inquiry or trial, including the forfeiture and confiscation of property laundered or proceeds of ML (S364, CPC). Additional confiscation powers are available under the MDA (S27-29), Gambling Control Act (S40-41), and TSOFA (S24). Upon application by the Public Prosecutor, Courts can also order the confiscation of property of corresponding value (called 'substitute confiscation orders') for drug dealing or serious offences (Part 4A, S33, CDSA, S 21, TSOFA). The wording of S18-19, CDSA refers to the restraint of 'any property', which is sufficiently broad to include property of corresponding value.

Criterion 4.8 –

Singapore enables the confiscation to be extended to other property of a person convicted of ML, predicate offence or TF where the court is satisfied that such property is derived from criminal conduct. Singapore's definition of property is broad, in line with the prevailing definition of criminal property in the FATF Glossary (see c3.4). If a person holds or has held property or interest in any property (including income accruing from such property or interest) disproportionate to a person's known source of income which cannot be explained to the satisfaction of the court, until provided to the contrary, this is presumed to be derived from criminal conduct and can be confiscated (S6(6), 7(6), 10(1) and 11(1), CDSA). In practice, forensic accountants within LEAs conduct 'unexplained wealth' or 'concealed income analysis' on the known income sources of the defendant to identify potential criminal benefits derived by the defendant for confiscation. As the confiscation order is made against the defendant personally, this can extend to other assets of the defendant and allows agencies to confiscate property of corresponding value.

Criterion 4.9 –

Singapore has measures, including legislative measures, to enable the confiscation of criminal property without requiring a criminal conviction in relation to a case involving ML or predicate offences. With respect to TF, where a court is satisfied on a balance of probabilities, that property is owned or controlled by a terrorist or a terrorist entity, it will order the forfeiture of the same to the Government without the need for a criminal conviction (S 21(a), 24 TSOFA). In all cases, confiscation is foreseen for persons that have absconded or died in the course of an investigation (S 29-31, CDSA, S63. OCA, S370, 372 CPC). The Public Prosecutor can also apply to the Courts for a confiscation order when a subject engages in and derives benefits from 'organised crime activity' – defined as a serious offence. (S 48, 51, 61, OCA).

Asset recovery and tax authorities

Criterion 4.10 –

With a view to enhancing asset recovery efforts and supporting the identification of criminal property, Singapore enables their competent authorities and tax authorities to co-operate, co-ordinate and share information domestically (see c.4.1d). The Inland Revenue Authority of Singapore (IRAS) has powers to recover tax (it has civil recovery powers) and can share domestic tax information with other LEAs to facilitate investigations or prosecutions of serious offences (S610(B) and Part 19, ITA, S6C, GDSA, S16A(5), FTZA). Singapore's competent authorities and tax authorities have access to STRs submitted by REs and can access financial intelligence hosted in STRO's database for AML/CFT investigations, regulatory work or for their own purposes (e.g. tax investigations in the case of IRAS) (see R.29).

Asset management, return and disposal

Criterion 4.11 –

Singapore has mechanisms for managing, preserving and, when necessary, disposing of, frozen, seized, or confiscated property, including, where appropriate, the pre-confiscation sale of property. There is no asset management office as such. Confiscated assets are the custody of competent authorities who seize them (S 35, CPC). A court may order the release (sale) of any seized property on certain conditions (e.g. to pay for basic living or medical expenses, reasonable reimbursement of legal fees, etc.), or upon conclusion of legal proceedings (S 35(7), S 364-370 CPC, as amended by S 14-17, MLA). The High Court may also order the sale of any property that is caught by a restraint order provided the Court is satisfied that the value of the property is likely to depreciate, or undue costs are involved in maintaining the property, or the sale would be in the interest of justice (S19A, CDSA). The proceeds from the sale of forfeited criminal assets, along with any forfeited cash are deposited into the Consolidated Fund, which is centrally managed by the Accountant General's Department, on behalf of the Singapore Government (Article 145 of the Constitution of the Republic of Singapore). The WoG Guidelines on Asset Management and Crypto-Assets provide LEAs further guidance and best practices on managing assets, including highly depreciative assets or assets with high maintenance costs. The guidelines direct LEAs to bank any seized currency/BNI into the Accountant General Department's account.

Criterion 4.12 –

Singapore has measures that enable authorities to enforce a confiscation order and realise the property or value subject to the confiscation order, leading to the permanent deprivation of the property or value subject to the order. The High Court may make a restraint order to prohibit any person from dealing with any realisable property and appoint the Public Trustee or any person as a receiver to realise the property in respect of the confiscation order (S19(1) and S22, CDSA). The Court can also order property to be forfeited to the State where no person makes a claim to the property (S375(5,7), CPC, S24,25, TSOFA). CNB officers can also exercise the powers to forfeit and dispose of drug assets (S27-29, MDA).

Criterion 4.13 –

Singapore has mechanisms to:

Sub-criterion 4.13(a) - Return confiscated property to prior legitimate owners (S370(2)(d-e), CPC). Once legal proceedings are completed, authorities will promptly dispose of the seized assets. In the course of investigations, the investigating agency will identify parties that appear to have an interest in the property on a best effort basis.

Sub-criterion 4.13(b) - Use confiscated property to compensate victims of crime. Under S 364 and 370, CPC, a Court can order the disposal of property and/or the use of property for compensation or restitution. In this circumstance, as directed by SOPs, LEAs can use the seized assets/property to restitute funds to victims, and Singapore provided case studies showing this occurs in practice (paragraphs 21 to 27, WoG Guidelines on Asset Management). Case studies also show that Singapore can facilitate the use of voluntary restitution by offenders to reimburse victims and restitute funds to foreign jurisdictions in transnational cases for the purpose of victim compensation (Box Story 14 and 20, 2024 National Asset Recovery Strategy, 2024) (see R.38).

> *Weighting and conclusion –* Singapore's legal framework broadly covers the requirement of R.4 concerning confiscation and provisional measures. The application of provisional measures for up to one year is also too long and inconsistent with an emergency measure. These are minor deficiencies.
>
> Recommendation 4 is rated **Largely Compliant**.

Recommendation 5 – Terrorist financing offence[48]

In the 4th round MER, Singapore was rated Largely Compliant on R.5. The deficiency was that the criminal sanctions available for legal persons convicted of the TF offence and persons convicted of TF ancillary offences were too low to be sufficiently dissuasive.

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, 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

[48] Recommendation 5 was not under review. Therefore, the text for the Recommendation is copied from MER 2016 and FUR 2019, with minor non-substantive edits included from Singapore.

terrorist, 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 c.5.4 below).

Criterion 5.2^{bis} - The TF offence under the TSOFA meets the requirement of criterion 5.2^{bis} and includes the travel of individuals for the purpose of the perpetration, planning, or preparation of, or participation in terrorist acts or the providing or receiving of terrorist financing.

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 be 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 c.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 (370 000), 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. Section 6B of the TSOFA increased the penalty for ancillary offences by making a person who abets, conspires or attempts to commit a terrorism financing offence under section 3, 4, 5 or 6 of the Act to be liable to the same punishment as if the person had committed the offence under the applicable section.

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 c.3.10). The maximum criminal fine available for legal persons is

SGD1 million (USD774 700) or twice the value of the property (including funds derived or generated from the property), financial services or other related services, or financial transaction, as the case may be, in respect of which the offence was committed. 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.

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).

Criterion 5.11 –

> *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 are too low to be sufficiently dissuasive.
>
> Recommendation 5 is rated **Largely Compliant**.

Recommendation 6 – Targeted financial sanctions related to terrorism and terrorist financing [49]

In the 4th round MER, Singapore was rated Largely Compliant with R.6. The main shortcoming related to PSMDs not being subject to supervision by the competent authorities and the competent authorities receiving information indirectly from any persons who were required to report terrorist property to the Commissioner of Police.

Identifying and designating

Criterion 6.1 –

Sub-criterion 6.1(a) - Singapore has designated the 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. MHA also serves as the Secretariat to the IMC-TD.

Sub-criterion 6.1(b) - The IMC-TD SOP sets out mechanism(s) for identifying targets for designation that is based on the designation criteria set out in the relevant UNSCRs.

Sub-criterion 6.1(c) - The IMC-TD designates a terrorist based on the definition provided in Section 2 of

[49] Recommendation 6 is newly assessed, as Singapore has made legal, regulatory or operational framework changes since its last mutual evaluation.

the TSOFA. There is no specific threshold in the mechanism for designation that requires an evidentiary standard of proof of "reasonable grounds" or "reasonable basis" when deciding whether or not to make a proposal for designation; and there is nothing ensuring designations are not conditional upon the existence of a criminal proceeding. However, the common law basis for judicial review for the decision is the "reasonable person" test whereby the court must find that no reasonable person could have made the decision.

Sub-criteria 6.1(d, e) - Designations are proposed to the UN through MFA who will submit the completed standard UN designation form containing (a) the relevant information on the proposed person/entity and (b) a statement of the case for designation with details on the basis for the proposed listing. MFA will contact the state(s) of residence and/or nationality of the individual/entity concerned to seek additional information, if required.

Criterion 6.2 –

Sub-criterion 6.2(a) - In the case of designations pursuant to UNSCR 1373, the relevant IMC-TD agencies are to make proposals for designation, and the proposals are to be considered by the IMC-TD prior to surfacing to the Minister for Home Affairs' approval. Once designations are made, the information is promptly provided to reporting entities via a gazette on the public-facing Singapore Statutes Online website, and email advisories/alerts by MAS and supervisory authorities of DNFBPs within 24 hours.

Sub-criterion 6.2(b) – Proposals are made by the ISD, which is surfaced through MHA as the IMC-TD Secretariat, and it is considered by the members of the IMC-TD, who may then evaluate if that designation is merited, prior to surfacing to the Minister for Home Affairs for approval pursuant to Section 38(a) of the TSOFA. The IMC-TD SOP sets out mechanism(s) for identifying targets for designation that is based on the designation criteria set out in UNSCR 1373.

Sub-criterion 6.2(c, d) - The IMC-TD SOP specifies that foreign countries may also make requests to Singapore for persons/entities to be designated under UNSCR 1373. This will be done through MFA and/or other appropriate international co-operation channels and will be assessed by the IMC-TD. As the competent authority, the IMC-TD will determine if there are reasonable grounds or basis for each designation, including requests made by foreign countries. Chairman of IMC-TD will then seek the approval of the Minister for Home Affairs upon determining there are reasonable grounds or basis for the terrorist designation.

Sub-criterion 6.2(e) - For such outgoing requests, ISD and/or relevant agencies will provide as much relevant information as possible to facilitate the foreign country/jurisdiction's designation process.

Criterion 6.3 –

Sub-criterion 6.3(a) - Law enforcement officers have powers under the CPC (Sections 20-21, 22(1)-23(1), 32-34), 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 and relevant procedures can operate ex parte against a person or entity who has been identified and whose proposal for designation is being considered.

Freezing

Criterion 6.4 –

Dealings with any property owned or controlled by any terrorist or terrorist entity, including persons/entities listed in the First Schedule to the TSOFA are prohibited by Section 6(1) of the TSOFA. Further, section 4(1)(b) creates an offence if a person makes property available knowing or having

reasonable grounds to believe that, in whole or in part, they will be used by or will benefit any terrorist or terrorist entity.

All UNSC 1267 designations are automatically included in the First Schedule of the TSOFA; however, to take into account the time difference between Singapore and New York, the law only takes effect in Singapore on the date immediately following the date of addition to the UN list. For domestic 1373 designations, the freezing obligation takes immediate effect after gazetting. Requests by another country for domestic designations in Singapore pursuant to UNSCR 1373 proceed under the IMC-TD SOP and bring designated persons/entities to the First Schedule of TSOFA as per section 38(a) and are again captured by section 6.1(c).

Criterion 6.5 –

Sub-criterion 6.5(a), (b), (c) - TSOFA Section 6(1) contains a comprehensive prohibition against dealing that operates as a mechanism requiring asset freezing without delay.

TSOFA Sections 4 and 5 prohibit directly or indirectly using, possessing and providing property and services for terrorist purposes, and section 6 of the TSOFA prohibits dealing in property of terrorists and terrorist entities. The definition of property in Section 2 of the TSOFA is broad enough to encompass "any funds or other assets, economic resources, or financial or other related services".

As per section 6(1) of the TSOFA, no person in Singapore and no citizen of Singapore outside Singapore may deal, directly or indirectly, in any property that the person knows or has reasonable grounds to believe is owned or controlled by or on behalf of any terrorist or terrorist entity. TSOFA Section 6.1(c) prohibits provision of any financial services or any other related services in respect of any property to or on the direction or order of any terrorist or terrorist activity. However, there is no specific inclusion of property that is owned "wholly or jointly" by a designated person or entity (indirectly or directly).

Sub-criterion 6.5(d) - MAS and DNFBP supervisors communicate designations to FIs and DNFBPs through gazetting on the public-facing Singapore Statutes Online website, the MAS webpage and an email advisory/update from MAS and DNFBP supervisors to their regulated entities which contains guidance and links to the consolidated websites, including MHA's IMC-TD webpage[50].

Sub-criterion 6.5(e) - Section 8.1 of the TSOFA also requires that anyone who has "possession, custody or control" of any property or information of any transaction or proposed transaction in respect of any property belonging to any terrorist must report the information to the Commissioner of Police. This obligation to report is mandatory.

Sub-criterion 6.5(f) - There is no provision that protects the rights of bona fide third parties acting in good faith when implementing the obligations under R.6 (TFS related freezing). While sections 11, 19 and 24 allow for protection in the case of seizure or forfeiture, these are not related to good faith activities related to freezing.

Criterion 6.6 –

Sub-criteria 6.6(a) - (f) - The CTF section of the MHA website outlines the following avenues for designated individuals, groups, undertakings or entities to seek review or appeal for de-listing:

- For those designated pursuant to UNSCRs 1267, 1988 and 1989, the public-facing MHA website directs those who wish to submit a de-listing request to the independent Ombudsperson via a link to the UN Sanctions Committee's website.[1]
- For those domestically designated pursuant to UNSCR 1373, the MHA website directs designated persons or entities to write to MHA to request de-listing and unfreezing of the funds or other assets

[50]Countering the Financing of Terrorism:https://www.mha.gov.sg/what-we-do/managing-security-threats/countering-the-financing-of-terrorism

of persons and entities which do not, or longer, meet the criteria for designation pursuant to UNSCR 1373.

The MHA IMC-TD public-facing website[1] provides links to the relevant "Sanctions Committee website" for International UN Designations, be it pursuant to UNSCR 1267/1989 or UNSCR 1988, for a de-listing request. The MHA website outlines that once a person or entity has been de-listed as a terrorist, his/her funds or assets can be unfrozen as the obligation to keep these frozen no longer exists. The MHA IMC-TD public-facing webpage outlines the mechanisms available for persons or entities, including (i) the information required to support the appeal for the unfreezing of funds/de-listing, and (ii) directly stating that: *"Anyone, including designated persons or entities, may also contact MHA if they* ***inadvertently had their funds or assets frozen*** *under the above-mentioned UNSCR; for example,* ***because of a false positive."***

Sub-criterion 6.6(g) - The practice in Singapore is for delistings to go through the IMC-TD, MFA and then gazettal on the public-facing Singapore Statutes Online webpage. The public-facing Singapore Statutes Online webpage is also connected to MASnet which has FIs and DNFBPs as subscribers. Most sectors have 100% of their population subscribed to MASnet. For the few DNFBP sectors that do not have a 100% subscription rate, the sector supervisor communicates with each member of the sector.

De-listing, unfreezing and providing access to frozen funds or other assets

Criterion 6.7 –

It is noted that Section 7 of the TSOFA allows the Minister of Home Affairs to exempt any person from sections 4(1)(b) or 6 or both, in respect of any specified activity or transaction or a class of specified activities or transactions carried out by the person or citizen. This provision directly addresses basic expenses, for the payment of certain types of fees, expenses and service charges, or for extraordinary expenses, in accordance with the procedures set out in UNSCR 1452 and any successor resolutions.

> ***Weighting and conclusion –*** Singapore has a robust legal framework identifying, designating and freezing in relation to TF TFS under the Terrorism (Suppression of Financing) Act 2002. The IMC-TD (MHA) is the competent authority for proposing designations pursuant to UNSCR 1267 and UNSCR 1373. The IMC-TD is led by MHA, with participation of SPF (CAD), MFA, AGC and MAS. In relation to asset freezing, there is no explicit provision to clarify that the prohibition against dealing requires that the subject not be given prior notice, and that the prohibition extends to property that is owned "wholly or jointly" by a designated person or entity. There are no provisions under the laws governing TF TFS related to bona fide rights of third parties. Recommendation 6 is rated **Largely Compliant**.

Recommendation 7 – Targeted financial sanctions related to proliferation[51]

In the 4th round MER, Singapore was rated Largely Compliant on R.7. The deficiency was in relation to no provision in accordance with the exemptions under the UNSCRs and the implementation was left to discretion of the authorities.

[51] Recommendation 7 was not under review. Therefore, the text for the Recommendation is copied from MER 2016, with minor non-substantive edits included from Singapore.

Criterion 7.1 –

Singapore implements provisions in relation to targeted financial sanctions pursuant to UNSCRs against DPRK in accordance with the MAS Financial Services and Markets regulations and Variable Capital Companies (VCC) regulations (for FIs supervised by MAS)[52] and UN regulations (for the general public, including DNFBPs and money lenders). 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 the respective regulations and cover all types of funds and other assets, regardless of the type of ownership or possession (see section 13 of the MAS DPRK regulations, section 8 of the VCC regulations and sections 9 and 10 of the UN DPRK regulations).
- *Sub-criterion 7.2(d)* - The MAS and UN DPRK Regulations collectively apply to any person in Singapore and any Singapore citizen outside Singapore, including FIs 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 18 for DPRK) or the police (UN Regulations section 14 for DPRK).
- *Sub-criterion 7.2(f)* - Bona fide third parties are protected by law for complying with any MAS regulations (section 15(3) Financial Services and Markets Act 2022 (FSM Act), section 83(3) Variable Capital Companies Act 2018 (VCC Act)) or UN regulations (section 3 UN Act 2001).

Criterion 7.3 –

For FIs, MAS supervises compliance with the MAS DPRK regulations (section 15(5) FSM Act, section 83(5) VCC Act). A breach of the regulations is considered an offence, punishable by a fine not exceeding SGD 1 million (USD 740 000). For DNFBPs, the UN Act 2001 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 (USD370 000) 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 (USD 740 000).

Criterion 7.4 –

- *Sub-criterion 7.4(a)* - The MAS website contains all the necessary information for delisting, including a link 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 FSM Act (section 189) and the VCC Act (section 95) allow MAS to grant exemptions from its regulations such as the MAS regulations issued under the FSM Act and VCC Act respectively, and they also contain the exemption conditions set out in UNSCR 1718. For non-MAS-regulated entities, the UN Regulations contain the correct conditional exemptions (section 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) which is the mechanism for communicating de-listings to the FIs and the DNFBPs. Unfreezings will be resolved with the relevant

[52] Financial Services and Markets (Sanctions and Freezing of Assets of Persons — Democratic People's Republic of Korea) Regulations (2023) [https://sso.agc.gov.sg/SL/FSMA2022-S235-2023?DocDate=20230426] and Variable Capital Companies (Sanctions and Freezing of Assets of Persons) Regulations (2020) [https://sso.agc.gov.sg/SL/VCCA2018-S29-2020?DocDate=20230426]

parties, including the FIs and DNFBPs that may have mistakenly frozen the funds and assets of the false positives.

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 FSM Act, VCC Act and UN 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 explicit provision in accordance with the exemptions under the UNSCRs. Recommendation 7 is rated **Largely Compliant**.

Recommandation 8 – Non-profit organisations (NPOs) [53]

In the 4th round MER, Singapore was rated Largely Compliant with R.8. Whilst there were a variety of government institutions involved in the supervision of NPOs and necessary co-operation and co-ordination mechanisms were in place, the MER noted there was no clear articulation of a central contact point with respect to NPOs. The MER also noted that Singapore's ability to conduct TF investigations on organisations at risk could be enhanced by further knowledge on TF matters particularly within those institutions responsible for the supervision of NPOs.

Taking a risk-based approach

Criterion 8.1 –

Sub-criterion 8.1(a) – As part of the sectoral vulnerability assessment conducted by each NPO regulator

Singapore has identified the subset of organisations that falls within the FATF definition of NPOs. As of 31 December 2023, there are 2 659 entities falling within the FATF definition of NPO (see Table 1 below), of which approximately 200 have been identified as the high-risk subset.

Table 1: Breakdown of the number of NPOs by regulator (as of 31 December 2023)

NPO regulator	COC	ACRA	MUIS			ROS	Total
Type of NPO	Charities	CLGs (NPO)*	Mosque	Madrasah	WMS	Societies (NPO)*	
Number of NPOs	2 398	122*	70	6	1	62*	2 659

* Comprise CLGs and societies that fall within the FATF definition of NPO but not registered as a charity under the Charities Act 1994 (Charities Act).

Sub-criterion 8.1(b) - The Singapore TF NRAs 2020 and 2024 include a section on NPOs and conclude that NPOs pose a medium-low risk of TF abuse.

Sub-criterion 8.1(c) - Based on the 2024 TF Threat Assessment and TF Vulnerability Assessment for the NPO sector, charities that have higher exposure to overseas activities (relative to other NPOs) are assessed to be of relatively higher risk of TF abuse. Regulation 21(1) of the Charities (Fund-raising Appeals for Local

[53] Recommendation 8 is newly assessed due to changes to the FATF Standards for which Singapore has not previously been assessed.

and Foreign Charitable Purposes) Regulations 2012[54] (Fund-raising Regulations)stipulates the requirement for any person who wishes to conduct or participate in any fund-raising appeal for foreign charitable purpose(s) to apply to the COC for a permit (FRFCP permit). This applies to all NPOs but NPOs that are part of the high risk subset have more reporting requirements than other NPOs. Accordingly, proportionate mitigation measures have been implemented by the COC, as currently described.

Sustained outreach concerning terrorist financing issues

Criterion 8.2 –

Sub-criterion 8.2(a) - NPOs in Singapore are subjected to regulatory requirements to promote accountability, integrity and public confidence in the administration and management of NPOs.

Charities

The COC regulates the charity sector in Singapore supported by five Sector Administrators (SAs) from the Ministry of Education, Ministry of Health, Ministry of Social and Family Development, Sport Singapore and People's Association. The SAs supervise registered charities that are established for charitable purposes that fall under the mandate of the respective government agencies (education, health, social and welfare, sports, and community development), and the remaining charities come under the direct supervision of the COC (Section 41 of the Charities Act). Section 7(8) of the Charities Act mandates all institutions established for charitable purposes to apply for registration as charities. It further requires all charities to notify the COC of changes in the governing board members, key officers and trustees, as well as amendments to the governing instrument of charities.

The Charities Act was amended in 2018 to provide for the disqualification of individuals from acting in the capacity as governing board members, key officers, and trustees of a charity, if he/she has been convicted of any offence involving terrorism, TF, or ML, under Section 28 of the Charities Act. The COC conducts periodic screening to ensure such individuals do not gain control of the management and administration of charities. In a lower risk environment, this is a reasonable mitigation to the risks of illicit abuse of charities and charitable resources in support of terrorism and TF.

The Fund-raising Regulations regulate local fund-raising activities for charitable, benevolent or philanthropic purposes (including those conducted by third parties for charities) and fund-raising activities for foreign charitable purposes. The Fund-raising Regulations set out the legislative requirements for proper accountability of funds and clear representation in the conduct of fund-raising activities, including the purpose and intended beneficiaries. Such requirements are also applied to fund-raising activities conducted by non-registered charities, including the CLGs and societies.

CLGs

ACRA is the corporate regulatory authority and the Registrar of Companies in Singapore. CLGs are subject to the same regulatory and reporting requirements under the Companies Act, as other company types regulated by ACRA. Such reporting requirements include filing annual returns (Section 197(1) of the Companies Act), filing information in the registers of beneficial owners (BO) with the central BO registry (Section 386AN(1) and (2) of the Companies Act) maintained by ACRA and requiring financial statements of CLGs to be audited, unless exempted (Section 205(1) of the Companies Act).

Under Sections 175 and 179 of the Companies Act, CLGs are required to hold Annual General Meetings (AGM), before filing annual returns with ACRA. Additionally, Section 201 of the Companies Act requires the directors of every company, including CLGs, to present the financial statements for the year at its AGM. The AGM serves as an important platform to increase the accountability of the management of CLGs, where

[54] Charities (Fund-raising Appeals for Local and Foreign Charitable Purposes) Regulations 2012 - https://sso.agc.gov.sg/SL/CA1994-S530-2012

the CLGs address members' concerns. The annual returns of CLGs include its financial statements, which are made publicly available[55], promoting corporate transparency of CLGs.

Mosques, Madrasahs and WMS

Mosques, madrasahs and Wakaf Masyarakat Singapura (WMS) are administered by Majlis Ugama Islam Singapura (MUIS) under the Administration of Muslim Law Act (AMLA). MUIS is a statutory board of the Singapore Government and its Council, being the overall decision-making body, is appointed by the President of Singapore, with recommendation from the Minister-in-charge of Muslim Affairs. MUIS has established the Mosque Financial Regulations (MFR), Financial and Procurement and Payment Guidelines for Mosque, Madrasah, Wakaf and Zakat (MMWZ) operations to provide guidance to mosques and madrasahs on financial controls and proper governance. Mosques and madrasahs are required to comply with the MFR and Financial, Procurement and Payment Guidelines for MMWZ Operations established by MUIS. For WMS, the Administration of Muslim Law (Majlis Wakaf) Rules 2024 (AMLA Majlis Wakaf Rules) under the AMLA stipulates its management, which include the maintenance of records, preparation of financial statements and governance relating to its acceptance of contributions.

Schedule 2 of the AMLA requires all mosques and the WMS to keep proper accounts and records of its transactions and affairs. Additionally, mosques are required to comply with the MFR, which are reviewed by professional external auditors appointed by MUIS during the annual audit of the financial statements of mosques. Under the provisions of the AMLA, the audited financial statements of mosques must be submitted to MUIS no later than six months from the close of the financial year. The financial statements of the WMS must be submitted to MUIS no later than three months from the close of the financial year. Under the agreements of the Joint Madrasah System (JMS), the audited financial statements of madrasahs are to be submitted to MUIS no later than six months from the close of the financial year.

Societies

Under the Societies Act, societies must maintain proper accounts and records of their transactions and affairs and must submit an Annual Return including audited accounts to ROS. Societies are also required to submit their audited Statement of Accounts within 60 days of the conclusion of any fund-raising appeal. These statutory requirements allow for closer monitoring of the societies' financial activities. Societies are also required to apply to ROS to change its name, place of business and constitution.

Sub-criterion 8.2 (b), (c) – The relevant agencies undertake outreach and educational programmes, work with NPOs to develop and refine best practices, and encourage NPOs to conduct transactions via regulated financial channels. Safer Giving campaigns target the donor community, including material on verifying the beneficiary and purpose of donations.

In February 2023, the COC launched a Terrorist Financing Risk Mitigation Toolkit for Charities (the Toolkit), which comprises a step-by-step risk assessment framework and recommended mitigating measures, to guide charities in identifying TF risks, assessing the level of risks, prioritising and mitigating the identified risks in a systematic manner. Following the launch of the Toolkit, the COC rolled out training sessions that are targeted at the higher risk charities, in particular the religious charities that conduct and support overseas activities and charitable causes, and charities that facilitate humanitarian and disaster relief work, in high-risk jurisdictions and/or near conflict zones.

MUIS conducts periodic updates for Mosque Management Board (MMB) and school leaders on mosques and madrasahs financial policies and procedures, including matters relating to TF risks and abuse. MMBs attend such trainings regularly at the start of each term of appointment and during re-appointments.

[55] The annual return and financial statements are available for a small fee via http://www.bizfile.gov.sg.

ROS has published a Code of Governance for Registered Societies that provides best practices to societies in carrying out their duties, managing society funds and properties, and a Guidance Note - Protecting Your Society against Money Laundering & Terrorist Financing (AML/CFT Guidance Note for Societies) on its website since June 2015. The AML/CFT Guidance Note for Societies seeks to increase awareness among societies of the risks of TF abuse and how they may safeguard themselves against such abuse. The AML/CFT Guidance Note for Societies is updated periodically, including in September 2024. Annually, ROS also issues email advisories to the societies about AML/CFT resources and encourages the societies to circulate such information to its members, staff, and volunteers to create awareness.

Sub-criterion 8.2(d) - In the Toolkit, Appendix D provides a list of recommended mitigating measures for charities, one of which is for charities to ensure that transactions or fund transfers are conducted via regulated financial channels to minimise diversion while funds are in transit. There are also guidances published on the Charity Portal, one of which was titled "How Charities can Safeguard Against Terrorist Financing". The guidance highlighted that charities should ensure that transactions are conducted via regulated financial channels wherever possible to minimise any potential abuse by terrorist organisations while funds are in transit.

Focused, proportionate and risk-based oversight or monitoring of NPOs

Criterion 8.3 and 8.4 (a) –

Singapore has a regulatory regime governing the licensing and reporting for NPOs. On the issue of TF risks, relevant measures are related to outreach and awareness raising. In light of the limited TF risks manifested in Singapore this is appropriate.

There are also measures where the oversight and monitoring is conducted on the basis of a categorisation of NPOs risks: Singapore requires any person who wishes to conduct or participate in any fund-raising appeal for foreign charitable purpose(s) to apply to the COC for a permit (FRFCP permit). This regime is established to allow the COC to mitigate such risks by maintaining oversight of the end-use of funds raised and focusing on those in relation to higher risk jurisdictions. In addition, where such fund-raising appeals involve foreign beneficiaries, partner(s) and/or NPOs that are located in high-risk jurisdictions and conflict zones/regions, additional security screenings are conducted with security agencies. Permit holders are required to furnish a statement of accounts in relation to the fund-raising appeal to the COC to account for the funds raised and disbursed after the conclusion of the fund-raising appeal.

Charities are required to disclose the quantum and countries where expenditure and capital outlay have been spent, remitted to, or disbursed to locations outside Singapore, as part of their annual returns (Regulation 8AA of the Charities (Accounts and Annual Report) Regulations 2011). Based on these disclosures, the COC is able to target charities that remit funds and conduct activities in high-risk jurisdictions and conflict zones for targeted outreach sessions and engagements.

Criterion 8.4 (b) –

The NPO regulators are empowered with a range of sanctions under the Charities Act, Companies Act, Societies Act and AMLA that can be applied on NPOs or persons acting on behalf of these NPOs for violations:

Charities Act

The COC can remove a charity from the register of charities and refuse the registration of an institution as a charity if it appears that the continued registration of a charity or registration of an institution as a charity, is contrary to public interest. Further, the COC has powers to act for the protection of charities after an inquiry has been instituted and that he is satisfied that there has been misconduct or mismanagement in

the administration of the charity, and it is necessary or desirable to act for the protection of the property of the charity. Amongst such actions, the COC may, by order:

a) Establish a scheme for the administration of the charity;
b) Remove or suspend trustee, governing board member, officer, agent or employee of the charity who has been responsible for or privy to the misconduct or mismanagement or has by his or her conduct contributed or facilitated it; and,
c) Restrict the transactions, which may be entered into, in administration of the charity, without approval by the COC.

The Charities Act and the Fund-raising Regulations also empower the COC to take various action against charities and persons who have conducted fund-raising including prohibiting, restricting and suspending fund-raising and sets out penalties for failure to comply with the regulatory requirements for the conduct of fund-raising appeals. Penalties for offences under the Charities Act are up to SGD 10 000 (USD 7 400) for fines; up to three years for imprisonment; disqualification of individuals who are convicted of offences involving terrorism, TF and/or ML from acting in the capacity as a governing board member, key officer and trustee for any charity under Section 28. A disqualified person would also not be able to hold any key positions in another entity which is a member or governing board member of a charity.

Companies Act

A CLG with a charitable purpose connected with persons, events or objects outside Singapore, which contravenes the Charities Act and its subsidiary regulations, may face consequences including being wound up or struck off the company register.

Additionally, CLGs are required to file their audited financial statements as part of their annual returns, unless exempted under Section 205B of the Companies Act. Where material non-compliances with accounting standards are established, ACRA can take the following actions:

a) Issue advisory letters to inform directors of the material non-compliances and encourage them to take note in the preparation of future financial statements;
b) Seek remediation actions from the company, such as revision of past financial statements;
c) Issue warning or impose composition sum against the director to deter future offence(s); and/or
d) Prosecute directors in court to deter potential offender(s).

AMLA

MUIS is empowered to remove MMB members for mismanagement of mosques and failure to comply with the provisions of rules set by MUIS. MUIS can also take actions, to rectify cases of non-compliance with the established financial policies and procedures by mosques, madrasahs and wakafs, discovered during the annual audits. Such actions may include the improvement of processes and removal of staff and MMBs of mosques as well as mutawalli/trustee of wakafs. Where financial irregularities are discovered from the annual audit, MUIS refers the findings to the LEAs for further investigation of potential criminal breaches.

Societies Act

Section 12 of the Societies Act prohibits and allows for the removal of an individual from acting as an officer of a registered society if:

a) he/she has, while being a member of a society, been convicted for an offence involving the unlawful expenditure of the funds of the society; or,

b) he/she has been declared in writing by the Minister to be unfit to act as an officer of a society by reason of any conviction for a criminal offence other than that specified in paragraph (a) unless the written permission of the Minister to do so act is first obtained.

Under Section 24 of the Societies Act, a society may be ordered to be dissolved whenever it appears to the Minister that the society is being used for unlawful purposes or for purposes prejudicial to public peace, welfare or good order in Singapore, or against Singapore's national security or interest.

In addition, NPOs are liable to criminal prosecution and penalties as legal persons under the TSOFA, which criminalises the collection, provision or use of funds with the knowledge or reasonable belief that these funds will be used to support terrorist activities. Please refer to Recommendation 5 for more details.

Effective information gathering and investigation

Criterion 8.5 –

Sub-criterion 8.5(a) - The AML/CFT SC, IAC, RTIG and specific workgroups facilitate information-sharing and exchange in relation to NPOs suspected to be involved in terrorism or TF between NPO regulators, ISD, CAD and STRO. The COC, ACRA, ROS and MUIS are members of these forums.

In August 2023, the COC and security agencies established formalised written procedures to enhance co-operation and co-ordination efforts between both agencies on conducting risk assessments, detecting and mitigation risks of abuse of higher risk charities and collaborating on TF-related outreach. In addition, there are existing written guidelines established by CAD-Counter-Financing of Terrorism Branch (CFTB) for the referral of information relating to TF, which applies to all agencies including the NPO regulators.

Sub-criterion 8.5(b) - Investigations into NPOs suspected of being involved or actively supporting the financing of terrorism are led by CAD-CFTB. Investigations into NPOs suspected of being involved or actively supporting terrorism are led by security agencies. CAD-CFTB and security agencies work closely in these investigations and are supported by the respective NPO regulators.

Sub-criterion 8.5(c) - All NPO regulators maintain information collected through annual returns regarding the administration and management of NPOs under their purview, which can be shared with LEAs to facilitate criminal investigations. Information regarding the activities of charities is published on the Charity Portal; annual returns filed by CLGs are accessible by the public via Bizfile; the list of societies registered with ROS are publicly accessible and MUIS has full access to information regarding the administration and management of mosques and JMS madrasahs via the central accounting system and database of MMB members.

Sub-criterion 8.5(d) - NPOs regulators, ISD, CAD and STRO can leverage the established mechanisms via the AML/CFT SC, IAC, RTIG and specific workgroups to facilitate sharing and exchanges of information relating to suspicion of NPOs being involved in TF abuse or used as a conduit for TF, as well as to co-ordinate preventive and investigative actions. As described in the writeup on criterion 8.5(a), the Formalised Written Procedures further facilitates prompt information sharing and co-ordination of actions between the COC, ISD, NPO regulators and LEAs including CAD-CFTB, where relevant.

Under the TSOFA, every person in Singapore (including COC, ACRA, MUIS and ROS) is required to provide information about transactions or proposed transactions relating to property, funds or other assets belonging to terrorists or terrorist entities and acts of TF through the filing of Suspicious Transaction Reports to STRO. The NPO regulators are further guided by the written guidelines established by CAD-CFTB on prompt referrals of information relating to TF.

Effective capacity to respond to international requests for information about an NPO of concern

Criterion 8.6 –

The Attorney-General's Chambers is the designated Central Authority in Singapore that processes requests for MLA. For international co-operation in relation to suspected TF or forms of terrorist support, STRO and CAD are the primary points of contact for FIU-to-FIU and TF related informal requests respectively. MHA and ISD would also be involved where the request relates to terrorism. Details regarding MLA and international co-operation are provided in Recommendations 37 and 40.

> *Weighting and conclusion –* All criteria are met.
>
> Recommendation 8 is rated **Compliant**.

Recommendation 9 – Financial institution secrecy laws[56]

In the 4th round MER, Singapore was rated Compliant on R.9.

Criterion 9.1 –

There are statutory confidentiality requirements for banks and merchant banks (s.47 of the Banking Act 1970 (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 – paras 5, 7, 8 and 9 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 4, Division 2 of the Financial Services and Markets Act 2022 (FSM 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 –* All criteria are met.
>
> Recommendation 9 is rated **Compliant**.

Recommendation 10 – Customer due diligence [57]

In the 4th round MER, Singapore was rated Compliant on R.10.

Criterion 10.1 –

The use of anonymous accounts, or accounts in fictitious names is prohibited. The Moneylenders (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing) Rules 2009 ("Moneylenders (PMTFPF) Rules") 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.

[56] Recommendation 9 is largely sourced from MER 2016 with minor non-substantive edits included from Singapore but is newly assessed only insofar as it relates to the coverage of VCCs.

[57] Recommendation 10 is largely sourced from MER 2016 with minor non-substantive edits included from Singapore but is newly assessed only insofar as it relates to the coverage of VCCs.

When CDD is required

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, capital markets intermediaries and recognised market operators[58] are required to perform CDD for occasional transactions above SGD 20 000 (USD 15 500). Given the nature and business of a VCC, where its customers are its members, the concept of occasional transaction do not exist. The thresholds for moneylenders are lower (disbursement of loans of aggregate value exceeding SGD3 000 (USD 2 320)). For payment services specified under the PS Act[59], payment service providers have to conduct CDD for transactions exceeding SGD 5 000 (USD 3 870). Remittance agents, which provide CBMT services, and DPTSPs perform CDD for all remittance and digital payment token transactions.

Required CDD measures for all customers

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 PMTFPF Rules 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 PMTFPF Rules for moneylenders, but they do not deviate from the principles above.

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 other provisions of the MAS Notices and the relevant Guidance documents, this provision meets the definition of ultimately having a controlling interest in the legal person, set out in footnote 71 to c.10.10. The MAS Notices and Directives, and the PMTFPF Rules for moneylenders explicitly provide for exemptions in relation to this requirement. These exemptions, which relate to particular types of FIs and activities, are consistent with the example in footnote 69 to c.10.10.[60]

[58] In 2019, MAS issued AML/CFT directives to organised market operators which deal with non-FI customers that trade on their organised market without going through a capital market intermediary. MAS has standardised the directive requirements under a new AML/CFT Notice for organised market operators, which came into effect on 14 January 2025.

[59] The provision of stored value facilities (SVF) and money changers (as referenced in Singapore's 2016 MER) are now treated as regulated activities of "account issuance" and "money-changing service" under the PS Act.

[60] 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

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.

Specific CDD measures required for legal persons and legal arrangements

Criterion 10.8 –

FIs 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 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 71 to c.10.10. As also mentioned above, the MAS Notices and Directives, and the PMTFPF Rules for moneylenders also explicitly provide for exemptions in relation to this requirement which are consistent with the example in footnote 69 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 PMTFPF Rules 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

respect of its beneficial owners; a FI set out in Appendix 1 to the Notices and Directives; a FI 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 FIs.

other types of legal arrangements, the persons in equivalent or similar positions must be identified.

CDD for Beneficiaries of Life Insurance Policies

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.

Timing of verification

Criterion 10.14 –

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 require FIs not to enter into any business relationship or perform any occasional transactions exceeding SGD 20 000 (USD 15 500) or an occasional cross-border wire transfer that exceeds SGD 1 500 (USD 1 160) 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 FI 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 10.15 –

Please refer to analysis under criterion 10.14.

Existing customers

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.

Risk-Based Approach

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 FI 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.

Failure to satisfactorily complete CDD

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. FIs are required to consider if the circumstances are suspicious so as to warrant the filing of an STR.

CDD and tipping-off

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 – All criteria are met.

Recommendation 10 is rated **Compliant**.

Recommendation 11 – Record-keeping[61]

In the 4th round MER, Singapore was rated Compliant on R.11.

Criterion 11.1 –

The Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 (CDSA), Financial Services and Markets Act 2022 (FSM Act) and VCC 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. 42 and 43, FSM Act: s. 16, VCC Act: s.84(3)(b)). For moneylenders, the requirement to keep CDD records is also set out in the Moneylenders (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing) Rules 2009 ("Moneylenders (PMTFPF) Rules).

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 (PMTFPF) Rules: rule 7B.

Criterion 11.2 –

The various MAS Notices and Directives and the Moneylenders (PMTFPF) Rules 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 (PMTFPF) Rules 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 (PMTFPF) Rules, FIs are required to ensure that:

- the MAS or other relevant authorities in Singapore and the internal and external auditors of the FI 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

[61] Recommendation 11 is largely sourced from MER 2016 with minor non-substantive edits included from Singapore but is newly assessed only insofar as it relates to the coverage of VCCs.

- 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 – All criteria are met.

Recommendation 11 is rated **Compliant**.

Recommendation 12 – Politically exposed persons (PEPs)[62]

In the 4th round MER, Singapore was rated Compliant on R.12.

Criterion 12.1 –

For foreign PEPs, FIs are required to implement the four additional measures set out in R.12 (risk management systems, senior management approval, establishing the source of funds/wealth, and ongoing monitoring). The text of the MAS Notices and Directives and Moneylenders (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing) Rules 2009 ("Moneylenders (PMTFPF) Rules") closely follows the text of R.12.

Criterion 12.2 –

The various Notices and Directives and Moneylenders (PMTFPF) Rules 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 Moneylenders (PMTFPF) Rules.

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 – All criteria are met. Recommendation 12 is rated **Compliant**

[62] Recommendation 12 is largely sourced from MER 2016 with minor non-substantive edits included from Singapore but is newly assessed only insofar as it relates to the coverage of VCCs.

Recommendation 13 – Correspondent banking [63]

In the 4th round MER, Singapore was rated Compliant on R.13.

Criterion 13.1 –

The FIs 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 –

FIs 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 –* All criteria are met.
>
> Recommendation 13 is rated **Compliant**.

Recommendation 14 – Money or value transfer services[64]

In the 4th round MER, Singapore was rated Largely Compliant with R.14. The last MER considered that Singapore had implemented most elements of the Recommendation, for instance MVTS are licensed and supervised by MAS, which has taken a number of initiatives to ensure that all MVTS are licensed. However, the last MER noted that the financial penalty imposed on unlicensed MVTS was relatively low. Since then, Singapore has taken measures to address these deficiencies.

Criterion 14.1 –

In Singapore, businesses providing money-changing, domestic and CBMT services are licensed, regulated and supervised by the MAS under the PS Act.

Criterion 14.2 –

Singapore uses a series of measures involving various agencies to identify natural or legal persons that provide any regulated payments services, which includes money-changing, CBMT services, and domestic money transfer services, without a licence and to raise awareness among relevant parties on this issue. CAD works closely with MAS to investigate unlicensed payment service providers, measures include: (1) physical surveillance through walkabouts; (2) detection via complaints, tip-offs and whistle blowing reports; (3)

[63] Recommendation 13 was not under review. Therefore, the text for the Recommendation is copied from MER 2016, with minor non-substantive edits included from Singapore.

[64] Recommendation 14 is newly assessed, as Singapore has made legal, regulatory or operational framework changes since its last mutual evaluation.

analysis of STRs and other intelligence; (4) referral from other agencies; (5) raising awareness among investigators; (6) outreach to payment service providers, in particular those offering CBMT services (remittance agents); (7) raising public awareness of licensing status of remittance agents; (8) outreach to the financial sector; (9) targeted efforts focused on higher risk areas/sectors (e.g. migrant foreign worker community); and (10) outreach to the general public.

Criterion 14.3 –

The Payments Department at MAS is charged with supervising holders of payment services licence.

Criterion 14.4 –

Payment service providers are 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 jurisdictions where the agents operate, upon request (Paragraph 14.4 of MAS Notice PSN01).

Criterion 14.5 –

Payment service providers are required to include all its agents in its AML/CFT programme and monitor them for compliance with its programme (Paragraph 14.2(d) of MAS Notice PSN01).

> *Weighting and conclusion –* All criteria are met.
>
> Recommendation 14 is rated **Compliant**.

Recommendation 15 – New technologies[65]

In the 4th round MER, Singapore was rated Compliant on R.15.

New technologies

Criterion 15.1 –

At country level, MAS identifies and assesses the ML/TF risks of new technological developments across the financial sector. For example, MAS published the VA RA in 2024, focusing on the threats arising from the misuse of virtual assets as well as an assessment on the sectors that are more vulnerable. For requirements on FI level, please refer to c.15.2.

Criterion 15.2 –

At FI level, MAS AML/CFT Notices require FIs 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,
- 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, and
- Pay special attention to any new products, practices and technologies that favour anonymity.

The Moneylenders (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing) Rules 2009 (Moneylenders (PMTFPF) Rules) require moneylenders to identify and assess the ML/TF/PF risks of a new product, practice, or new or developing technology for both new and existing products prior to launching or using them, and to take appropriate measures to manage and mitigate the risks.

[65] Recommendation 15 is newly assessed due to changes to the FATF Standards for which Singapore has not previously been assessed.

Virtual assets and virtual asset providers

Criterion 15.3 –

Sub-criterion 15.3(a) - Singapore updated its assessment of the ML, TF, and PF risks associated with DPT Service Providers (DPTSPs) in the 2024 ML NRA, TF NRA, and PF NRA respectively. In addition, Singapore refreshed its VA RA in 2024 to complement the NRAs.

Sub-criterion 15.3(b) - MAS adopts a risk-based approach to its AML/CFT/CPF supervision of DPTSPs, dCMP token service providers and DTSPs. Specifically for DPTSPs, Singapore has (i) adopted licensing requirements to ensure that only DPTSPs with sound controls are admitted into this sector; (ii) required CDD measures to be applicable from the first dollar (a zero threshold approach) as the ML/TF/PF risk awareness for the sector is nascent internationally, and (iii) conducted extensive AML/CFT/CPF focused outreach (both before putting in place the relevant AML/CFT/CPF requirements and on an ongoing basis) to raise industry awareness.

Sub-criterion 15.3(c) - DPTSPs, dCMP token service providers and DTSPs are required to take appropriate steps to identify, assess and understand its ML/TF/PF risks in relation to its customers, the countries/jurisdictions its customers are from or in, the countries/jurisdictions they operate in, and their products, services, transactions and delivery channels. They are also required to put in place measures which are approved by senior management to effectively manage and mitigate such risks that have been identified or notified to it by the relevant authorities in Singapore, monitor the implementation of those policies, procedures and controls, and enhance them if necessary, and perform enhanced measures where higher risks are identified to effectively manage and mitigate those higher risks. DPTSPs, dCMP token service providers and DTSPs are allowed to take simplified CDD measures where it is satisfied that the risks of ML/TF are low, and are not allowed to perform simplified CDD measures 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 or notified by relevant authorities in Singapore or other foreign authorities, or where there is suspicion that ML/TF is involved; for such cases, enhanced CDD would have to be applied.

Criterion 15.4 –

Sub-criterion 15.4(a) - In Singapore, DPTSPs, dCMP token service providers and DTSPs are required to be licensed.

Sub-criterion 15.4(b) – MAS undertakes fit and proper tests. See c.26.3 for MAS's procedures in assessing whether senior management, the directors, controllers (including beneficial owners) and substantial shareholders of FIs are fit and proper, which also apply to DPTSPs, dCMP token service providers and DTSPs.

Criterion 15.5 –

MAS detects persons conducting unlicensed financial activities through their ongoing surveillance of the financial sector and other channels (e.g. whistleblowing, complaints, referrals from other authorities and data analytics techniques). Where there are persons identified to be carrying out unlicensed financial activities, MAS would conduct checks on them to determine if there are basis to take actions against them, including referrals to the CAD of the SPF for further investigations. Such persons may also be included in the MAS Investor Alert List (IAL), to alert the public that these persons are not regulated by MAS so that investors can take the necessary precautions and refer such persons to LEAs for investigation. Singapore has a range of sanctions for unlicensed VASPs. The maximum penalty for providing DPT service without a licence is the same as that for other payment services as detailed in c.14.2.

Criterion 15.6 –

Sub-criterion 15.6(a) - MAS is Singapore's integrated financial sector regulator that regulates and supervises DPTSPs, dCMP token service providers, and DTSPs for AML/CFT, with powers designated in the FSM Act, PS Act, SFA, and FAA. Singapore adopts a risk-based approach to supervision.

Sub-criterion 15.6(b) - MAS has adequate powers to supervise or monitor and ensure compliance by VASPs (including DPTSPs, dCMP token service providers and DTSPs) with requirements to combat money laundering and terrorist financing, including powers to conduct examinations and supervisory visits, as well as off-site surveillance and auditing. MAS also reviews reports from DPTSPs, dCMP token service providers and DTSPs, such as reports from internal and external auditors as part of its assessment of the VASP's compliance with AML/CFT requirements. In the case of failing to comply with AML/CFT requirements, MAS has the power to withdraw, restrict or suspend the DPTSP, dCMP token service provider or DTSP's licence. MAS can impose regulatory and supervisory measures for all FIs (including DPTSPs, dCMP token service providers, and DTSPs) it regulates, including for AML/CFT breaches. MAS' supervisory penalties and sanctions are guided by MAS' AML/CFT Penalty Framework, which sets out the financial penalties and measures MAS would impose against FIs.

Criterion 15.7 –

MAS issued a set of guidelines to set out their supervisory expectations. In 2020, MAS also worked with the Association of Cryptocurrency Enterprises and Start-ups, Singapore (ACCESS), to publish an industry-led Code of Practice to promote regulatory compliance in AML/CFT among DPTSPs. MAS has shared observations and findings from its AML/CFT supervisory interventions 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 supervisory interventions of regulated DPTSPs, dCMP token service providers and DTSPs are communicated to the industry. Singapore have provided industry specific STR indicators to assist VASPs in detecting suspicious transactions.

Criterion 15.8 –

Singapore has a range of proportionate and dissuasive criminal, civil and administrative sanctions for FIs, including DPTSPs, dCMP token service providers or DTSPs, that fail to comply with their obligations (see c.35.1). As with the case of other FIs, these sanctions can be applied to directors and senior managers (see c.35.2).

Criterion 15.9 –

DPTSPs, dCMP token service providers and DTSPs in Singapore are required to comply with the requirements set out in Recommendations 10-21 as set out in respective MAS Notices, with the following qualifications:

Sub-criterion 15.9(a) - For DPTSPs, dCMP token service providers and DTSPs, which are assessed to be of higher ML/TF/PF risk, CDD is required for all customers and transactions and is not subjected to any designated threshold as specified in c.10.2b.

Sub-criterion 15.9(b) - DPTSPs, dCMP token service providers and DTSPs are required to ensure that value transfer of SGD 1 500 (USD 1 160) or more are accompanied by accurate originator information on the originator's address, or national identity number, or customer identification number, or date and place of birth as specified in c.16.1. This is higher than the minimum threshold allowed in R.16.

For value transfers where the beneficiary institution pays out the transferred digital token(s) (including DPTs and dCMPs) in cash or cash equivalent to the value transfer beneficiary in Singapore, a beneficiary institution shall identify and verify the identity of the value transfer beneficiary if the identity has not been previously verified, without being subjected to any designated threshold as specified in c.16.14 (Paragraph

13.13 of MAS Notice PSN02, Paragraph 10A.13 of MAS Notice SFA04-N02 and Paragraph 14.13 of MAS Notice FSM-N27).

Criterion 15.10–

Singapore has in place communication mechanisms, reporting obligations and monitoring referred to in criteria 6.5(d), 6.5(e), 6.6(g), 7.2(d), 7.2(e), 7.3 and 7.4(d) that are applicable to DPTSPs, dCMP token service providers and DTSPs.

Criterion 15.11 –

The legislative levers and co-operation mechanisms that Singapore has for FIs are applicable to virtual assets and VASPs (see R.37 and R.40).

> *Weighting and conclusion –* Singapore meets most of the criteria in relation to development of new products, practices and technologies, as well as those related to VASPs (covering DPTSPs, dCMP token service providers and DTSPs). However, minor deficiencies remain in relation to the threshold of SGD 1 500 (USD 1 160) which is (due to exchange rate fluctuations) higher than the FATF Standard threshold for capturing accurate originator information (1 000 EUR/USD).
>
> Recommendation 15 is rated **Largely Compliant**.

Recommendation 16 – Wire transfers [66]

In the 4th round MER, Singapore was rated Compliant on R.16.

Originator's financial institutions

Criterion 16.1 –

MAS Notices and Directives oblige FIs to ensure that all cross-border wire transfers of SGD 1 500 (USD 1 160) or more are accompanied by accurate originator information and beneficiary information as specified in c.16.1. This threshold of SGD 1 500 (USD 1 160) is higher than the FATF Standard threshold for capturing information (1 000 EUR/USD). If cross-border wires are bundled in a batch, the MAS Notices and Directive oblige FIs to ensure that the batch contains all the required and accurate information and is traceable.

Criterion 16.2 –

Please refer to analysis under criterion 16.1.

Criterion 16.3 –

The MAS Notices and Directive oblige FIs to ensure that cross border wire transfers below the threshold of SGD 1 500 (USD 1 160) are accompanied by accurate originator and beneficiary information.

Criterion 16.4 –

Please refer to analysis under criterion 16.3.

Criterion 16.5 –

For domestic wire transfers, the MAS Notices/Directives oblige ordering FIs to include information that is required for cross-border transfers. In case the information is not available, FIs are required to make this

[66] Recommendation 16 is newly assessed.

information available within three business days of a request by the beneficiary institution or relevant authorities.

Criterion 16.6 –

Please refer to analysis under criterion 16.5.

Criterion 16.7 –

The MAS Notices and Directive oblige FIs to collect all originator and beneficiary information and to keep the information for five years; however, the threshold for complete information in c.16.1 is higher than the FATF Standard. 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 FIs 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 FIs 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.

Criterion 16.8 –

Please refer to analysis under criterion 16.7.

Intermediary financial institutions

Criterion 16.9 –

Please refer to analysis under criterion 16.7.

Criterion 16.10 –

Please refer to analysis under criterion 16.7.

Criterion 16.11 –

Please refer to analysis under criterion 16.7.

Criterion 16.12 –

Please refer to analysis under criterion 16.7.

Beneficiary financial institutions

Criterion 16.13 –

The MAS Notices/Directive oblige beneficiary FIs 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 1 500 (USD 1 160) and if not already identified). Beneficiary FIs are also required to take reasonable measures to identify cross border wire transfers that lack the required information.

Criterion 16.14 –

Please refer to analysis under criterion 16.13.

Criterion 16.15 –

Please refer to analysis under criterion 16.13.

Money or value transfer service operators

Criterion 16.16 –

MAS Notice PSN01 obliges holders of payment services licenses for specified payment services, that is, money-changers, domestic and CBMT service providers, including their agents, to comply with all of the requirements of Recommendation 16 (noting the higher level threshold detailed above). In the case that a holder of a payment services license for money-changing and/or domestic/CBMT services 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 16.17 –

Please refer to analysis under criterion 16.16.

Implementation of targeted financial sanctions

Criterion 16.18 –

The MAS Notices/Directive oblige FIs to screen all wire transfer originator and beneficiary information against lists and information provided by the MAS. Section 15 of the Financial Services and Markets Act 2022 also obliges FIs to take freezing actions against designated persons and entities, pursuant to the relevant Regulations promulgated. Further, pursuant to the TSOFA, all persons in Singapore (including all FIs in Singapore), are prohibited from dealing with assets of any UN designated terrorists as well as persons designated by Singapore authorities.

> *Weighting and conclusion –* Most provisions are in place; however, Singapore's threshold of SGD 1 500 (USD 1 160) is (due to exchange rate fluctuations) higher than the FATF Standard threshold for capturing information (1 000 EUR/USD).
>
> Recommendation 16 is rated **Largely Compliant**.

Recommendation 17 – Reliance on third parties[67]

In the 4th round MER, Singapore was rated Compliant on R.17.

Criterion 17.1 –

MAS Notices/Directives oblige FIs 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.

Criterion17.2 –

The MAS Notices and Directives permit FIs 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

[67] Recommendation 17 is largely sourced from MER 2016 with minor non-substantive edits included from Singapore but is newly assessed only insofar as it relates to the coverage of VCCs.

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 (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing) Rules 2009 does not permit moneylenders to rely on a third party for the performance of CDD measures unless it is approved by the Registrar of Moneylenders, under the Ministry of Law (MinLaw). As part of the approval process, MinLaw 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, MinLaw 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 –* All criteria are met.
>
> Recommendation 17 is rated **Compliant**.

Recommendation 18 – Internal controls and foreign branches and subsidiaries[68]

In the 4th round MER, Singapore was rated Compliant on R.18.

Criterion 18.1 –

MAS Notices and Directives and the Moneylenders (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing) Rules 2009 (Moneylenders (PMTFPF) Rules) 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 Moneylenders (PMTFPF) Rules 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 FI'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.

[68] Recommendation 18 is largely sourced from MER 2016 with minor non-substantive edits included from Singapore but is newly assessed only insofar as it relates to the coverage of VCCs.

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 –* All criteria are met.
>
> Recommendation 18 is rated **Compliant**.

Recommendation 19 – Higher-risk countries[69]

In the 4th round MER, Singapore was rated Largely Compliant on R.19 because of concerns as to whether the required enhanced CDD provide for a sufficient wide range of measures that are proportionate to the risks in all instances.

Criterion 19.1 –

FIs 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 Moneylenders (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing Rules 2009 (Moneylenders (PMTFPF) Rules) (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 Moneylenders (PMTFPF) Rules, 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 the Ministry of Law (MinLaw) notifying the FIs of the relevant FATF documents.

[69] Recommendation 19 is largely sourced from MER 2016 with minor non-substantive edits included from Singapore but is newly assessed only insofar as it relates to the coverage of VCCs.

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 16 of the Financial Services and Markets Act 2022 (FSM 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 45(1) and 93(2)(l)(i)-(iii) of the Moneylenders Act 2008, MinLaw has similar powers in relation to moneylenders[70]. 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. MinLaw uses a similar approach to advise moneylenders about weaknesses in the AML/CFT systems of other countries[71].

> *Weighting and conclusion –* Singapore enacted changes to its system to comply with most of the requirements of Recommendation 19 for its 2016 MER. 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 transactions[72]

In the 4th round MER, Singapore was rated Largely Compliant for R.20, with the main deficiency pertaining to the timeliness in the reporting of STRs.

Criterion 20.1 –

A FI that suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity or are related to TF are required to report promptly its suspicions to Singapore's FIU (STRO) (S45(1), CDSA). The requirement to file an STR to STRO applies to 'any person' who knows or has reasonable grounds to suspect that any property represents the proceeds of drug dealing or criminal conduct, including TF, or is used/intended to be used in connection to criminal conduct. Filing an STR should be made as soon as reasonably practicable after it comes to the person's attention (S45(1), CDSA). MAS has stipulated in guidance to REs that the filing of STRs should not exceed 5 business days after the establishment of the suspicion, and no later than 1 business day after the establishment of a suspicion where an STR relates to a positive TFS sanction. This is considered adequate.

Criterion 20.2 –

FIs are required to report all suspicious transactions, including attempted transactions, regardless of the amount of the transaction. The requirements to report suspicious transactions (see c.20.1) applies regardless of whether the transaction was completed (S45(2), CDSA). This is reinforced by MAS Notices and Directives.

---

[70] The Registrar of Moneylenders has powers to issue directions under section 45(1) and the Minster for Law has powers to make rules under section 93(2) of the Moneylenders Act 2008.

[71] Each moneylender is also notified about the latest FATF public statements mentioned above via email.

[72] Recommendation 20 is newly assessed, as Singapore has made legal, regulatory or operational framework changes since its last mutual evaluation.

Weighting and conclusion – All criteria are met.

Recommendation 20 is rated **Compliant**.

Recommendation 21 – Tipping-off and confidentiality[73]

In the 4th round MER, Singapore was rated Compliant on R.21.

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 sections 45(7), 47(1), and TSOFA sections 8(5),10(4) and 10A.

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 sections 57(1) and (2) and TSOFA sections 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 57 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: Paragraphs 14.1 and 14.4; MAS Notice 626A: Paragraphs 16.1 and 16.4; MAS Notices 314, FAA-N06. SFA02-N05 and SFA13-N01: Paragraphs 12.1 and 12.4.; MAS Notices VCC-N01, SFA04-N02 and SFA03AA-N01: Paragraphs 13.1 and 13.4; MAS Notice PSN01: Paragraphs 18.1 and 18.4).

Weighting and conclusion – All criteria are met.

Recommendation 21 is rated **Compliant**.

Recommendation 22 – Designated non-financial businesses and professions (DNFBPs): customer due diligence[74]

In the 4th round MER, Singapore was rated Partially Compliant with R.22, based on deficiencies with regard to the inadequate CDD requirements applicable to casinos, real estate agents, PSMDs and accountants, and the fact that the record-keeping obligations for real estate agents and accountants were not provided by law. Since then, Singapore addressed most of the deficiencies related to public accountants and PSMDs through the legislation of the Precious Stones and Precious Metals (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing) Act 2019 (PSPM Act), and the amendments to its Accountants Act and relevant subsidiary legislation. As the deficiencies related to real estate agents and casinos remain unaddressed and given the inherently higher risk of casinos, moderate shortcomings are still affecting the DNFBP sectors and Singapore therefore remained rated Partially Compliant with R.22 in the Third Follow-up Report in 2019. Since then, Singapore has taken further steps to address the remaining deficiencies noted in the last MER.

[73] Recommendation 21 was not under review. Therefore, the text for the Recommendation is copied from MER 2016, with minor non-substantive edits included from Singapore.

[74] Recommendation 22 is newly assessed, as Singapore has made legal, regulatory or operational framework changes since its last mutual evaluation.

Criterion 22.1 –

The CDD requirements set out in R.10 are required to be applied in the following situations:

Sub-criterion 22.1(a) - Casinos: The Gambling Regulatory Authority (GRA) regulates casinos and the requirements for casinos to conduct CDD are set out in section 139(1) of the Casino Control Act 2006 and Part III of the Casino Control (Prevention of Money Laundering Terrorism Financing and Proliferation Financing) Regulations 2009. Legislative amendments were implemented in 2024 to lower the CDD threshold for financial transactions to SGD 4 000 (USD 3 000), which is in line with the FATF threshold requirement of USD/EUR 3 000.

Sub-criterion 22.1(b) - Real estate agents and salespersons (EA/RES) and developers: The CEA is the government agency that regulates Singapore's real estate agency industry. The CDD requirements are imposed on EA/RES through section 44B of the Estate Agents Act 2010 and Regulations 4, 5, 6 and 9 of the Estate Agents (Prevention of Money Laundering and Financing of Terrorism) Regulations 2021. EA/RES are now required to conduct CDD on the unrepresented counterparty involved in the property transaction to fully align CDD requirements with the FATF standards.

For developers, the Controller of Housing under the URA regulates developers selling uncompleted properties. Since 2023, developers are required to perform CDD measures on purchasers who purchase uncompleted properties from them (section 12B of the Housing Developers (Control & Licensing) Act 1965 and Part 2 of the Housing Developers (Anti-Money Laundering and Terrorism Financing) Rules 2023, and section 5A(2) of the Sale of Commercial Properties Act 1979 (SCPA) and Part 2 of the Sale of Commercial Properties (Anti-Money Laundering and Terrorism Financing) Rules). CDD is to be conducted for persons, entities or legal arrangements on whose behalf the purchaser, a natural person, is acting for (Rule 5(d) of the Housing Developers (Prevention of Money Laundering, Proliferation Financing and Terrorism Financing) Rules and Sale of Commercial Properties (Prevention of Money Laundering, Proliferation Financing and Terrorism Financing) Rules 2023).

Sub-criterion 22.1(c) - Dealers in Precious Stones and Metals (PSMDs): PSMDs are required to undertake CDD measures under section 16 of the Precious Stones and Precious Metals (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing) Act 2019 (PSPM Act) and Part 2 of the Precious Stones and Precious Metals (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing) Regulations 2019 (PSPM (PMLTFPF) Regulations) before they engage in any cash transaction with a customer above SGD 20 000 (USD 15 500) or its equivalent in value.

In 2020, amendments were made to the (PSPM (PMLTFPF) Regulations)[75] to address the deficiencies (verifying persons acting on behalf of the customer; understanding the nature of the customer's business and its ownership and control structure for customers that are legal persons or legal arrangements; and verifying the powers that regulate and bind the legal person or arrangement) as outlined in the 2019 Follow Up Report.

Additional amendments were made in May 2024 to the PSPM Act to expand the scope of precious products to include precious products priced above SGD 20 000 (USD 15 500), regardless of the value attributable to the PSPM components.

Pawnbrokers: Pawnbrokers are required under section 75 of the Pawnbrokers Act 2015 (PBA) to undertake CDD measures under paragraphs 2(1) and 2(2) of the Third Schedule of the PBA before providing a loan or making a transaction exceeding SGD 20 000 (USD 15 500).

Sub-criterion 22.1(d) – Lawyers, notaries, other independent legal professionals and accountants: For lawyers, the principle to conduct CDD is set out in section 70C of Part 5A of the Legal Profession Act 1966

[75] The PSPM (PMLTFPF) Regulations were known as the Precious Stones and Precious Metals (Prevention of Money Laundering and Terrorism Financing) Regulations 2019 (PSPM (PMLTF) Regulations) prior to December 2024, when they were amended.

(LPA), and the CDD requirements are set out in Part 2 of the Legal Profession (Prevention of Money Laundering, Financing of Terrorism and Proliferation Financing) Rules 2015 (LP (PMLFTPF) Rules). CDD is to be conducted on natural or legal persons on whose behalf a client is acting, and on natural or legal persons that are acting on behalf of a client.

Accountants[76] are required by the Accounting and Corporate Regulatory Authority (ACRA) to undertake CDD measures when they prepare for or carry out transactions for their customers under Rule 5 read with Rule 3(2) of the Accountants (Prevention of Money Laundering and Financing of Terrorism) Rules 2023 (Accountants (PMLFT) Rules) which came into effect in 2023. ISCA's Ethics Pronouncement 200 requires professional accountants to comply with the same set of AML/CFT requirements set out in the Accountants (PMLFT) Rules. Accounting service providers that carry out designated activities[77] in relation to provision of accounting services are subject to requirements described in 22.1(e) below.

Sub-criterion 22.1(e) - Trust and company service providers (TCSPs) (known in Singapore as CSPs): CSPs are required to conduct CDD in accordance with the detailed CDD requirements set out in in CSP Regulations 2025 enforced under section 17 of the CSP Act which took effect in June 2025.

Criterion 22.2 –

The record keeping requirements in c.11.2-c.11.4 are covered by the various sub-sector specific statutes. In particular, the 2019 Follow Up Report identified deficiencies that record keeping requirements for real estate agents and professional accountants are not set out in law (respectively promulgated by CEA Circular for real estate agents and EP-200 for accountants). Singapore has taken steps to address these deficiencies since then. For accountants, the requirement to maintain records on transactions and information obtained through CDD measures is set out in the Accountants (PMLFT) Rules effective from 2023, and via the CSP Act. Record keeping obligations are set out in laws and enforceable means for EA/RES (section 44C of the Estate Agents Act 2010 and Regulation 13 to 15 of the Estate Agents (PMLFT) Regulations) and newly included developers (section 12C of HDCLA, rule 15 of the Housing Developers (Anti-Money Laundering and Terrorism Financing) Rules 2023 (HD(AMLTR)R), section 5B of SCPA and rule 15 of the Sale of Commercial Properties (Anti-Money Laundering and Terrorism Financing) Rules (SCP(AMLTF)R)).

Criterion 22.3 –

The PEP requirements in c.12.1-c.12.4 are covered by the various sub-sectors' specific statutes and rules. In particular, the 2019 Follow Up Report identified deficiencies in relation to professional accountants and PSMDs which are not licensed as pawnbrokers. Since then, the EP-200 which contains the necessary requirements for professional accountants is now an enforceable means for all accountants and the obligation for PSMDs to conduct the specified CDD for PEPs is now included in the PSPM (PMLTFPF) Regulations.

Criterion 22.4 –

All DNFBPs are required to identify and assess the ML/TF/PF risks that may arise in relation to the development of new products and new business practices, as well as undertake the risk assessments prior to the launch or use of such products, practices and technologies and take appropriate measures to manage and mitigate the risks.

[76] This refers to professional accountants who are members of the Institute of Singapore Chartered Accountants and would include public accountants regulated by ACRA.

[77] Designated activities include (a) buying or selling of real estate; (b) management of client money, securities or other assets; (c) management of bank, savings or securities accounts; (d) organisation of contributions for the creation, operation or management of corporations; and (e) creation, operation or management of legal persons or legal arrangements, or buying and selling of business entities.

Criterion 22.5 –

Casino operators are not allowed to rely on third parties to perform CDD on their behalf. For other DNFBPs requirements to comply with obligations set out in R.17 in relation to reliance on third party provisions are set out in the sector specific regulations and notices.

> *Weighting and conclusion –* Singapore's Third Follow-up Report in 2019 found that most DNFBPs were subject to enforceable CDD obligations and noted deficiencies relating to casinos, EA/RES and professional accountants. Since then, Singapore has taken further steps and addressed the deficiencies through legal and regulatory amendments. All criteria are met.
>
> Recommendation 22 is rated **Compliant**.

Recommendation 23 – DNFBPS: other measures[78]

In the 4th round MER, Singapore was rated Partially Compliant with R.23, based on deficiencies in relation to enforceability of measures for accountants and limited requirements related to PSMDs. The 4th round MER also noted that in relation to high-risk countries, the provisions in laws or enforceable means did not necessarily provide a wide-range of measures proportionate to risks. Singapore had addressed some of the identified deficiencies, and was re-rated as Largely Compliant with R.23 during the 3rd Enhanced Follow-up Report in 2019.

Criterion 23.1 –

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 –

All DNFBPs have internal control requirements set out through enforceable means.

Criterion 23.3 –

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 countermeasures or has identified a country as having weaknesses in its AML/CFT regime. However, the required enhanced CDD measures in the various sector-specific statutes do not provide for a sufficient wide range of measures that are proportionate to the risks in all instances (see also c.19.1). In addition, these measures will also depend on other factors such as the DNFBP supervisors notifying the DNFBPs of the relevant FATF documents.

Criterion 23.4 –

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 are subject to obligations regarding internal controls, measures against higher-risk countries and tipping-off. 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 **Largely Compliant**.

[78] Recommendation 23 is newly assessed, as Singapore has made legal, regulatory or operational framework changes since its last mutual evaluation.

Recommendation 24 – Transparency and beneficial ownership of legal persons[79]

Singapore was rated partially compliant with R.24 in its 2016 MER. The main shortcomings noted in the 2016 MER related to: the NRA not assessing ML and TF risks associated with legal persons; gaps in foreign registered company information and residency requirements; and deficiencies in the length of time that relevant company information must be kept. The MER in 2016 further noted that Singapore permitted nominee shareholders and nominee directors and there was no legal requirement relating to disclosure to third parties of this status. Singapore addressed most of the identified deficiencies and was re-rated as largely compliant during the 3rd Enhanced Follow-up Report in 2019. There are several new requirements for R.24 under the 2022 FATF Methodology.

Scope extends to companies and other legal persons

Criterion 24.1 –

The requirements of R.24 apply to all forms of domestic legal persons in Singapore. Domestic companies (public and private), LLPs, VCCs, societies, co-operative societies and mutual benefit organisations represent the legal persons operating in Singapore. General Partnerships, Sole Proprietorships (GPs/SPs) and Limited Partnerships (LPs) also operate and are other types of legal persons in Singapore. Domestic companies, GPs/SPs, LPs, Limited Liability Partnerships (LLPs) and VCCs established in Singapore are required to be registered with ACRA, Singapore's corporate registrar and regulator.

Foreign-incorporated companies are required to be registered with ACRA if they establish a place of business or carry on a business in Singapore (registered foreign companies).[80] Once registered with ACRA, these registered foreign companies are subject to Recommendation 24 requirements.

Where a foreign company only conducts the activities prescribed under section 366(2) of the Companies Act, the foreign company is not carrying on a business in Singapore for the purposes of the Companies Act and is not required to register with ACRA. These activities include: maintaining a bank account; investing in funds; holding property; effecting any sale through an independent contractor; and any such other activity as the Minister may prescribe (s366(2), Companies Act). To date the Minister has not prescribed any other activity. The activities set out above act as Singapore's determination of 'sufficient link' to meet the minimum information requirements. The relationship between this determination and Singapore's LPRA is set out below under c24.3.

Criterion 24.2 –

ACRA's website provides information on the creation of all types, forms and basic features of legal persons in Singapore; the process for the creation of legal persons in Singapore; and the processes for obtaining and recording of basic and BO information relating to legal persons operating in Singapore.

Risk assessment and risk mitigation

Criterion 24.3 –

Sub-criterion 24.3(a) - Singapore published a *Legal Persons Risk Assessment* (2024 LPRA) in October 2024, which updated the 2019 LPRA. The 2024 LPRA builds upon the *2024 Money Laundering National Risk Assessment and the 2024 Terrorism Financing National Risk Assessment*. The LPRA assesses risk associated with all forms of legal person in Singapore. Whilst using a range of qualitative and quantitative information,

[79] Recommendation 24 is newly assessed due to changes to the FATF Standards for which Singapore has not previously been assessed.

[80] Part 11, Division 2 of the CA - section 366(1) and section 366(2) of the CA

the risk assessment did not properly analyse vulnerabilities such as how well controls are working (e.g.in light of instances of non-compliance or involvement of legal persons in ML/TF). It also lacked depth of analysis regarding unregistered foreign companies, misuse of VCCs, SFOs and in the ability to build a network of legal persons and legal arrangements to obscure BO (see Core Issue 5.1 for more detail). Some mitigations have been put in place, but these are not fully in line with Singapore's risk profile for misuse of legal persons – in particular, legal persons used in networks (see Core Issue 5.2).

Sub-criterion 24.3(b) - The LPRA rates the ML risks posed by Unregistered Foreign Companies as high and the TF risk as medium/low. The Legal Persons Risk Assessments (both 2019 and 2024) considered foreign-created companies: both those with "sufficient links" as set out in the Companies Act and therefore must register with ACRA, and those that do not and therefore are unregistered. Neither risk assessment considered the types of foreign legal entities to which Singapore is exposed to, nor the resulting risks. In particular, the criterion for sufficient connection to Singapore (that require registration) did not consider ML/TF risk as it was set over 50 years ago. Whilst finding unregistered foreign companies to be of high risk, no further mitigations have been put in place (the sole mitigation remains requiring reporting entities to apply ECDD if high risk factors are found). In particular, Singapore has set out activities that exempt non-registered foreign companies from the minimum information requirements, but these activities have not been assessed against the ML/TF risks posed by the activities (e.g. banking transactions and investing in Singapore), and whether registration could mitigate risks from these high-risk foreign companies.

Basic information

Criterion 24.4 –

All Singapore created legal persons, and foreign companies with a sufficient link to Singapore must register with ACRA and provide basic information (section 19(1) Companies Act, and Regulation 16 of the Companies (Filing of Documents) Regulations "applicable form"). There is one minor gap as there is no requirement to provide ACRA with a copy of the agreement for the LLP. Similar requirements apply for Societies, Mutual Benefit Organisation and Cooperative Societies with their respective registrars.

Criterion 24.5 –

There is no one law requiring companies to obtain and record their basic information. Instead, most of this information is inherently obtained and recorded for the company to fulfil two legislative obligations: an obligation to maintain company records, and to produce financial statements at a company's General Meeting. Taken together, these obligations may cover most but not all the basic information.

Sub-criterion 24.5(a) – Company records are defined in the Companies Act as "any register, index, minute book, accounting record, minute or other document required by the Act to be kept by a company". It is plausible, but not clear, this would include company name, proof of incorporation, legal form and status, the address of the registered office, and basic regulating powers. The financial statements required to be produced for the general meeting (which must be held at least once in a calendar year) must include a list of Directors but does not have to include a unique identifier.

Sub-criterion 24.5(b) – Private companies are not required to maintain a register of members but required to update their electronic register of members maintained with ACRA before any allotment or transfer of shares may take effect (s63(2) and s126(2), Companies Act). Public companies are required to maintain a register of members (s190, Companies Act) and keep the register at its registered office or another office in Singapore (s191(1), Companies Act). Registered foreign companies must keep a public register of its shareholders containing the names and addresses of the shareholders, the date on which each person was entered in the register as a shareholder, number of shares held, and amount paid for the shares (s380(1), Companies Act 1967). There is no requirement to obtain and record categories of shares, including the

nature of any associated voting rights. Registered foreign companies are required to update any changes to the particulars of shareholders in a register within 30 days (s380(4), Companies Act).

Section 81 of the VCC Act requires VCCs to maintain a register of members (subscribers) which includes the name, address, and shareholding detail of every member, and to keep it up-to-date. LLPs are required to maintain information (s35, LLP Act) of its partners in all material aspects within the LLP's own books and records. Co-operative societies are required to maintain a register of members and register of shares held by each member (s18, Co-operative Societies Act 1979). The Schedule to the Mutual Benefit Organisations Act 1960 prescribes that every MBO must have in its rules, requirements relating to "The keeping of a register with particulars of the age, name and address of any member or subscriber and the nominee (if any) of the member or subscriber to the organisation". As prescribed under their constitutions, Societies require their secretaries to maintain an up-to-date register of members at all times.

Sub-criterion 24.5(c) - A public company is required to maintain a register of shareholders at its registered office but may keep the register at another office of the company in Singapore or at the Singapore office of a third party responsible for maintaining the register on the company's behalf (s 191, Companies Act). Where the register is kept in an office other than the registered office, the public company must notify the ACRA Registrar of the address within 14 days and notify ACRA Register if the address changes within 14 days of the change (s191, Companies Act).

VCCs are required to maintain a register of members under section 81 of the VCC Act. The register must be kept at the registered office of the VCC but if the register is compiled and maintained at another office of the VCC in Singapore, the register may be kept at that other office (s81(7) VCC Act; s191 Companies Act). A registered foreign company is required to keep a register of its members at its registered office in Singapore or at some other place in Singapore and lodge a notice with the ACRA Registrar specifying the address at which the register of members is kept (s379(1) and (2), Companies Act). If there is any change in the address at which the public register of members is kept, the foreign company must, within 30 days after the change, lodge a notice of the change with ACRA (s379, Companies Act 1967).

Beneficial ownership information

Criterion 24.6 –

Singapore utilises a multi-pronged approach involving companies maintaining an internal Register of Registrable Controllers (internal RORC), the particulars of which must then be filed into ACRA's central RORC (central RORC); an alternative mechanism for VCCs that are not required to register BOs with ACRA; and powers to access information on BO obtained by FIs and DNFBPs as part of their CDD obligations (see R.10 and R.31).

Sub-criterion 24.6(a)

Obligation to hold own BO – adequate accurate and up to date

Domestic and foreign registered companies are required to keep a register of its registrable controllers (s386AF, Companies Act) (internal RORC**)**. Singapore's law permits registrable controllers to be a corporate controller or an individual controller. An "individual controller" of a company is an individual who has a significant interest in, or significant control over, the company or the foreign company (s386AB, Companies Act).Section 386AFA of the Companies Act provides that where a company knows or has reasonable grounds to believe that it has no ultimate beneficial owner, each director with executive control and each chief executive officer of the company is taken to be an ultimate beneficial owner, and the information of this ultimate beneficial owner has to be entered into the company's register of controllers. This complies with the interpretative note to R10.

VCCs are required to maintain an up-to-date register of beneficial owners, which is defined as the natural person who ultimately owns or controls the VCC and includes any person who exercises ultimate effective control over a legal person (paragraphs 2.1, and 7.17 to 7.20, MAS Notice VCC-N01). There is a requirement for VCC's to verify the accuracy the information obtained on beneficial owners for the purposes of the register (7.13B MAS Notice).

Accurate and up to date

The Companies Act (ss 386AI (1), 386AIA and 386AF(7), 386AK(1), and Schedule 2 of the Companies (Registers of Controllers, Nominee Directors, Nominee Shareholders and Members of Foreign Companies) Regulations 2017 set out provisions to ensure domestic and foreign companies are required to take reasonable steps to identify its registrable controllers, and maintain accurate and up to date details. However, there is not a specific requirement to verify all controllers of a legal entity that has a significant interest in, or significant control over, the company (S386AG). This means there is no obligation for the information held to be accurate.

Co-operation with competent authorities

ACRA has a range of powers to: require companies (domestic and foreign) and LLPs to produce information and documents; inspect, examine and make copies of registers; and make necessary inquiries to enforce any written law (s386AM, Companies Act 1967; s53, LLP Act). Any person failing to comply is guilty of an offence (s386AM, Companies Act 1967; s53, LLP Act). A new offence was established in 2024 that applies to a person who, in complying with ACRA's powers to inspect, examine and inquire, without exercising due diligence, provides any information that is false or misleading (s386AM(4A), Companies Act 1967; s53(4A), LLP Act) was passed in Parliament. Requirements for companies and LLPs to have a least one director/manager ordinarily resident in Singapore supports the ability of ACRA to access BO (s145, Companies Act; s29, LLP Act)., There are enforceable requirements for companies and LLPs to produce information in response to ACRA's information gathering powers in a timely manner (section 39 ACRA Act, section 386AM(4) of the Companies Act and section 53(4) of the LLP Act).

Co-operation with Fis and DNFBPs

Companies (domestic and foreign) and LLPs do not have an express obligation to co-operate with FIs and DNFBPs to provide adequate, accurate and up-to-date on BO information. However, this is somewhat mitigated by the requirement that FIs and DNFBPs must not commence or continue business relations with any customer or undertake any transaction for any customer if CDD measures cannot be completed (see R.10). Directors have been prosecuted for 'cheating' (S417 of the Penal Code) when providing false BO information to an FI.

Sub-criterion 24.6(b)(i) Singapore introduced reforms in 2020 to establish a central register of controllers of domestic and foreign companies (s386AN, Companies Act; s54, LLP Act) within ACRA (central RORC). Since 2020 all companies (domestic and foreign) and LLPs have been required to lodge with ACRA the particulars contained in their register of controllers (RORC) and notify ACRA when there are changes to the information in their register of controllers (s386AN, Companies Act 1967; s54, LLP Act). There are some gaps in ensuring information held on the central RORC is accurate and adequate (see c24.8). Singapore uses an alternative mechanism for VCCs that are not required to register BOs with ACRA. The assessment team is not satisfied that the alternative approach for VCCs is based on a documented decision that factors in risk, context and materiality.

Sub-criterion 24.6(b)(ii) - Singapore has implemented alternative mechanisms for VCCs. VCCs must engage an "eligible" financial institution (EFI) (one licensed by MAS as an FI) to carry out its AML/CFT/PF obligations (paragraph 4, MAS Notice VCC-N01). As such, the EFI must conduct CDD on the VCC and provide this information to MAS upon request. This information is likely to be adequate, accurate and up to date, but

it relies upon LEAs knowing which EFI to contact for the information. This is likely to limit efficient and timely access.

Sub-criterion 24.6(b)(iii) - Singapore law enforcement and other agencies can exercise their powers to access information on BO obtained by FIs and DNFBPs as part of their CDD obligations (see R.10 and R.31). The information recorded by FIs/DNFBPs must be made available to the relevant authority upon lawful order within a reasonable time period or any specific time period imposed by the requesting authority (section 20 of the Criminal Procedure Code).

Criterion 24.7 –

ACRA has an obligation to keep a record of all transactions with the Registrar under the scheduled laws carried out using the electronic transaction system unless otherwise ordered by an order of the court. This effectively means these records must be kept indefinitely under section 27(6)(a) of the Accounting and Corporate Regulatory Authority Act 2004 (ACRA Act).

Where a company has been struck off or dissolved, a person who was the officer of the company must ensure that the information and records of the company are retained for a person of at least five years after the date on which the company was dissolved (s344H, Companies Act 1967). Similarly, the obligation to retain information and records relating to a dissolved LLP for a period of at least 5 years after the date the LLP was dissolved is imposed on all persons who were partners or managers of the LLP immediately before the LLP was dissolved (s71, LLP Act).

The liquidator of a company or LLP has an obligation to retain the information and records relating to the affairs of the company for five years after the date of dissolution of the company (s195, Insolvency, Restructuring and Dissolution Act 2018; paragraph 67, Fifth Schedule, LLP Act).

Timely access to adequate, accurate and up-to-date information

Criterion 24.8 –

Adequate: As companies file the particulars held in their internal RORC to the central RORC, the deficiency stemming from corporator controllers (24.6(a)) also occur here, as any corporate controller (without a corresponding individual controller) listed in an internal RORC will also be listed in the central RORC. When the corporate controller is an unregistered foreign company they do not have to file their BO information with the register – as such there is inadequate information for these companies with foreign unregistered corporate controllers.

Accurate: The information filed in ACRA's central RORC is that of the company's own internal RORC, which is not verified by the company (see above). ACRA can obtain any information from a specified entity for the purpose of verifying the accuracy of any document or information in ACRA's repository and improve the accuracy of data in ACRA's registers (s30A, ACRA Act). ACRA is empowered to use information obtained from any public agency or government body (including the courts) for the purpose of reflecting the disqualification status of individuals in ACRA's register (s173F, Companies Act).

Up to date: Any change to the controllers' information must be updated in the company or LLP's register of controllers and filed with ACRA's central BO register within two business days (Second Schedule to the Companies (Registers of Controllers, Nominee Directors, Nominee Shareholders, and Members of Foreign Companies) Regulations 2017; Second Schedule to the Limited Liability Partnerships (Register of Controllers) Regulations 2022).

There are insufficient mechanisms in Singapore to ensure that basic information and BO information in the central RORC register is adequate and accurate. The primary concerns are that corporate controllers that are unregistered foreign companies do not file their BO information; and that there is no substantive process for the information on ACRA's registry to be verified for accuracy.

Criterion 24.9 –

All competent authorities have timely, direct access to the basic information filed with the ACRA Registrar as it is publicly available on the ACRA website (ss6(1)(c) and 27(1)(c), ACRA Act). The registers for societies and mutual benefit organisations are published annually, and access to the register of co-operative societies is available on the Registry of Co-operative Societies website.

S386ANA(6) of the Companies Act permits the Registrar (ACRA) to disclose any information in the central BO register upon request by a public agency if it is for the purpose of law enforcement. LEAs, including CAD, have the powers to obtain BO information from FIs, DNFBPs and any business entity registered with ACRA for their investigations. These powers allow LEAs to: ask questions on BO (ss21 and 22, CPC); compel production of BO information and at a location stipulated by the LEA for the purpose of an investigation (ss20 and 235, CPC; ss36 and 37, CDSA)); and search premises and persons for beneficial information (s34, CPC; s40, CDSA, and s11, TSOFA).

Criterion 24.10 –

Foreign companies that meet the sufficient link test in the Companies Act are required to follow the requirements relating to maintaining an internal RORC and filing into the central BO RORC. Singapore has set out a wide range of activities that exempt non-registered foreign companies from the minimum information requirements under ACRA, but this determination has not been made in the context of the ML/TF risks presented by such companies (see 24.3). Information on the BO of non-registered foreign companies is only accessible to competent authorities domestically where such information is held by FIs and DNFBPs. Singapore can request international co-operation to obtain information on unregistered foreign companies (see R.37 and R40).

Criterion 24.11 –

Basic information collected by ACRA as part of the registration process and filed in the company register is open to public inspection by any person on payment of a prescribed fee (s12(2)(a), Companies Act 1967). This provides FIs, DNFBPs and other countries' competent authorities with the ability to access basic information held on ACRA's register through the Bizfile portal (www.bizfile.gov.sg) for a prescribed fee.

Obstacles to transparency

Criterion 24.12 –

Singaporean companies are prohibited from issuing bearer shares and bearer share warrants are (s66, Companies Act). Bearer shares and bearer share warrants that existed prior to the establishment of the prohibition in 1967 have been converted to a registered form (s66, Companies Act).

Criterion 24.13 –

Nominee shareholders and nominee directors are permitted under Singaporean law. Nominee shareholders have an obligation to inform their respective companies or foreign companies (ss386ALA and 386ALB, Companies Act 1967). Companies (domestic and foreign) are required to keep a register of nominee shareholders (s386ALA, Companies Act; Regulation 10A, Companies (Registers of Controllers, Nominee Directors, Nominee Shareholders, and Members of Foreign Companies) Regulations 2017).

Nominee directors have an obligation to inform the company of their nominee status, provide prescribed particulars of the person for whom the director is a nominee, and update the company of changes in those particulars or status as nominee (s386AL(1), Companies Act 1967). Companies and foreign companies are required to keep the register of nominee directors (s386AKA(1), Companies Act; Regulation 9, Registers of Controllers, Nominee Directors, Nominee Shareholders, and Members of Foreign Companies) Regulations 2017. Amendments to the Companies Act which came into effect in June 2025 provides that, ACRA is to

keep a central register of nominee directors and a central register of nominee shareholders for domestic and companies and foreign companies (section 386ANA(1), Companies Act 1967.

Liability and sanctions

Criterion 24.14 –

Since Singapore's last mutual evaluation (when sanctions were noted as being too low to be dissuasive) most of the penalties have not changed, and some fines (for late filing) have been reduced. Penalties for new offences, outlined above, are similarly too low to be dissuasive.

Breaches of requirements relating to the register of controllers, register of nominee directors and register of nominee shareholders in Part 11A of the Companies Act 1967 and Part 6A of the LLP Act carry a fine on conviction of up to SGD 25 000 (USD 19 400) per offence.

The Companies Act was amended in 2024 to establish a new offence for providing, without exercising due diligence, any information that is false or misleading in a material manner to ACRA or an officer of ACRA or a public agency administering or enforcing any written law relating to obligations under section 386AM(1)-(2) of the Companies Act (s386AM(4A)). A maximum fine of SGD 25 000 (USD 19 400) can apply (s386AM(4A), Companies Act). to the offence of providing without exercising due diligence (section 53(1)-(2) of the LLP Act 2005), (section 386AM(4A) of the Companies Act 1967; section 53(4A) of the LLP Act 2005).

Any person who fails to comply with a direction from the ACRA Registrar to produces its register of partners under an LLP be guilty of an offence and shall be liable on conviction to a fine not exceeding SGD 5 000 (USD 3 870).

International co-operation

Criterion 24.15 –

Sub-criterion 24.15(a) - Singapore can provide and seek a wide range of international co-operation, including providing and seeking information on BO (see R.37 and R.40). The grounds for refusal are not unreasonable or unduly restrictive (see R.37 and R.40).

Sub-criterion 24.15(b) - Basic information on companies (domestic and foreign), LLPs and VCCs is available to foreign competent authorities via ACRA's online Bizfile system for the payment of the prescribed fee (www.bizfile.gov.sg).

Sub-criterion 24.15(c) - Foreign competent authorities can request information on shareholders from AGC as part of an MLA request (see R.37). LEAs and other competent authorities can utilise their direct access to ACRA's central BO register to assist foreign competent authorities with their information requirements. Beyond this, LEAs and other competent authorities can also use their investigative and enforcement powers to obtain basic and BO information from: (i) directors and shareholders/members of a company; and (ii) FIs and DNFBPs (see R.31). Sections 87 and 88 of the VCC Act, read together with the FSM Act, empower MAS to provide assistance in relation to a request for information on VCCs by a foreign AML/CFT authority. For LEAs and other competent authorities, the provisions set out in R.40 (e.g. those set out in criterion 40.2) would similarly apply for requests pertaining to information on a VCC.

Sub-criterion 24.15(d) - LEAs can assist their foreign counterparts in obtaining BO information using their powers under domestic law where the request contains reliable and sufficient information on the foreign predicate offence committed and its nexus to a possible ML offence in Singapore (section 386AN(6), Companies Act applied with Regulation 10D of the Companies (Registers of Controllers, Nominee Directors, Nominee Shareholders, and Members of Foreign Companies) Regulations), These provisions apply if LEAs

are able to show that "the information so requested is for the purpose of enabling the public agency to administer or enforce any written law or conduct public procurement".

LEAs, FIU and other competent authorities can exercise the powers of the Registrar to inspect, make copies and make inquiries relating to the register, as well as require registered companies (domestic and foreign) and LLPs to produce its register, or register of nominee directors and nominee shareholders and any document relating to those registers for the purpose of administering or enforcing any written law (s386AN, Companies Act; s53, LLP Act).

Sub-criterion 24.15(e) - Singaporean competent authorities monitor the quality of assistance (see criterion 40.4).

Sub-criterion 24.15(f) – Competent authorities can directly access the ACRA register holding basic information on companies (domestic and foreign) and LLPs, which makes basic information readily accessible. ACRA has a central registry of registrable controllers for companies (domestic and foreign) and LLPs, and companies (domestic and foreign), LLPs and VCCs have obligations to keep a register of beneficial owners, so the information is kept in a readily accessible manner (see criterion 24.6).

Sub-criterion 24.15(g) **-** The AGC is the central authority for MLA and responsible for responding to international requests for BO information, with a standard request form is available on the AGC website to facilitate and expedite the granting of MLA requests. The Inland Revenue Authority of Singapore administers the Exchange of Information on Request channel for BO information requests for tax purposes. BO information may also be provided through other informal channels which include through exchange of information between FIUs (see criterion 40.9 to 40.11), financial supervisors (see criterion 40.13 to 40.15) and law enforcement authorities (see criterion 40.18 to 40.20).

> ***Weighting and conclusion –*** Singapore provides adequate information regarding the types of legal persons that can be formed in Singapore, mechanism for their creation and processes for access to basic and beneficial information. There are also robust mechanisms, led by ACRA's registry, to ensure basic information is accessible.
>
> Singapore has recently completed a second risk assessment specific to legal persons in Singapore and found a range of risks present. This risk assessment is largely reliant on global information, international engagements, public-private collaboration and prosecution data, and would benefit from more detailed analysis of how well the controls are working and a comparison of actual use to intended use of legal persons and structures in Singapore (e.g. VCCs).
>
> Appropriate mechanisms have been put in place for nominee directors and shell companies.
>
> Singapore utilises a multi-pronged approach involving ACRA's central RORC; an alternative mechanism for VCCs that are not required to register BOs with ACRA; and powers to access information on BO obtained by FIs and DNFBPs as part of their CDD obligations (see R.10 and R.31). However, the assessment team has is not satisfied that the alternative approach for VCCs is based on a documented decision that factors in risk, context and materiality.
>
> Further, gaps in relation to verification requirements and accuracy (stemming from the central RORC being an identical copy of the legal person's own internal RORC), and ability to identify corporate controllers as BOs (without having to identify the natural person behind the corporate controller), limit the BO information accessible by competent authorities and the timeliness of such access. ACRA conducts limited examinations of legal persons to ensure accuracy of BO information and its coverage could be improved.
>
> As a large financial centre, Singapore has significant exposure to banking and financial activities by non-registered foreign companies, and there are insufficient mitigations in place. Singapore has exempted non-registered foreign companies from the minimum information requirements, without

grounding this exemption on an analysis of risk, context and materiality. Other than obtaining the CDD done by an FI or DNFBP on the non-registered Foreign Companies, Singapore does not have robust mechanisms for access to BO information. Singapore is also able to rely on international co-operation mechanisms to obtain basic and BO information from their home jurisdictions.

Recommendation 24 is rated **Partially Compliant**.

Recommendation 25 – Transparency and beneficial ownership of legal arrangements[81]

Singapore was rated partially compliant with R.25 in the 2016 MER. The main shortcoming related to a lack of enforceable obligations on trustees (including professional trustees) to collect BO information relating to a trust beyond the immediate beneficiary. Singapore was re-rated to compliant with R.25 in the follow-up report dated November 2019. There are several new requirements for R.25 under the 2022 FATF Methodology.

Scope extends to express trusts and other similar arrangements

Criterion 25.1 –

Two types of legal arrangements (as defined by the FATF) can be formed under Singapore law: express trusts, including LTCs, the Central Depository, registered business trusts (BTs), collective investment schemes (CIS), real estate investment trusts (i.e. trusts constituted under CIS that invest primarily in real estate assets), securities depositories and other express trusts such as residual trusts; and Muslim *wakafs*. Charitable purpose trusts can also be established under Singapore law and are an exception to the general rule that express trusts should be set up for the benefit of ascertainable beneficiaries. A trustee of a charitable purpose trust can only be either a LTC or a non-professional (i.e., a residual trustee). The requirements of R.25 apply to all legal arrangements operating in Singapore.

Criterion 25.2 –

The different types, forms, and basic features of legal arrangements in Singapore (express trusts, charitable trusts and *wakafs*) and the process for setting up legal arrangements in Singapore are identified, described and made publicly available on Singapore's Ministry of Law's public website. The processes for obtaining basic and BO information for trusts is provided under various legislations and made publicly available also through the Singapore Ministry of Law's public website.

Risk assessment and risk mitigation

Criterion 25.3 –

Singapore published the Legal Arrangement Risk Assessment (LARA) on 30 October 2024. The LARA assesses the ML/TF risks associated with legal arrangements including foreign legal arrangements with sufficient links with Singapore and supplements existing national ML/TF risk assessments published in 2024. The methodology for the LARA drew on case studies and typologies (mainly international), STRs, questionnaires completed by FIs and DNFBPs and open-source information. The LARA makes conclusions about when an LTC will very limited supporting analysis or evidence. There was limited analysis of the manner in which trusts with a nexus to Singapore (as per c25.3 (a) – (c)) are used in practice, and the scale of trust formation and use. In the context of a large financial centre, the LARA provides limited analysis on

[81] Recommendation 25 is newly assessed due to changes to the FATF Standards for which Singapore has not previously been assessed.

risks associated with Singaporean trusts with a foreign resident trustee, or foreign legal arrangements that have banking or investment links to Singapore. As such, the assessment team holds concerns that the risk assessment does not go into sufficiently depth into the misuse of legal arrangements in Singapore (see further Core Issue 5.1).

Many of the sectors identified as high risk and medium-high risk in Singapore's NRA regularly engage with trusts; in particular, Banks and LTCs.

Singapore has taken some steps to manage and mitigate the risks posed by foreign legal arrangements with links in Singapore (see criteria 25.4-25.12). However, overall, as set out in Core Issue 5.2, the assessment team cannot conclude that Singapore has taken appropriate steps to mitigate the ML/TF risks associated with the sectors highlighted above.

Basic and Beneficial ownership information

Criterion 25.4 –

Sub-criterion 25.4(a)

Trusts not managed by an LTC or PTC "residual trusts"

The Trustees Act 1967 (TA Act) applies to any residual express trusts and imposes obligations to obtain accurate, adequate and up-to-date BO information (Regulations 4 and 5, Trustees (Transparency and Effective Control) Regulations 2017; Regulation 7, Trustees (Transparency and Effective Control) Regulations 2017).

Trusts where a defined body is trustee

LTCs: Trusts managed by an LTC are covered under the Trust Companies Act 2005 and when acting as a trustee required to obtain accurate, adequate and up-to-date BO information through its CDD obligations (paragraphs 6.4, MAS Notice TCA-N03, paragraph 6.24, MAS Notice TCA-N03). The Guidelines then provide guidance to trust companies on the requirements in MAS Notice TCA-N03 (which has force of law).

BTs: Under section 69 of the Business Trust Act 2004 (BT Act) Trustee Managers (TMs) have obligations to maintain relevant information; and TMs are required to verify the accuracy of information.

Wakafs: MUIS, which is a government statutory board, is the trustee-equivalent for all wakafs in Singapore and the legal owner of all wakaf assets but can appoint a private mutawalli (custodian) to assist MUIS to manage the wakaf. Section 58(5)(c) of AMLA, read with reg 5(1)(b) of the Administration of Muslim Law (Mutawallis and Trustees) Rules 2018, allows MUIS to impose terms and conditions on mutawallis. These mutawallis appointed by MUIS are then responsible to register the wakaf under section 64(2) of AMLA, and maintain relevant information Clauses 1(g), (h) and (i), read with Schedule A of the Terms and Conditions of Mutawalli Appointment provides that mutawallis have to collect, verify and keep up-to-date identification information of all beneficiaries.

Charitable trusts are regulated under the Charities Act 1944 (Charities Act) and must provide particulars of the charity to the Commissioner of Charities upon registration (s7). A trustee of a charitable purpose trust can only be either a LTC, or a residual trustee, so the statutory requirements applicable to LTC and residual trustees (see above) apply to charitable purpose trusts.

Sub-criterion 25.4(b)

LTC – Where the parties to the trusts are legal persons or legal arrangements, LTCs must obtain basic and BO information of the legal person or legal arrangement. Where the trust relevant party is a legal person or legal arrangement, the LTC is required to identify the "connected parties" of the trust relevant party and obtain their names and unique identification number. Where the LTC assess the risk of the trust relevant

party are "not high" and is unable to obtain the unique identification number of the "connected party" after taking reasonable measures, the LTC may obtain the date of birth and nationality of the connected party. Where a legal person or arrangement is acting in a relevant trust position, the LTC is required to identify the (natural person) controller of that legal person/arrangement and verify the identity of that controller ((IV) Identification and Verification of Identity of Effective Controller, MAS Notice TCA-N03).

Charitable trust - A trustee of a charitable purpose trust can only be either an LTC or a residual trustee. The statutory requirements applicable to LTCs and residual trustees therefore apply to charitable purpose trusts.

Sub-criterion 25.4(c)

Trustees of residual trusts must take reasonable steps to obtain information on each person appointed or engaged as service supplier to the trust, including the name of the service supplier, registered or business address, contact details and, where the service supplier is an entity, the name of the individual authorised to act of the service supplier (Regulations 6(1) and 6(2), Trustees (Transparency and Effective Control) Regulations 2017, Regulation 6(4), Trustees (Transparency and Effective Control) Regulations 2017)).

LTCs have obligations to hold basic information on regulated agents of, and services provides to the trust (Regulation 20, Trust Companies Regulations).

TMs of BTs do not have explicit obligations to hold basic information on all types of regulated agents of, and service providers to the trust, as they are not applicable in the specific context. TMs are only required to notify MAS of any changes to any particulars in the register of registered business trusts maintained by MAS, including the particulars of the TM, auditor of the business trust and secretary of the trustee-manager (Regulation 8 and Second Schedule, Business Trust Regulations 2006).

CDP's admission process for depository agents includes collecting the following information: name of depository agent; country of incorporation; registered address in Singapore. Regulation 4 of the Securities and Futures (Central Depository System) Regulations 2015). CDP does not have an obligation to hold basic information on any service providers, as they are not applicable in the specific context.

CIS investment advisers, registrars and auditors must be named in the prospectus of a CIS (Part V, Third Schedule, Securities and Futures (Offers of Investments) (Collective Investment Schemes) Regulations 2005). The manager of the CIS is also required to inform the Authority on an ongoing basis of any significant changes to the CIS, including the replacement, removal or appointment of a manager, sub-manager, investment adviser or trustee to the scheme (paragraph 3.2 (d)(v), Code on Collective Investment Schemes).

A trustee of a charitable purpose trust can only be either a LTC, or a residual trustee, so the statutory requirements applicable to LTC and residual trustees (see above) apply to charitable purpose trusts.

Mutawallis are required to obtain and verify the identity and/or basic information and authority of agents and service providers before they are engaged to the satisfaction of MUIS (Clauses 1(j) and (n), read with Schedule B of the said Terms and Conditions). In other cases where MUIS is the mutawalli, its wholly-owned subsidiary which manages the wakaf is contractually required to process payments to contract service providers and maintain proper and adequate accounts and records (s3, Schedule 1b, Master Agreement, Management Services for Institutional Assets (Mosques, Madrasahs and Wakafs).

Criterion 25.5 –

Trustees of LTCs, CDP, CIS's and charitable purpose trusts are required to maintain the information in criterion 25.4 for at least 5 years after their involvement in the trust or similar legal arrangement ceases (paragraph 10.3, MAS Notice TCA-N03; paragraph 11.3, MAS Notice SFA 03AA-N01; Regulation 7(c), Trustees (Transparency and Effective Control) Regulations 2017). Trustee-managers of registered business trusts are required to ensure that all books and papers of the registered business trust are retained for a

period of at least 5 years after the date on which the business trust is deregistered (paragraph 4.1, MAS Notice BTA1-N01).

MUIS' records management policy, which is produced with reference to the Government-wide manuals requires MUIS to retain relevant information on *wakafs* for at least 5 years and archive the information, meaning the information will not be destroyed. See also clause 1(n), read with Schedule B of the Terms and Conditions of Mutawalli Appointment.

Criterion 25.6 –

Trustees of LTCs, CDP and CIS' are required to ensure the CDD data, documents and information collected on trusts is kept up-to-date by undertaking reviews (paragraph 6.24, MAS Notice TCA-N03; paragraph 6.23, MAS Notice SFA-03AA-N01; paragraph 6.23, MAS Notice SFA-13-N01). Guidance on frequency of reviews is provided in accompanying guidelines.

Residual trustees are required to ensure an accurate record of information obtained and is maintained and updated in a timely manner (Regulation 7, Trustees (Transparency and Effective Control) Regulations 2017).

TMs are required to verify the accuracy of information collected on unit holders, keep it up-to-date or identify a natural person with ultimate effective control (Section 135, 136, 137J, 137K of SFA; Part IV of SF(DOI)R).

A trustee of a charitable purpose trust can only be either a LTC or a residual trustee, so the statutory requirements applicable to LTC and residual trustees (see above) apply to charitable purpose trusts.

For *wakafs*, clause 1(i) of the Terms and Conditions of Mutawalli Appointment states that *mutawallis* have to keep a proper and updated record of all distribution of funds to beneficiaries, including basic and BO information of the beneficiaries. No distributions of funds to beneficiaries may be made until this obligation is complied with. Likewise, for all other *wakafs* where MUIS is the *mutawalli*, MUIS must also update the list of beneficiaries, before disbursements are made.

Criterion 25.7 –

Sub-criterion 25.7(a)

- **LTCs and CIS trustees:** MAS Notices include a set of underlying principles to serve as a guide for LTCs and CIS trustees in the conduct of their operations and business activities (paragraph 3.1, MAS Notice TCA-N03; paragraph 3.1, MAS Notice SFA13-N01). These include the underlying enforceable principle that trust companies shall disclose to FIs and DNFBPs that it is acting as a trustee (paragraphs 3.1(d) and (e), MAS Notice TCA-N03; paragraphs 3.1(d) and (e), MAS Notice SFA13-N01).
- **Trustee-managers of registered business trusts**: MAS Notice BTA1-N01 issued on 9 June 2025 imposes an obligation on TMs to disclose their status as a trustee of the BT to FIs and DNFBPs when establishing contact relating to or during the course of its management and operation of the registered business trust as its trustee-manager (paragraph 3.1).
- **CDP:** CDP is the sole securities depository in Singapore and it is stated under section 81SI of the SFA, as well as on the CDP's website, that the CDP holds book-entry securities deposited with it as a bare trustee for the collective benefit of depositors.
- **Trustees of Residual Trusts:** Trustees of residual trusts are required to take reasonable steps to inform FIs and DNFBPs that they are acting for the relevant trust when forming a business relationship (Regulation 8, Trustees Transparency and Effective Control Regulations 2017).
- **Charitable purpose trusts:** Statutory requirements applicable to LTCs and residual trustees (see above) apply to charitable purpose trusts.

- **Wakafs:** There is no requirement for *mutawallis* to disclose to FIs and DNFBPs that they are acting on behalf of a *wakaf* when entering into a business relationship or conducting a transaction. The extent to which MUIS is required to make such a disclosure is unclear, but Singapore indicate that MUIS' status as a trustee equivalent is discernible to FIs and DNFBPs and that MUIS only opens bank accounts in the name of the *wakaf*.

Sub-criterion 25.7 (b) and (c) – There do not appear to be any laws or enforceable means that prevent trustees of express trusts and the trustee-equivalent for *wakafs* from cooperating or providing information as required by the Standards.

Timely access to adequate, accurate and up-to-date information

Criterion 25.8 –

Singapore's supervision of LTCs acts as a mechanism to ensure the information LTCs collect on BO is accurate. Whilst this does occur during on-site examinations of LTCs, the coverage is low within the reporting period meaning many LTCs are not being checked for compliance with these obligations. entities (see Core Issue 5.4). No mechanism exists for residual trust as the trustees are not supervised.

Criterion 25.9 –

Singapore predominantly uses 25.9(c) to provide competent authorities with access to basic and BO information – this is the only mechanism to provide such information on trusts managed by an LTC and residual trusts and does not provide efficient and timely access by competent authorities to relevant information.

Singapore considered whether 25.9(a) and 25.9(b) would assist their competent authorities and decided against. However, this consideration was conducted on the basis of risk, context and materiality of Singapore context, with significant assumptions made with very limited supporting evidence (see Core Issue 5.4 for more details).

Singapore uses 25.9(a) for BTs, Wakafs (both low risk trusts) and charitable trusts. The Business Trust Registrar is required to maintain a register of registered business trusts (s5, BT Act). Basic information on substantial shareholders of the TM are maintained on the Register (Second Schedule, BT Regulation; Part 7 of SFA; S137K of SFA). With respect to BO information, TMs of listed BTs are required to announce this through the Singapore Exchange (section 137R of the SFA). BO information is publicly available on Singapore Exchange's website.

All *wakafs* must be registered with MUIS, which maintains a register of *wakafs* (s64, AMLA).[82]

All institutions which are established for charitable purposes (including charitable purpose trusts) must apply to be registered with the Commissioner of Charities (COC), unless exempted from registration. The registration must include a copy of the governing instrument (i.e., trust deed), which would contain information on the trust's ownership (including details on the settlor and trustees), as well as the charitable purposes for which the trust is established (s7, Charities Act 1994).

As per c25.9(c), FIs and DNFBPs have obligations to identify and verify beneficial owners of customers that are a trust or other legal arrangement and hold basic and beneficial information relating to that trust or *wakaf*. LEAs have the necessary information-gathering powers to gain access to this information in a timely manner (see criterion 25.10) if they know which FI or DNFBP has the trust as its customer.

[82] Section 64 of the AMLA. The register of *wakafs* maintained by MUIS may be inspected by any person upon payment of S$16 for every inspection (rule 3(1) of the Administration of Muslim Law (Wakaf and Nazar Am) Rules).

Criterion 25.10 –

LEAs and the FIU have all the necessary powers for timely access to information held by trustees (ss 20, 21, 22, 34 and 235, CPC; ss 5(3), 40, CDSA; s11, TSOFA; s 65B(3), Income Tax Act 1947).

Liability and sanctions

Criterion 25.11 –

Sub-criterion 25.11 (a) – MAS is empowered by s 16 of the FSMA to issue directions or make regulations (under s 192 of the Act) to any FI or class of FI as it considers necessary for the prevention of ML or TF. This broad power specifically includes CDD measures and record keeping (s 16(2), FSMA) and compliance is mandatory (s 16(3), FSMA).

FIs are defined under s 2 of the FSMA to mean, *inter alia*, any trustee for a collective investment scheme (CIS), any trustee/manager of a business trust registered under the Business Trust Act 2004, any licensed trust company (LTC), and any other person licensed, approved, authorized, designated, recognized, registered or otherwise regulated under this Act or any other MAS scheduled Act.

A FI that fails to comply with a direction or contravenes a regulation, shall be guilty of an offence and liable upon conviction to a fine not exceeding SGD 1 million (USD 740 000) and, for a continuing offence, a further fine of SGD 100 000 (USD 74 000) per day or part of a day (s 16(4), FSMA).

The FSMA also prescribes a general duty on any person who provides it with information, under or for the purposes of the Act, to use reasonable care to ensure the information is not false or misleading. This general duty does not override specific sanctions but operates as a catch-all. A penalty of a fine not exceeding SGD 50 000 (USD 37 000) or a term of imprisonment not exceeding 2 years, or both, applies to an individual and a fine not exceeding SGD 100 000 (USD 74 000) in any other case (s 176, FSMA).

Wakafs are administered by MUIS under AMLA.

Sub-criterion 25.11 (b) –

- LTCs and PTCs: MAS Notice TCA N03 provides legal liability for failure to comply with requirements on identification of parties to a trust and obtaining information relating to the legal arrangement.
- Trustee-managers of registered business trusts (Section 13, 69, 70 of the BTA; Part 7 of the SFA; Part IV of the SF(DOI)R). Penalties for breaches under the BTA carry a fine on conviction of up to SGD 25 000 (USD 18 500). Penalties for trustee-managers of BTs range from a maximum fine on conviction of SGD 25 000 (USD 18 500) to a maximum fine on conviction of up to SGD 250 000 (USD 194 000) and/or imprisonment for a term not exceeding 2 years.
- The Central Depository (MAS Notice SFA03AA-N01 and Section 16(4) of the FSM Act). Failure to comply with the measures in MAS Notice SFA03AA-N01 is a criminal offence, and pursuant to section 16(4) of the FSM Act the Central Depository shall be liable on conviction to a fine not exceeding SGD 1 million (USD 740 000), though MAS can offer composition (see meaning below) of up to SGD 500 000 (USD370 000).
- Trustees of CIS (MAS Notice SFA13-N01; Section 16(4) of the FSM Act). Failure to comply with the measures in MAS Notice SFA13-N01 is a criminal offence, and pursuant to section 16(4) of the FSM Act the approved trustee shall be liable on conviction to a fine not exceeding SGD 1 million (USD 740 000), though MAS can offer composition (see definition below) of up to SGD 500 000 (USD 370 000).
- Trustees of Residual Trusts (Part 7 of the Trustees Act and the Trustees Regs). In November 2024, Parliament passed the MACMAOMA, which increases the maximum fine to SGD 25 000 (USD 18 500) per contravention, in line with the maximum fine for similar AML/CFT breaches for companies and company officers, trustee-managers of BTs, and accounting firms.

- Wakafs - MUIS' officers are obliged to comply with its policies and guidelines. A failure to do so may result in disciplinary sanctions pursuant to the Public Service (Disciplinary Proceedings) Regulations. MUIS is a government statutory board (i.e., a public agency).

Sub-criterion 25.11 (c) - A person convicted of failing to comply with a production order issued by the police or an authorised person[83] where the order is issued for the investigation or trial of an (domestic) arrestable offence is liable to imprisonment of up to six (6) months, or a fine of up to SGD 5 000 (USD 3 700) (for individuals), or both (s20(7), CPC). For body corporates, LLPs, partnerships or other incorporated associations the penalty is up to SGD 10 000 (USD 7 400) and for all other cases the penalty is a fine of up to SGD 1 500 (USD 1 100) or imprisonment up to one month (s20(7), CPC).

The Penal Code has offences where a person intentionally omits to produce or deliver a document or electronic record to a public servant where the person is legally bound to produce such a document or electronic record (s175). The penalty for this offence for individuals is imprisonment up to one (1) month or a fine of up to SGD 1 500 (USD 1 100), or both, and for non-individuals a fine of up to SGD 10 000 (USD 7 400) (s175, Penal Code). The Penal Code also has offences where a person legally bound to give any notice or provide information to a public servant in the manner and time required by law fails to provide such notice or information (s176). The penalty for this offence for individuals is imprisonment up to one (1) month or a fine of up to SGD 1 500 (USD 1 100), or both, and for non-individuals a fine of up to SGD 10 000 (USD 7 400) (s175, Penal Code). The failure to comply with a production order issued under sections 36 and 37 of the CDSA is an offence punishable upon conviction to a fine up to SGD 10 000 (USD 7 400) or to imprisonment up 2 years or both (s39, CDSA).

International co-operation

Criterion 25.12 –

Sub-criterion 25.12 (a) – Singapore can provide and request a wide range of MLA assistance relating to BO information on trusts and other legal arrangements under MACMA (see R.37).

Sub-criterion 25.12 (b) and (c) – Singapore can facilitate access by foreign competent authorities to BO information held domestic authorities, and exchange domestically available information on trusts and other legal arrangements with foreign competent authorities (see R.40). There is no public body that holds BO information on trusts in a centralised manner.

Sub-criterion 25.12 (d) - Singapore's competent authorities can use their powers, in accordance with domestic law, to obtain BO information on behalf of their foreign counterparts (section 5(3), CDSA). This includes accessing information held by the identified FI or DNFBP.

Sub-criterion 25.12 (e) - AGC is Singapore's Central Authority for mutual legal assistance, including responding to MLA requests for BO information. Information about making an MLA request to Singapore is publicly available on the AGC website.[84] For other international co-operation requests for BO information about trusts, STRO, the various LEAs and competent authorities are the primary points of contact for information by their foreign counterparts.

> ***Weighting and conclusion –*** Singapore is a global centre for wealth management, for which trusts are used as a vehicle to hold and manage wealth. As such, deficiencies relating to efficient and timely access to BO information, and the accuracy of it (particularly where trusts may be used in a network

[83] "Authorised person" is defined under s 20(9) of the CPC to mean any person authorised in writing by the Commissioner of Police for the purposes of the section, as well as any officer of a prescribed law enforcement agency (e.g., IRAS, Singapore Customs, the Gambling Regulatory Authority of Singapore etc.) who is authorised by the head of that law enforcement for the purposes of the section.

[84] www.agc.gov.sg

with other legal persons and legal arrangements) have been most heavily weighted. BTs, wakafs, and CIS trusts have been least heavily weighted.

Singapore has assessed the ML/TF risks for trusts and similar trust arrangements but the assessment team has concerns about the robustness of the LARA.

Obligations are placed on trustees and trustee equivalents to obtain and hold a range of basis and BO information on the trust and wakafs.

Competent authorities use information held by FIs and TCSPs as the primary means to gain access to information for trusts. In the absence of a public authority that holds this information, and the lack of verification requirements in relation to some trusts, the assessment team cannot conclude adequate, accurate and up-to-date information on the basic and BO of the trusts or other similar legal arrangements, trustees and trust assets, is accessible efficiently and in a timely manner by competent authorities. A more robust consideration of the multi-pronged approach is needed for Singapore's risk, context and materiality.

A range of sanctions apply to breaches of obligations to ensure the transparency of BO of trusts and wakafs which appear to be proportionate and dissuasive. Singapore can rapidly, constructively and effectively provide information co-operation in relation to information that is available, including BO information on trusts and other legal arrangements where the relevant FI or DNFBP holding the information is known.

Recommendation 25 is rated **Partially Compliant**.

Recommendation 26 – Regulation and supervision of financial institutions[85]

In the 4th round MER, Singapore was rated Largely Compliant with R.26, based on deficiencies with fit and proper requirements, and supervision for moneylenders was not appropriately risk-based.

Criterion 26.1 –

MAS is the financial sector regulator that regulates and supervises the following FIs for AML/CFT/CPF: banks (including merchant banks), payment service providers, external asset managers, fund management companies, broker-dealers and corporate finance advisory firms, non-bank credit card issuers, approved trustees, finance companies, direct life insurers, insurance brokers, securities depository, financial advisers, approved exchanges and recognised market operators, and digital token service providers. MinLaw is designated with the responsibility of regulating and supervising moneylenders, including for AML/CFT/CPF purposes (see sections 5, 6, 43, 45 and 93 of the Moneylenders Act 2008, and the Moneylenders (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing) Rules 2009 (Moneylenders (PMTFPF) Rules)).

Market Entry

Criterion 26.2 –

MAS licenses or approves all Core Principles FIs in Singapore, which include banks, finance companies, direct life insurers, financial advisers, fund management companies, external asset managers, and approved trustees. Most other categories of FIs are also subject to a licensing regime by MAS. The Central Depository (Pte) Limited (CDP) is subjected to a designation (akin to licensing) regime, and it is specifically designated under section 81SF of the Securities and Futures Act 2001 (SFA). Moneylenders are licensed by MinLaw.

[85] Recommendation 26 is newly assessed as Singapore has made legal, regulatory or operational framework changes since its last mutual evaluation.

MAS' licensing regime and standard operating procedure manuals do not explicitly prohibit any shell bank from being established and from operating in Singapore; however, the MAS BD Administration of Licenses standard operating procedure manual explicitly does. In addition, the licensing procedures used by MAS to consider bank applications de facto prohibit shell banks as they consider capital adequacy, liquidity ratios etc.

Criterion 26.3 –

MAS screens the senior management, the directors, controllers (including beneficial owners) and substantial shareholders of the applying FI to ensure they are "fit and proper", including whether they are criminals or associates of criminals. The percentage thresholds[86] used to determine whether one is a controller and/or substantial shareholder ensures that any person holding a significant or controlling interest in the FI will be screened. Where MAS has concerns arising from the screening process, it has powers to revoke the approval previously granted to the FI/applicant or impose licensing actions (e.g. suspension or revocation of license). After the licence or approval has been granted, FIs are required to seek approval from MAS for changes in key appointment holders (including directors), controllers and substantial shareholders. FIs are also expected to inform MAS when they become aware of any matter that would affect their controllers, shareholders or key appointment holders who do not meet the "fit and proper" criteria. Such individuals will have to dispose of their interest if they are controllers or substantial shareholders or be removed from their management position in FIs. In addition, MAS regularly monitors for significant developments (including through STRs), adverse news, and changes to shareholding structures or takeover bids of FIs in Singapore and follows up with the FIs where necessary.

In relation to moneylenders, MinLaw screens all directors, substantial shareholders, and managers and employees of the applicant against police records, sanctions lists and news media before granting a licence or approval of its management (including directors) or assistant/employee or substantial shareholding. After the licence or approval has been granted, a moneylender is required on an on-going basis to seek approval from MinLaw for changes to its business profile (i.e. changes to its directors, substantial shareholders, managers and employees) who will be screened by MinLaw accordingly.

Risk-based approach to supervision and monitoring

Criterion 26.4 –

MAS regulates and supervises Core Principles FIs in line with the Principles set by the BCBS, IOSCO, and IAIS, including the application of consolidated group supervision for AML/CFT purposes. 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' "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 a "Compliant" rating for 12 of the 15 Principles relevant to AML/CFT and "Largely Compliant" for the remaining three 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 28 Principles, and "Broadly Implemented" for the remaining Principles.

Payment Service Providers carrying out domestic and/or CBMT activities, money changers and other non-core principles FIs (including VCCs) are also regulated and supervised by MAS for AML/CFT. Moneylenders are regulated by MinLaw and are subject to AML/CFT requirements.

[86] For instance, under the licencing conditions imposed on banks incorporated in Singapore, licensees are required to seek MAS' approval for any change of its members or shareholdings of its members which will result in any person, alone or acting together with any connected person, being in a position to control not less than 12% of the voting power in the licensee or to hold interest in not less than 12% of the issued shares of the licensee.

Criterion 26.5 –

MAS and MinLaw adopt a risk-based approach, and their frequency and intensity of on-site and off-site supervision has regard to FIs' ML/TF risk. Each supervisor considers the ML/TF risks present in the country, the policies, internal controls and procedures associated with the institution or group and the characteristics of the FI.

Criterion 26.6 –

MAS conducts an inherent ML/TF risk assessment of each FI (FIRA), and supplements this with an assessment of the robustness of the FIs' controls. For the higher risk sectors (i.e. High Risk and Medium-High Risk sectors in the ML NRA), the frequency of the inherent ML/TF risk assessment ranges from annually to once every 2 years, and for those that fall under the Medium Low and Lower Risk sectors in the ML NRA, inherent risk assessment is performed at least once every 4 years.

MinLaw reviews the risk profiles of the moneylenders it supervises yearly. MinLaw is kept updated of intended changes to a moneylender's business plans and activities, which may affect compliance with the provisions of the Moneylenders Act 2008 and updates their risk profiles on an ongoing basis.

> *Weighting and conclusion –* All criteria are met.
>
> Recommendation 26 is rated **Compliant**.

Recommendation 27 – Powers of supervisors [87]

In the 4th round MER, Singapore was rated Compliant on R.27.

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 examinations (FSM Act section 16; SFA section 150; and Securities and Futures (Central Depository System) Regulations 2015: regulation 29). MAS also uses external inspectors and FIs' internal and external auditors to review their institution's compliance with AML/CFT requirements. MinLaw (Moneylenders Act 2008: sections 43 and 45, and Moneylenders (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing) Rules 2009 (Moneylenders (PMTFPF) Rules), rule 10.

Criterion 27.2 –

MAS and MinLaw have the authority to conduct examinations and supervisory visits of FIs, including moneylenders, to examine their AML/CFT controls and procedures (FSM Act section 16; SFA section 150; Securities and Futures (Central Depository System) Regulations 2015, regulation 29; and Moneylenders Act 2008: sections. 43 and 45, and Moneylenders (PMTFPF) Rules: rule 10).

Criterion 27.3 –

MAS has authority to access all relevant information, and broad powers to require co-operation by the FIs it supervises, including the power to compel production of information (FSM Act section 16; Securities and Futures Act 2001 (SFA) section 150; and Securities and Futures (Central Depository System) Regulations 2015, regulation 29). MinLaw has similar powers under the Moneylenders Act 2008 (sections 43 and 45); and the Moneylenders (PMTFPF) Rules 2009 (rule 10). These powers to compel production of information or to obtain access to information for supervisory purposes do not require a court order.

[87] Recommendation 27 was not under review. Therefore, the text for the Recommendation is copied from MER 2016, with minor non-substantive edits included from Singapore.

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 MinLaw 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 MinLaw relies on its enforcement guidelines for moneylenders which set out the measures MinLaw may take against moneylenders, including imposing administrative and criminal sanctions. See also analysis regarding R.35 below.

> *Weighting and conclusion –* All criteria are met.
>
> Recommendation 27 is rated **Compliant**.

Recommendation 28 – Regulation and supervision of DNFBPs[88]

In the 4th round MER, Singapore was rated Partially Compliant with R.28 as PSMDs without pawnbroker's licenses were not subject to regulation, sanctions that were not appropriately proportionate or dissuasive and supervision was not performed on a risk-sensitive basis.

Casinos

Criterion 28.1 –

Casino operators are required to be licensed by GRA. At the point of application for a casino licence and subsequent renewal of a casino licence, the GRA 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 the casinos' associates (being beneficial owners, substantial shareholders, board of directors and certain senior management personnel), and special employees (persons holding a licensable function), and include consideration if the individual is a criminal or an associate. Casino operators are required to notify the GRA in writing when there are changes to the status of their associates and special employees. When informed of such changes, the GRA performs the necessary checks on the suitability of these associates and/or special employees.

DNFBPs other than casinos

Criterion 28.2 –

- For EA/RES: CEA
- for developers: URA
- for PSMDs and pawnbrokers: MinLaw
- for lawyers/law practice entities: MinLaw and LawSoc
- for accountants: ACRA and ISCA for professional accountants
- for LTCs: MAS
- for CSPs: ACRA

[88] Recommendation 28 is newly assessed as Singapore has made legal, regulatory or operational framework changes since its last mutual evaluation.

Criterion 28.3 –

Competent authorities and SRBs mentioned above in c.28.2 generally have the powers to carry out on-site AML/CFT examinations and off-site monitoring for their categories of DNFBPs. Those sectors with AML/CFT obligations that were covered in the 2016 MER continue to have the identical supervisor that uses the identical supervisory powers. Those are detailed in the 2016 MER's technical compliance annex. Since that time, Singapore has also provided AML/CFT supervisory powers in the following manner:

Accountants: ACRA has put in place a system to monitor public accountants' compliance with the AML/CFT requirements. In Singapore's 3rd FUR 2019, it was observed that while ISCA was the supervisor for monitoring AML/CFT compliance by professional accountants, they did not yet have the necessary powers to undertake AML/CFT examinations of professional accountants – examinations took place on a voluntary basis. Since 2022, ISCA has implemented a compliance monitoring program for professional accountants. These reviews are done pursuant to ISCA's powers under its Constitution (Articles 12A.2 and .5), where it is empowered to request information for the purpose of assessing its members compliance with Ethics Pronouncement 200 (EP 200) as well as powers under its Rules (Rules 64 and 137 of ISCA (Membership and Fees) Rules) to take action and prescribe disciplinary procedures and sanctions for non-observance of EP 200 requirements by its members. Professional accountants were covered under the CSP Act on 9 June 2025.

Developers: URA has implemented a system to monitor the developers' compliance with AML/CFT requirements. Developers selling uncompleted properties are regulated under the Housing Developers (Control and Licensing) Act (HDCLA) and Sale of Commercial Properties Act (SCPA). The Controller of Housing (COH) has the power to require developers to provide information to ascertain if the developers have complied with the AML/CFT requirements (s.12C and s.14 of the HDCLA and s.5B and s.7A of the SCPA).

Criterion 28.4 –

(a-b) Competent authorities generally have the necessary powers to inspect and monitor DNFBPs' compliance as well as 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. Those that were covered in Singapore's previous mutual evaluation are detailed in that mutual evaluation's technical compliance annex. Since that time:

Accountants: For professional accountants, ISCA has the necessary powers to perform its functions (see R.28.3) and to prevent criminals or their associates from being registered as ISCA members; both at the time of registration and when changes occur (Rules 5, 64, 65 and 137 of ISCA (Membership and Fees) Rules). Professional accountants were covered under the CSP Act on 9 June 2025.

Developers: For developers, URA has implemented an AML/CFT regime in June 2023. This includes COH having powers to request for information to assess compliance with the AML/CFT requirements. HDCLA and SCPA prohibit persons from becoming a developer or a substantial shareholder of a developer or holding a responsible position in a developer or in substantial shareholders of a developer if they have been convicted of offences involving fraud, dishonesty, money laundering or terrorism financing offences; however, this does not include a full prohibition on criminals becoming developers (sections 5 and 12F of the HDCLA and sections 5D and 5F of the SCPA).

Proportionate and dissuasive sanctions: See R.35.

All DNFBPs

Criterion 28.5 –

The competent authorities generally conduct risk assessment exercises for DNFBPs to guide their AML/CFT supervisory approaches, and the frequency and intensity of their inspection efforts. Those that were covered in Singapore's previous mutual evaluation are detailed in that mutual evaluation's technical compliance annex. Since that time:

PSMDs: For PSMDs, risk-based supervision commenced in 2020 after the implementation of the 2019 AML/CFT regulatory framework for PSMDs. MinLaw assesses the ML/TF/PF risk of individual PSMDs based on a number of risk assessment criteria.

Accountants: ACRA commenced risk-based supervision in 2020, focusing examinations on higher-risk accountants. In 2023, ACRA updated its risk assessment framework. ACRA represented that its risk-based supervision towards accountants will continue under the CSP Act, which came into effect one month prior to the assessment team's visit.

Developers: COH commenced AML/CFT examinations in 2024 using a risk-based approach, following the implementation of the AML/CFT requirements in June 2023. This include the developers of projects involved in the *3B$ case* which are rated high risk and are prioritised for inspection. Other risk factors taken into consideration in risk profiling are the market segment in which the projects are located (e.g. core central region of Singapore, rest of central region of Singapore), projects with high foreigner purchases etc. URA has commenced the audit on 8 high-risk rated developers in 2024.

Lawyers, notaries, other independent legal professionals: Since 2024, MinLaw has taken over responsibility for supervision of law practice entities (LPEs) from LawSoc. MinLaw has developed a risk assessment framework which it uses to carry out risk-based supervision of LPEs and continues to refine its risk-based supervisory methodology and supervision plans.

> *Weighting and conclusion –* Singapore has covered most of the requirements of Recommendation 28. There are minor deficiencies in the dissuasiveness and proportionality of sanctions for lawyers and law practice entities.
>
> Recommendation 28 is rated **Largely Compliant**.

Recommendation 29 – Financial Intelligence Units (FIU)[89]

In the 4th round MER, Singapore was rated Compliant for R.29

Criterion 29.1 –

Section 5 of the CDSA confirms the establishment and functions of the STRO including its 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 45). These disclosures include STRs, cash transactions reports (CTRs) by casino operators, precious stones and precious metals dealers, and pawnbrokers, and cross border movement of physical

[89] Recommendation 29 is newly assessed as Singapore has made legal, regulatory or operational framework changes since its last mutual evaluation.

CBNI reports (CMRs). STRs, CMRs, and CTRs are filed electronically via the STRO Online Notices and Reporting (SONAR) platform[90].

Criterion 29.3 –

Sub-criterion 29.3(a) - Section 5(3) of the CDSA 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 CRIMES3' 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. Legislative amendments were also made, in 2024, to the Income Tax Act 1947, the Goods and Services Tax Act 1993, the Regulation of Imports and Exports Act 1995, and the Free Trade Zones Act 1966 to allow government agencies to share domestic tax data and trade data respectively with STRO, to augment its analysis on ML and TF activities and provide richer intelligence to LEAs and regulators. STRO can now access data sets from these organisations. STRO is also able to access all disclosures made by FIs to COSMIC, a digital platform which MAS co-developed with six major banks in Singapore to enable them to share information with one another on customers who may exhibit potential financial crime concerns. This access is legislated via Section 28L of the Financial Services and Markets Act 2022[91].

Criterion 29.4 –

STRO's analytical branches focus on receiving and analysing information.

Sub-criterion 29.4(a) - STRO conducts operational analysis. In 2022, STRO upgraded its operational analysis system (WINGS X) in order to further enhance its capabilities to process large volumes of reports received and improve the quality of financial intelligence produced.

Sub-criterion 29.4(b) - STRO conducts crime (such as tax crimes, online scams, business email compromise fraud, and corruption), industry (such as the banking sector, payment service providers, and the precious stones and precious metal dealers), 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 used in the various NRAs – and vice versa - the findings of the NRA and discussions at the AML/CFT SC and the RTIG 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 5(1)(b) of the CDSA. A number of working arrangements facilitate the dissemination towards relevant LEAs and/or regulatory authorities. Guidelines on referral of financial intelligence by STRO to Singapore Customs (Customs), Immigration and Checkpoints Authority (ICA), Central Narcotics Bureau (CNB), SPF, CPIB, Internal Security Department (ISD) and Inland Revenue Authority of Singapore (IRAS) are in place. Internal guidelines are in place to ensure this dissemination is made via dedicated, secured and protected channels. STRO is also able to disseminate the results of its analysis to competent authorities and foreign FIUs spontaneously and upon request (S48, CDSA).

[90] All AML/CFT supervisors (including MAS, GRA, IPTO, ACD) and competent authorities responsible for investigations into ML, TF and associated predicate offences have been given direct screening access to STRO's analytics and data management system, WINGS X. This provides convenient and real-time information to support their operational needs.

Criterion 29.6 –

STRO protects its information as follows:

Sub-criterion 29.6(a) - Section 77(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 1935. 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 SOP in this regard.

Sub-criterion 29.6(c) - Information security is maintained within STRO. STRO's systems, including WINGS X, are designed with information security in mind with an audit trail capturing users' actions. Access to STRO's systems, (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. STRO is located within SPF premises, however physical access to STRO facilities (which are 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) – (d) - STRO can make arrangements for spontaneous, information exchange with domestic competent authorities and foreign counterparts, without prior approval. The Head of STRO is also the Director of SPF-CAD. In line with dedicated SOPs (Delegation of Decision Making in STRO), the Director of CAD delegates strategic and operational decision-making (e.g. dissemination) to a Deputy Director (DD) of STRO who is responsible for strategic and operational decisions. Disseminations are normally under the responsibility of operational staff who sit under the Assistant Directors (AD). Cases can be escalated to the AD or DD. However, the SOPs do not guarantee that full organisational accountability is transferred to the DD STRO (for example, the Head of the FIU is the authorised signatory for STRO's MOUs/LOUs on the exchange of financial intelligence). Also, in practice, the Head of STRO may be consulted for information on important cases in a non-decision-making manner, which leaves some ambiguity to their role/responsibility.

While it is located within the SPF, 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 from CAD, allocated from the overall SPF budget (STRO funding has not been denied to date). STRO receives adequate resources and has full autonomy in deciding on its deployment to carry out its functions. An example of this would be the increase in staff since the last MER.

Criterion 29.8 –

STRO was recognised as a member of the Egmont Group in 2002.

> *Weighting and conclusion –* There is a minor deficiency with the lack of safeguards to preserve STRO's operational independence.
>
> Recommendation 29 is rated **Largely Compliant**.

Recommendation 30 – Responsibilities of law enforcement and investigative authorities[92]

In the 4th round MER, Singapore was rated Compliant for R. 30.

Criterion 30.1 –

Singapore has law enforcement authorities that have responsibility for ensuring that money laundering, predicate offences and terrorist financing offences are properly investigated, within the framework of national AML/CFT policies.

The main LEAs with responsibility for investigating ML/TF under Singapore's main AML legislation (the CDSA) are the SPF, Central Narcotics Bureau (CNB) and the Corrupt Practices Investigation Bureau (CPIB) (S2, CDSA), which are all well-resourced. Within SPF, the CAD (which also hosts STRO) is the lead LEA for investigating ML/TF (see below), while CID (which includes a financial investigation branch, FIB) is responsible for investigating ML arising from serious and organized crime, including unlicensed moneylending, vice, illegal gambling and cybercrime, etc. CNB (which includes financial investigation and intelligence divisions) is responsible for investigating ML arising from drug-related predicate offences and the CPIB is responsible for investigating ML arising from corruption[93] (bribery-related) offences. All CPIB are trained to handle ML investigations and introduced a Financial Investigation Branch in early 2025 to take on complex ML cases.

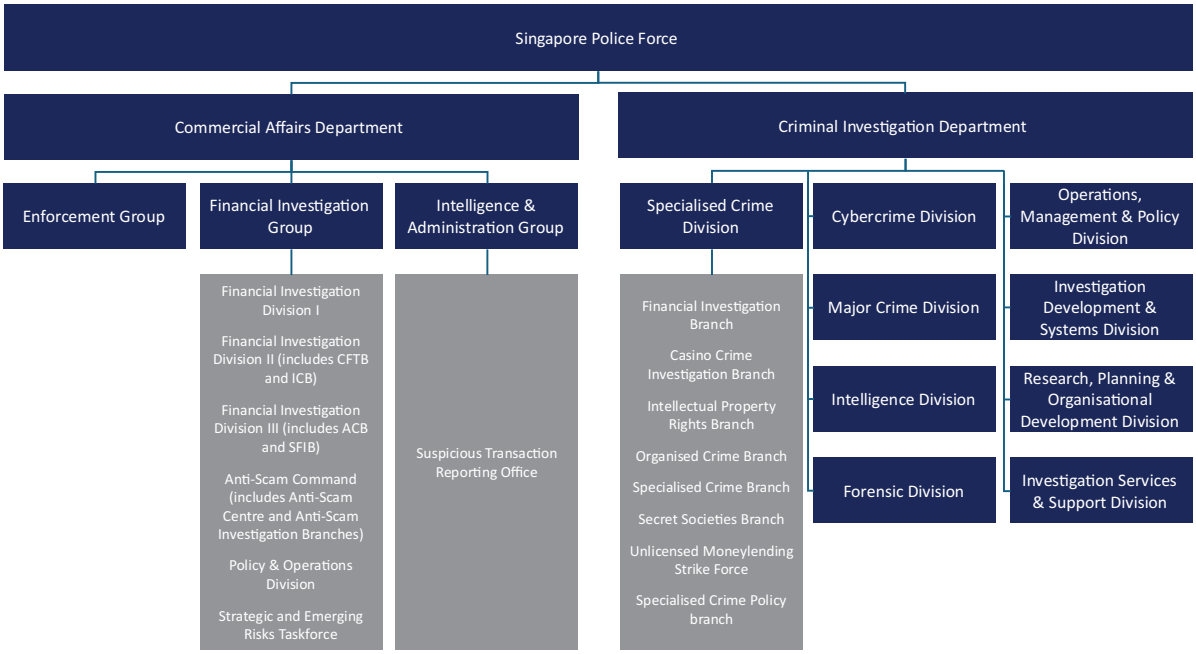
Within CAD, ML/TF investigation is the responsibility of a specific enforcement group, the Financial Investigation Group (FIG). FIG ensures that all ML/TF cases are properly investigated and provided with cross-jurisdictional assistance. Its human resources has doubled since the last MER to 194 staff. FIG comprises the following Divisions: Financial Investigation Divisions I, II, and III, the Anti-Scam Command, Policy & Operations Division, and the Strategic and Emerging Risks Taskforce. These Divisions host specialized Branches, including the CFT Branch (CFTB) and the International Co-operation Branch (ICB) (under FID II)[94], the Asset Confiscation Branch (ACB) and Specialised Fraud Investigation Branch (SFIB) (under FID III) and the Anti-Scam Centre (under the Anti-Scam Command). 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 FIDs 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. The Specialised Fraud Investigation Branch under FID III investigates offences relating to false or non-declarations of cross border movement of cash and bearer negotiable instruments.

[92] Recommendation 30 is newly assessed due to changes to the FATF Standards for which Singapore has not previously been assessed.

[93] ML investigations on embezzlement offences (which in Singapore's context include CBT offences, theft offences and cheating offences under the Penal Code) fall under the purview of SPF.

[94] STRO has its own international co-operation division

Figure A.1. CAD's and CID's Organisational Chart[95]



CFTB (which sits under CAD's FID II) is the lead CFT enforcement agency in Singapore. This includes tracing the assets of suspected terrorists to ensure that these assets are frozen in a timely manner. CFTB works closely with Singapore's Internal Security Department (ISD), which leads on the investigation of terrorism cases.

SPF's CID is tasked with investigating serious and organised crimes. The FIB within CID is responsible for tackling ML arising from offences under CID's purview. FIB also supports other CID units with ML cases.

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.

Other competent authorities (e.g. ICA, IRAS, the Ministry of Manpower, etc.) who have powers to investigate other serious predicate offences outlined in the Second Schedule of the CDSA (including all 21 categories of offences designated by the FATF, see c 3.2), refer ML cases to CAD.

Criterion 30.2 –

Law enforcement investigators of predicate offences are authorised to pursue the investigation of any related ML/TF offences during a parallel financial investigation, regardless of where the predicate offence occurred. SPF, CNB and CPIB are authorised to investigate ML cases arising from predicate offences under their respective purview (S2, S76, CDSA). For non-complex cases, SPF investigators pursue financial investigations in parallel with their predicate offence investigation. Other competent authorities who investigate predicate offences (including when committed abroad) refer ML activities to CAD to commence a parallel financial investigation or for further assessment. Referrals to CAD are guided by a SOP '*for*

[95] This is a simplified chart to show the most relevant SPF's units, divisions, and branches for the purpose of this assessment.

Predicate Agencies to Detect Possible Money Laundering Offences and Refer Money Laundering Cases to the Commercial Affairs Department for Parallel Investigations'.

Criterion 30.3 –

The main LEAs (SPF, CNB, and CPIB) tasked with conducting ML and TF investigations have the authority to expeditiously identify, trace, and initiate freezing and seizing of criminal property and property of corresponding value (S20, S32, S33, S34, S35 CPC; S19, S20, S36, S37, S40, S76, CDSA; S40, S41, S57, S58, S72, S73, OCA))[96]. Within FIG, all relevant branches deal with asset tracing in the context of a financial investigation case. The Anti-Scam Centre (ASC) under the CAD was set up to strengthen SPF's ability to quickly disrupt scammers' operations, mitigate victims' losses and it can swiftly freeze suspicious bank accounts involved in scams and intercept illicit funds. The Asset Confiscation Branch (ACB) focuses on asset tracing and analysis of concealed incomes. Competent authorities investigating predicate offences under the Second Schedule of the CDSA such as SC, IRAS and ICA are similarly equipped with powers to identify and trace assets involved in offences under their respective purviews.

Criterion 30.4 –

Singapore ensures that R 30 applies to competent authorities which are not law enforcement authorities per se. HSA, ICA, MOH, MOM, NEA, Nparks, and Singapore Food Agency are empowered under their respective legislations to conduct investigations into predicate offences under their purview. They are not authorised under the CDSA to conduct a ML investigation or a TF investigation (under TSOFA's provisions). The same SOPs mentioned in c30.3 apply to refer cases to CAD where applicable.

Criterion 30.5 –

CPIB is the relevant agency tasked with investigating ML related to corruption offences (S 17(1), PCA and S 2 CDSA). Investigation of TF offences is under the sole purview of CAD, and specifically CFTB. CPIB has sufficient powers to identify, trace and initiate freezing and seizing of criminal assets and property of corresponding value (S22, PCA, S2 and S76, CDSA) (see also c4.2, 4.4 and 4.5).

> *Weighting and conclusion –* All criteria are met
>
> Recommendation 30 is rated **Compliant.**

Recommendation 31 – Powers of law enforcement and investigative authorities[97]

In the 4th round MER, Singapore was rated Compliant for R.31

Criterion 31.1 –

The main LEAs which investigate ML, associated predicate offences and TF in (SPF, CNB, CPIB) are empowered to exercise a variety of investigative powers, including using compulsory measures for the following:

a) The production of records held by FIs, DNFBPs and other natural or legal persons (S20, CPC; S36-37, CDSA; S40, S41, S72-73, OCA)
b) Searching of persons and premises (S32-34, CPC; S40(1), CDSA; S40, S72 OCA).
c) Taking witness statements (S21, S22(1)-23(1), CPC; S40, OCA).

[96] While the referenced legislative provisions grant the same investigative powers to all ML LEAs, CNB, CPIB and SPF are also empowered with investigative powers by other legislations that can be used to investigate ML, TF and/or associated predicate offences, such as MDA (for CNB), PCA (for CPIB) and TSOFA (for SPF).

[97] Recommendation 31 is newly assessed due to changes to the FATF Standards for which Singapore has not previously been assessed.

d) Seizing and obtaining evidence (S35(1), CPC; S19-20, S76 CDSA; S40, S57-58, S72-73, OCA).

CAD, CNB and CPIB officers can exercise the same CPC investigative powers conferred to police officers from SPF in relation to their respective predicate offences (S64, PFA; S 32, MDA; S17, PCA). Section 2 of the CDSA provides SPF, CNB and CPIB officers with complementary powers of investigation and officers of the SPF have further powers under Section 2 of the TSOFA for TF investigations.

Other LEAs who investigate ML predicate offences within their purview under the Second Schedule of the CDSA (such as Singapore Customs, HSA, ICA, IRAS, MOH, MOM, NEA, NParks and SFA) have extensive information-gathering powers set by different legislations in line with the requirements of this criterion.

Criterion 31.2 –

Competent authorities conducting investigations can use a wide range of investigative techniques for the investigation of money laundering, associated predicate offences and terrorist financing. This includes accessing computer systems and decryption technology (S39 and 40, CPC). Officers are also allowed to let a person perform certain ML acts for the purpose of gathering evidence ((S50(3)(a) and S51(3)(a) of the CDSA). No explicit legislative provision allows the use of undercover operation, but this is recognised in SOPs and case law (*Public Prosecutor (PP) v Tan Tristen [2020] and PP V Muhammad Ali Hashim and Others [2001]*).

Criterion 31.3 –

Singapore ensures that competent authorities (such as SPF, CNB, CPIB) have timely access to a wide range of information, particularly to support the identification and tracing of criminal property and property of corresponding value. This includes basic and BO information, information from asset registries (land, property, vehicles, etc.), citizenship, residency or social benefit registries, trade data, and tax information.

In particular, competent authorities have mechanisms in place to:

a) Identify in a timely manner whether natural or legal persons hold or control accounts. The main LEAs tasked with investigating ML, associated predicate offences and TF, can compel the production of documents or information – including tax and trade-related information – which help in tracing criminal property and property of corresponding value (see c.31.1S6 GSTA; S6, ITA; S31, RIEA, S16A, FTZA). MAS is also able to direct FIs in Singapore to identify whether specific natural or legal persons own or control accounts (S3, S16, FSMA, S26 and 55ZD of the Banking Act 1970).

b) Ensure that competent authorities have a process to identify assets without prior notification to the owner. LEAs can use the powers of S20 (to compel the production of documents or 'things') with discretion and without giving prior notice to the owner.

Criterion 31.4 –

Competent authorities investigating ML, TF and associated predicate offences have direct screening access to STRO's data management and analytics systems (WINGS X) and/or are able to ask for all reports collected and held on this database for their investigations (see R.29). (Guidelines on screenings request received from other agencies).

> *Weighting and conclusion –* All criteria are met.
>
> Recommendation 31 is rated **Compliant**.

Recommendation 32 – Cash couriers[98]

In the 4th round MER, Singapore was rated Compliant for R.31

Criterion 32.1 –

Singapore has a written declaration system (called 'Cross Border Cash Reporting Regime', CBCRR) to detect cross-border movement of cash and bearer negotiable instruments (CBNIs) (S 59, CDSA). A CBCRR declaration form[99] for all physical movement into or out of Singapore of CBNIs exceeding the SGD 20 000 threshold (USD 14 800) or its equivalent in a foreign currency is required (S60 and 62, CDSA). This includes movement by travellers or through mail and cargo (S59(3) CDSA). Since May 2024, travellers submit CBCRR declaration forms digitally via the ICA website/MyICA mobile application, rather than through physical forms. All these declarations are compiled on SONAR. Additionally, cash movement reports for senders, carriers or recipients who move CBNI into and out of Singapore without physically entering or leaving Singapore may also filed digitally on SONAR.

Criterion 32.2 –

Criterion 32.3 –

Singapore has a declaration system in place.

Criterion 32.4 –

Upon discovery of a false declaration of currency or BNIs or a failure to declare or disclose them, CAD (with the support of ICA) have the authority to request and obtain further information from the carrier with regard to the origin of the currency or BNIs, and their intended use, drawing on CPC or CDSA powers. (see c 31.1).

Criterion 32.5 –

Persons who make a false declaration or disclosure are subject to proportionate sanctions. Singapore's penalty framework has evolved through amendments in 2018 and 2020, enhancing enforcement against CBCRR violations. False declaration or non-disclosures can lead to up to three years imprisonment and/or a fine of up to SGD 50 000 (USD 37 000) (S 60(2), 62(2), CDSA). Upon conviction, authorities can confiscate undeclared cash in respect of the breach above the SGD 20 000 threshold or USD 14 800 (S 64, CDSA). In addition, in cases of false or non-declaration of cash that are established to be linked to ML, TF or predicate offences, authorities can confiscate the full amount of detected cash (both declared and undeclared) and impose imprisonment terms on the offenders upon conviction. Authorities can also compound lesser breaches with no suspicion of ML, TF or predicate offences, meaning offenders can settle via monetary penalties up to SGD 20 000 (USD 14 800) (S 81, CDSA). Singapore also has a CBCRR composition framework (i.e. financial penalty in lieu of prosecution), expanding financial penalties for false and non-declarations by first-time CBCRR offenders who are not traced to ML, TF or predicate offences and with detected cash below SGD 100 000 (USD 74 000), beyond court convictions.

Criterion 32.6 –

Information obtained through the digital declaration system is automatically made available for competent authorities through SONAR (see c 32.1).

[98] Recommendation 32 is newly assessed as Singapore has made legal, regulatory or operational framework changes since its last mutual evaluation.

[99] These are also called Cash Movement Reports (CMRs)

Criterion 32.7 –

Singapore ensures there is adequate co-ordination among customs, immigration and other related authorities on issues related to the implementation of R 32. The IAC considers issues relating to the CBCRR and reports to the AML/CFT SC. IAC meets regularly to share information and co-ordinate policy decisions and implementation issues. SPF, ICA, Customs and STRO also hold meetings when necessary. The CBCRR SOP and *Guidelines on investigation into offences involving Cross Border Movements of CBNIs* are in place to detect CBCRR cases and to facilitate the referral of cases detected by STRO, ICA or Customs to CAD for further investigation. SPF, ICA, and other agencies also conduct interagency operations at checkpoints to detect cross-border movements of cash and other cross-border illegal activities.

Criterion 32.8 –

Competent authorities (such as ICA) are able to stop or restrain currency or BNIs for a reasonable time in order to ascertain whether evidence of ML/TF may be found in both situations set-out in this criterion, as directed by the Guidelines on investigation into offences involving Cross Border Movements of CBNIs. Upon detection of a false or non-declaration of CBNIs, ICA will proceed with the preliminary checks (such as ascertaining the type and amount of CBNI and establish source of CBNI) in accordance with the procedure set out in the CBCRR's SOP. The counting of actual CBNI amount is conducted in the presence of the traveller pursuant to s63(4) or S63(9) of the CDSA and the case will be referred to SPF/CAD for investigation. The investigation into CBCRR cases includes enquiries into the source and intended use of the cash, screening against other databases and examination of supporting documents. If there is a suspicion of ML, TF or associated predicate offences, SPF officers will use the generic seizure powers in Section 35 of the CPC to seize the CBNIs for further investigation (see R.4). The maximum duration of seizures under Section 35 of the CPC is one year or when investigations are completed, whichever is earlier (see c4.3b). While this process is subject to judicial review, the outer limit of a year seems inconsistent with the requirements of this criterion to detail currency/BNI for a reasonable time.

Criterion 32.9 –

Singapore ensures that the declaration system allows for international co-operation and assistance, in accordance with Recommendations 36 to 40. Information is retained in the following cases:

a) A declaration exceeds the prescribed threshold, since information contained in STRO's databases can be shared with foreign counterparts (S48, CDSA).
b) c) Cases of false and/or non-declaration investigated by CAD stored in SPF's case-wide management system, which also includes records linked to ML/TF/predicate offences/illicit activities.

Criterion 32.10 –

Singapore ensures that safeguards exist to ensure proper use of information collected through the declaration system, without restricting trade payments between countries for good and services, or the freedom of capital movement. 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 –

a) Persons who carry out a physical cross-border transportation of currency/BNI that are related to ML/TF or predicate offence are subject to sanctions applicable to ML/TF offences.
b) Measures consistent with Recommendation 4. For CBNIs that are seized, confiscation will be determined by the judicial authority under Section 364 CPC or Section 64 CDSA (where there are criminal proceedings) or Section 370 CPC (where there are no criminal proceedings).

Weighting and conclusion – Most requirements are met, and Singapore has a well-developed cash declaration regime. However, where there is a breach of CBCRR, LEAs are able to retain the CBNI until the investigation is completed, or for up to one year. While there is judicial oversight, this length of time – particularly the outer limit of one year – appears inconsistent with the requirement to stop or restrain cash/BNI for a reasonable time only.

Recommendation 32 is rated **Largely Compliant**.

Recommendation 33 – Statistics [100]

In the 4th round MER, Singapore was rated Largely Compliant with R.33. Singapore was assessed to have collected comprehensive statistics in areas such as ML/TF investigations, prosecutions and convictions, and MLA/other international co-operation. However, gaps in relation to total amounts of seizure/confiscations, and the number of cases in which seizure and confiscation occurred were identified.

Criterion 33.1 –

Singapore maintains comprehensive statistics on matters relevant to effectiveness and efficiency of their AML/CFT systems, including the statistics required by R.33.

Weighting and conclusion – All criteria are met.

Recommendation 33 is rated **Compliant**.

Recommendation 34 – Guidance and feedback [101]

In the 4th round MER, Singapore was rated Largely Compliant with R.34 as there were gaps in the provision of supervisory guidance and feedback.

Criterion 34.1 –

Singapore's competent authorities and supervisors has provided guidance and feedback to assist obliged entities in implementing national AML/CFT measures, in particular in detecting and reporting suspicious transactions.

Weighting and conclusion – All criteria are met.

Recommendation 34 is rated **Compliant**.

Recommendation 35 – Sanctions [102]

In the 4th round MER, Singapore was rated Partially Compliant with R.35 as sanctions allowed for legal persons for breach of TFS obligations, those allowed for DNFBPs and those allowed for NPO administrative penalties were insufficiently dissuasive.

[100] Recommendation 33 is newly assessed as Singapore has made legal, regulatory or operational framework changes since its last mutual evaluation.

[101] Recommendation 34 is newly assessed as Singapore has made legal, regulatory or operational framework changes since its last mutual evaluation.

[102] Recommendation 35 is newly assessed as Singapore has made legal, regulatory or operational framework changes since its last mutual evaluation.

Criterion 35.1 –

Sanctions for Recommendation 6: Sections 3 to 6 of the TSOFA sets out that anyone who contravenes their requirements are liable on conviction: (1) in the case of an individual, to a fine not exceeding SGD 500 000 (USD 370 000) or to imprisonment for a term not exceeding 10 years or to both; or (2) in any other case, to a fine not exceeding the higher of SGD 1 million (USD 740 000), or twice the value of the property (including funds derived or generated from the property), financial services or other related services, or financial transaction (as the case may be) in respect of which the offence was committed.

Sanctions for Recommendation 8: The Commissioner of Charities has powers to sanction violations of regulatory requirements, as set out in sections 7, 22, 23, 24, 26, 27 and 29 of the Charities Act 1994. These provisions offer a very wide range of administrative sanctions. Any person that contravenes the regulations shall be guilty of an offence and shall be liable on conviction to a fine not exceeding SGD 10 000 (USD 7 400) or to imprisonment for a term not exceeding three years or to both, and, in the case of a continuing offence to a further fine not exceeding SGD 100 (USD 74) for every day or part of a day during which the offence continues after conviction.

Sanctions for failure to comply with preventive measures in Recommendations 9 to 19 – FIs: AML/CFT requirements for FIs regulated by the MAS are set out in section 16 of the FSM Act and also in the MAS Notices and Directives issued under section 16 of the FSM Act. An FI that fails to comply with requirements set out under section 16 of the FSM 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 (USD 740 000) per offence and, in the case of a continuing offence, to a further fine of SGD 100 000 (USD 74 000) for every day or part of a 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, restrict business activities, suspend or withdraw a license, or issue a fine. These sanctioning powers can be found in the FSM Act and in the various FIs specific governing legislation. MAS' supervisory penalties and sanctions are guided by MAS' 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 Moneylenders (PMTFPF) Rules. A moneylender who is guilty of an offence under the Moneylenders (PMTFPF) Rules is liable to a fine not exceeding SGD 100 000 (USD 74 000) (Moneylenders (PMTFPF) Rules 2009: Rule 11). According to section 10 of the Moneylenders Act 2008, a moneylender is also liable to lose their licence. The fine of SGD 100 000 (USD 74 000) provides, 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, for a sufficiently broad range of proportionate and dissuasive sanctions for breaches of AML/CFT obligations. The range of sanctions include: the refusal to renew a moneylender's licence; the revocation or suspension of the licence; imposition of licence conditions; cancellation of approval granted to the management, director, or substantial shareholder of the moneylender; and issuance of written directions to the moneylender (Moneylenders Act 2008: sections 8, 10, 5 – 6, 14, 17, 45).

Sanctions for failure to comply with preventive measures in Recommendations 22-23 – DNFBPs: Since Singapore's last MER, Singapore has reviewed and enhanced the penalty frameworks for DNFBP sectors to bring penalty levels to a baseline of SGD 100 000 per breach (USD 74 000) in most instances. The exceptions to this baseline are:

For casinos, the sanction for AML/CFT breaches is a sum not exceeding 10% of the casino operator's gross gaming revenue (for serious breaches) or $S1 million (for any other ground of disciplinary action) per breach as set out in section 54 of the Casino Control Act 2006 (CCA).

For lawyers and law practice entities, the maximum financial penalty that can be ordered by the relevant regulator applied is SGD 100 000 per case (USD 74 000) under the (Legal Profession Act 1966 (LPA):

sections: 133, 145, 161, 174 and 175 for law practice entities; sections: 82B, 83, and 83A for lawyers). This SGD 100 000 (USD 74 000) maximum penalty for lawyers and law practice entities remains insufficient and is not proportionate and dissuasive.

For estate agents, the Estate Agents Act has been amended to increase the maximum financial penalty that a Disciplinary Committee (DC) can impose on an Estate Agents (EA)/Real Estate Sales Persons (RES) for AML/CFT breaches to SGD 200 000 per breach (USD 148 000) for EAs and SGD 100 000 (USD 74 000) per breach for RES. Developers also are subject to fines of up to SGD 100 000 (USD 74 000) per breach.

DNFBP supervisors 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 45 of the CDSA is applicable to all natural and legal persons in Singapore. Anyone who contravenes the provisions is liable upon conviction, if the person is an individual, to a fine not exceeding SGD 250 000 (USD 185 000) or to imprisonment not exceeding three years or to both, or if the person is not an individual, to a fine not exceeding SGD 500 000 (USD 370 000). This penalty is attached to each instance of a failure to report.

In addition, a FI or casino 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 16 of the FSM Act (i.e. breaching the relevant MAS AML/CFT Notice) and is liable to a fine of SGD 1 million (USD 740 000) per offence/breach or Regulation 19 of Casino Control (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing) Regulations 2009.

In relation to Recommendation 21: The offence of tipping-off in section 57 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 250 000 (USD 185 000) 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 16 of the FSM Act in terms of breaching the relevant MAS AML/CFT Notice would be liable to a fine of SGD 1 million (USD 740 000) per offence/breach.

Criterion 35.2 –

Sections 174 and 175 of the FSM Act imposes penalties and sanctions set out in section 16 of the FSM Act against an officer, employee or agent of an FI or LTC. As set out in sections 174(6) and 175(6) of the FSM Act, an officer would include any director, partner, chief executive, manager secretary, and a person holding a position analogous to that of President. Specifically, where a FI or LTC commits an AML/CFT offence, the officer or individual who (i) consented or connived or conspired with others to effect the commission of the offence by the FI or LTC; (ii) is knowingly concerned in or is party to the commission of the offence by the FI or LTC; or (iii) failed to take all reasonable steps to prevent or stop the commission of the offence, is guilty of the same offence as the FI or LTC and is liable on conviction to be punished accordingly. This is broad enough to encompass all of senior management functions.

Similarly, under section 89 of the Moneylenders Act 2008, sanctions under the Act are applicable not only to the moneylender but also to individuals involved in the management of the moneylender, including directors and senior management where an offence has been committed with their consent or connivance, or is attributable to any neglect on their part. 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 EAs and RESs comprise of professionals who are subject to the sanctions directly. Additionally, the self-regulatory bodies, including the Law Society and the ISCA, are able to impose disciplinary sanctions on their members. 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. Under sections 32(2) and 33(2) of the PSPM Act 2019, sanctions under the Act are applicable not only to PSMDs but also to individuals involved in the management of the PSMD, including any director, partner, chief executive, manager, secretary, or other similar officer. The same is true for pawnbrokers under section 80 of the PBA 2015 and developers under section 27 of the HDCLA and section 9 of the Sale of Commercial Properties Act 1979. Regarding CSPs, the Corporate Service Providers Act 2024 was passed in July 2024 and introduced an offence provision of a fine of up to SGD 100 000 (USD 74 000) per breach for CSPs and senior management of a CSP for contraventions of AML/CFT/CPF requirements. The senior management of a registered CSP who is involved in the offence (e.g. knew or ought reasonably to have known the offence would be committed and failed to take reasonable steps to prevent or stop the commission of the offence) is also guilty of an offence and liable on conviction to a fine not exceeding SGD 100 000 (USD 74 000) for each breach.

> *Weighting and conclusion –* Most requirements are met. There remains a minor deficiency in that the maximum penalty for lawyers and law practice entities remains insufficient and is not proportionate and dissuasive.
>
> Recommendation 35 is rated **Largely Compliant**.

Recommendation 36 – International instruments[103] [104]

In the 4th round MER, Singapore was rated Compliant with R.36

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 –

Singapore fully implements the Vienna Convention, the Palermo Convention, the Merida Convention and the Terrorist Financing Convention.

> *Weighting and conclusion –* All criteria are met.
>
> Recommendation 36 is rated **Compliant**.

Recommendation 37 – Mutual legal assistance[105]

In the 4th round MER, Singapore was rated Largely Compliant with R.37. The main deficiencies related to the inability to use domestic powers to take witness statements from the suspect or accused in response to an MLA, and the lack of domestic powers to use interception of communication.

[103] The UNCAC Implementation Review Mechanism (IRM), for which the UNODC serves as secretariat, is responsible for assessing the implementation of the UNCAC. The FATF assesses compliance with FATF Recommendation 36 which, in relation to the UNCAC, has a narrower scope and focus. In some cases, the findings may differ due to differences in the FATF and the IRM's respective methodologies, objectives and scope of the standards.

[104] Recommendation 36 was not under review. Therefore, the text for the Recommendation is copied from MER 2016, with minor non-substantive edits included from Singapore.

[105] Recommendation 37 is newly assessed as Singapore has made legal, regulatory or operational framework changes since its last mutual evaluation.

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 Mutual Assistance in Criminal Matters Act 2000 (MACMA), MLA treaties and membership to the ASEAN treaty on MLA. MLA can be provided on the basis of reciprocity even in the absence of an MLA treaty (S 16(2) of MACMA).

Criterion 37.2 –

The Attorney-General's Chambers (AGC) - and more specifically its International Legal Co-operation Team (ILCT) - constitutes the Central Authority (CA) 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 of SOPs and checklists to support the processing of MLA requests, which includes prioritization of requests. There is a central repository and management system – Intelligent Workspace (IW) - 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 –

MLA is not prohibited or made subject to unduly restrictive conditions. The MACMA outlines twelve mandatory grounds (Section 20) for refusal (e.g. the requests is of a political character and based on a person's race, religion, nationality, and four discretionary grounds to refuse assistance requests).

For assistance requiring the use of coercive powers, Singapore will refuse assistance if the foreign offence in question does not correspond to one or more of the listed offences in the MACMA Schedules (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) - Tax offences are considered "serious" offences under the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits Act) 1992 (Part 12 of the Second Schedule). 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.

Criterion 37.5 –

As a general rule, public officers in Singapore are bound by confidentiality as is required by the Official Secrets Act 1935 and the Government's internal guidelines governing the confidentiality of information received by public officers in the course of work. This requirement 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]* 1 SLR(R) 283).

Criterion 37.6 –

Dual criminality is not required for non-coercive forms of assistance. Dual criminality is a mandatory provision that applies to coercive measures requested under Divisions 2, 5 and 6 (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).

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 –

Powers and investigative techniques required under R.31 and available to domestic competent authorities are available in the context of MLA requests. The powers listed under the MACMA are exercised independently of a domestic investigation and include:

Sub-criterion 37.8 (a) - The production, search and seizure of "*any particular thing or description of thing*" – such as information, documents or evidence (including financial records) from FIs or other natural or legal persons (S 22 and 33-36 of the MACMA), and taking witness statements (S21A, MACMA).

Sub-criterion 37.8 (b) - Pursuant to the requirements of Article 11 of the Vienna 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 cannot be provided to foreign jurisdictions.

> *Weighting and conclusion –* All criteria are met.
>
> Recommendation 37 is rated **Compliant**.

Recommendation 38 – Mutual legal assistance: freezing and confiscation[106]

In the 4th round, Singapore was rated LC for R.38, with the main deficiency pertaining deficiencies of instrumentality order, and delays in the restraint of assets.

Criterion 38.1 –

Singapore has measures, including legislative measures, to take expeditious action in the widest possible range of circumstances in response to requests for co-operation by foreign countries seeking assistance to identify, trace, evaluate, investigate, freeze, seize and confiscate criminal property and property of corresponding value, either through CPC or MACMA (which apply concurrently).

When receiving an MLA, LEAs can rely on domestic provisions to provide assistance, particularly S35, CPC granting authorities wide powers to identify, investigate, freeze, seize and confiscate assets (see R.4). Through the powers provided in MACMA, at a requesting country's behalf, Singapore authorities can also seek production orders from the Singapore courts for "any particular thing or description of thing" for the purposes of any criminal matter in the requesting country (S22(1,3,4), MACMA). This legislative provision allows Singaporean authorities to assist with identifying, tracing, evaluating and investigating, any property

[106] Recommendation 38 is newly assessed due to changes to the FATF Standards for which Singapore has not previously been assessed.

which was used or was intended to be used in connection with the commission of any offence against the law of that country (S2, MACMA).

Moreover, authorities are empowered to assist in the restraining of the dealing of any property reasonably believed to be located in Singapore which may satisfy a foreign confiscation order (which covers the recovery, forfeiture or confiscation of any payment or property), and the enforcement and satisfaction of foreign confiscation orders against such property (S2, 29, 30 and Third Schedule, MACMA).

Property that may be frozen, seized or confiscated under these provisions includes any property in respect of which the foreign confiscation orders were or may be made, and therefore includes both criminal property and property of corresponding value (paragraphs 1(1), 7, 8, 10, 17 and 18 of the Third Schedule, MACMA).

SOPs do not set specific timelines but in practice, Singapore provided case studies showing that property can be restrained in as little as one month from the receipt of all necessary information in the foreign country's request for MLA in cases that do not involve an investigation into domestic offences under Singapore law.

Criterion 38.2 –

Measures in c 38.1 (either pursuant to CPC or MACMA) allow Singapore to recognize and enforce orders made on the basis of conviction and non-conviction-based confiscation proceedings, as set out in R 4. Under MACMA, a foreign country should request the AGC to assist in the enforcement and satisfaction of a confiscation order (which applies to recovery, forfeiture or confiscation), who must in turn apply to the General Division of the High Court for its registration (S 29-30, MACMA). Singapore can then give effect to foreign confiscation orders which are made in "any judicial proceedings", such as conviction and non-conviction based judgments (S29(1a), MACMA), where the foreign confiscation order is in force and "not subject to further appeal in the foreign country" (S30(2a), MACMA). During this time, the CA can also apply for restraint orders under MACMA or S35 CPC (see R.4) in response to foreign requests for the duration that the foreign confiscation order may be subject to appeal and is not fully enforced, which limits the risk of dissipation. Moreover, under S364, CPC, Singapore may dispose of property subject to foreign confiscation orders, but only after such orders are final and the time to appeal has expired. The fact that Singapore cannot directly enforce freezing and seizing orders (but uses domestic powers to do so) is a minor deficiency, which is ultimately given no weight as Singapore achieves the outcome set out in this criterion.

Criterion 38.3 –

In recognising and enforcing foreign freezing, seizing and confiscation orders, Singapore is able to rely on the findings of facts in the foreign order and enforcement is not conditional on conducting a domestic investigation. This approach was confirmed in the jurisprudence of *Steep Rise Ltd v AG* [2020] 1 SLR 872, at [26]-[27]. For Singapore to execute a foreign request, the latter needs to satisfy the relevant requirements of MACMA, such as including basic information on the purpose of request and nature of the assistance sought, summary of facts, etc. (S19(2), MACMA).

Criterion 38.4 –

Singaporean courts have the authority to issue freezing, seizing and confiscation orders for any property, whether located in Singapore or abroad (S4(5), S6, 7,19, 20 CDSA). The Attorney General may also request a foreign country to enforce a confiscation order issued by Singapore or to restrain dealing in any property located in the foreign country which may satisfy a confiscation order made in Singapore (S13, MACMA).

Criterion 38.5 –

Singapore has mechanisms to manage, preserve and, when necessary, dispose of frozen, seized or confiscated property at all stages of the cross-border asset recovery process, since the same powers and mechanisms outlined in R.4 apply to cross-border cases that satisfy a foreign confiscation order (Paragraphs 7 to 11, Third Schedule, MACMA).

Criterion 38.6 –

Singapore has:

a) measures to enable informal communication with other countries in asset recovery cases, including facilitating assistance before a request is made and updating countries, as appropriate, on the status of their requests. As shown through several case studies, the AGC regularly engages in informal communication with countries requesting MLA in asset recovery cases, either prior to a request or once it is received (see also R.37).

b) the authority to provide further related assistance on an initial request, without requiring a supplemental request. There are no guidelines or SOPs covering this, and further assistance is provided on a case-by-case basis. In practice, this may involve providing updates on any ongoing parallel domestic investigations in Singapore, or the sharing of documents such as public company annual reports, corporate information and land titles documents, amongst others. Singapore recognises that because of the fluid nature of investigations, the scope of the requested assistance can change. The CA may in these situations suggest refinements to the requesting state without the need for a supplementary request. This includes obtaining a production order to compel an entity to provide information on the flow of funds/property.

Criterion 38.7 –

Singapore is able to:

a) share confiscated property with other countries, either at its own motion, or at the request of another country, and in particular when confiscation is directly or indirectly a result of co-ordinated law enforcement actions. In the enforcement of a foreign confiscation order, following the realization of property, the Singapore High Court may direct any payments to be made out of the sums held by the Public Trustee or a court-appointed receiver (Paragraph 11(1), Third Schedule, MACMA). The Attorney-General is also empowered to apply for a court order to allocate specific sums from the realised assets to foreign countries. Singapore has developed a three-tiered asset sharing framework (similar to the USA) on sharing of confiscated assets with foreign countries, which serves as a guide and has been applied in specific circumstances where the victim(s) is/are unknown. This takes into account the level of contribution (i.e. the level of assistance rendered, and the resources expended) of both Singapore and the foreign country to the asset recovery process, as well as negotiated divisions on a case-by-case basis.

b) make arrangements, where appropriate, to deduct or share substantial or extraordinary costs incurred when enforcing a freezing, seizing, or confiscation order. This is usually negotiated on a case-by-case basis following the level of assistance or resources expended by Singapore and other countries in a particular case. This is handled by the relevant LEA in charge of a case. Singapore provided case studies documenting this practice.

Criterion 38.8 –

Singapore is party to a wide variety of treaties, arrangements, or other mechanisms to enhance co-operation in asset recovery, such as the Vienna Convention, the Palermo Convention, the Merida Convention, and the Terrorist Financing Convention (see R.36). Singapore has also signed bilateral (e.g. USA, India, etc.) and multilateral MLA treaties (such as ASEAN Treaty on MLA in Criminal Matters), which

cover asset recovery and is a member of Asset Recovery Interagency Network – Asia Pacific (ARIN-AP) and the South-East Asia Justice Network (SEAJust).

> *Weighting and conclusion –* All criterion are met.
>
> Recommendation 38 is rated **Compliant**.

Recommendation 39 – Extradition[107]

In the 4th round, Singapore was rated LC for R.39, with the main deficiency pertaining to the need to improve the legal basis for extradition in ML cases and the number of countries covered to include countries that are a greater risk for ML.

Criterion 39.1 –

Singapore is able to execute extradition requests in relation to ML/TF without undue delay. Sections 16-19 and 21-22 of the EA outline clear timelines for the processing of extradition requests to ensure a handling without undue delay of all proceedings, including ML, TF, and predicate offences. In particular:

Sub-criterion 39.1(a) - ML and TF are both extraditable offences in Singapore. Singapore adopts a threshold approach for determining whether an offence is extraditable. Under Section 2(1) of the EA, an offence (wherever committed) is extraditable as long as it has a maximum punishment of imprisonment for not less than two years or more severe punishment and is not on the list of excluded offences. These are listed in the First Schedule of the EA and are mainly regulatory in nature.

Sub-criterion 39.1(b) - The AGC uses the same platform for MLA (IW) to track, assign and file requests, as well as to monitor requests and notify / remind case officers of any deadlines that are set (see R.38).

Sub-criterion 39.1(c) - There are no unreasonable or unduly restrictive conditions on extradition. The EA provides a number of commonly accepted "extradition restrictions" (e.g. the restrictions related to offences of a political character (sections 8(1) and 9(1)) and prejudice on account of race, religion, nationality or political opinions, etc. (section10(1)).

Criterion 39.2 –

Singapore can extradite its own nationals as the EA 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*)[108].

Criterion 39.3 –

Dual criminality is a requirement for extradition. Singapore uses a conduct-based approach (Section 2(1) of the EA), by considering the underlying conduct as a whole. Therefore, technical differences in the manner in which another country categorises or denominates the offence does not pose an impediment to the provision of extradition.

Criterion 39.4 –

Singapore has simplified extradition mechanisms in place. (Section12(1)(a)(ii),EA). Singapore also provides a number of simplified processes for extradition with Malaysia and Brunei Darussalam (S 121 CPC).

> *Weighting and conclusion –* All criteria are met.
>
> Recommendation 39 is rated **Compliant**.

[107] Recommendation 39 is newly assessed as Singapore has made legal, regulatory or operational framework changes since its last mutual evaluation.

[108] Singapore has agreed to provide for nationality as a ground for refusal in its extradition treaties with Hong Kong SAR, Indonesia, and Germany.

Recommendation 40 – Other forms of international co-operation[109]

In the 4th Round MER, Singapore was rated LC against R.40, with the main deficiencies concerning the restrictions for STRO to share information due to the low number of MOUs/LOUs, inability to access and share trade information and some tax information, and the fact customs have some restrictions on the exchange of information.

General principles

Criterion 40.1 –

Singapore ensures that their competent authorities can rapidly provide the widest range of international co-operation in relation to money laundering, predicate offences and terrorist financing, both spontaneously, and upon request. Competent authorities have internal guidelines and SOPs that provide for the timeliness of response, setting out how to prioritize requests. Without prejudice to the latter, the shortcomings identified in R.5 may impact the scope of international co-operation that can be provided, although this is a minor deficiency.

Criterion 40.2 –

Sub-criterion 40.2(a) - Competent authorities in Singapore have a lawful basis for providing co-operation. Authorities co-operate with foreign counterparts based on international treaties and agreements, as well as MoUs/LoUs as appropriate and their own legislative provisions. This is contained in respective legislative Acts, common law principles (which highlight the importance of judicial precedents in the absence of a formal legal provision) and SOPs which allow for confidential exchange of information.

Sub-criterion 40.2(b) - Nothing prevents competent authorities from using the most efficient means to co-operate. While they can co-operate directly with their counterparts without the need for formal arrangements (e.g. MOUs), some competent authorities (e.g. MAS) have signed MOUs outlining terms for efficient co-operation.

Sub-criterion 40.2(c)-(e) - Competent authorities use clear and secure gateways and mechanisms for the transmission and execution of requests, their prioritisation and timely execution and for safeguarding information. Competent authorities all have their own set of international guidelines and SOPs enshrining this. With respect to confidentiality, as public servants, all officers within competent authorities are prohibited by law from sharing any information that is obtained in a manner which is contradictory to lawful directions issued with regard the information or which is without reasonable care to the safety of the information (S5, OSA, S 3 of the Statutory Bodies and Government Companies (Protection of Secrecy) Act, S 77, CDSA). Singapore Government Instructions for Security of Classified Information also set out general procedures and requirements on ensuring the confidentiality of information and apply to all government agencies in Singapore.

Criterion 40.3 –

Competent authorities in Singapore do not require formal arrangements (e.g. bilateral or multilateral agreements) to co-operate, as they are empowered by their SOPs to establish agreements such as MOUs. LEAs, STRO and MAS (as long as the conditions and requirements under S20-25 of the FSM Act are fulfilled, mainly relating to confidentiality of information) can all co-operate with their respective foreign counterparts without a need for MOUs. They can enter such agreements if required by the counterpart. IRAS requires formal arrangements to co-operate on exchange of information (EOI) for tax purposes and negotiates these agreements in a timely fashion. Although this requires the approval of MOF, no

[109] Recommendation 40 is newly assessed due to changes to the FATF Standards for which Singapore has not previously been assessed.

impediments were observed that limit the speed with which these agreements can be signed. See also c40.5.

Criterion 40.4 –

Upon request, competent authorities provide feedback to counterparts from which they received assistance and do so in a timely manner. Singapore indicates that, as outlined in SOPs, government agencies respond within seven working days to queries. STRO's Guidelines on Outgoing requests for assistance requires for feedback to be provided within two weeks, which is considered timely.

Criterion 40.5 –

Singapore does not prohibit and generally does not place unreasonable or unduly restrictive conditions on the provision of exchange of information or assistance, as long as a request is within the scope of purview of competent authorities. (STRO: S 48, CDSA; MAS and financial supervisors: S19-20, FSMA, IRAS: S6(4)(b), 6(4A); and part A of the ITA; ICA: S36B, IA, S55, PA). Competent authorities generally do not refuse a request for assistance on the four grounds listed in this criterion as long as foreign requests are clear, relevant and proportionate. The requesting party must also ensure the confidentiality, and the proper use of the information shared. MAS provides international co-operation only when several criteria are all satisfied which go beyond the requirements of R.40 (S19, FSM Act). For example, requests from foreign counterparts should specify the identity of the FI which has in its possession the information requested for or the fact that the request from the foreign counterpart must be of sufficient gravity. Although Singapore reports that no request has been refused in practice based on the criteria listed in S19, there is a potential to do so, which could hinder international co-operation.

Criterion 40.6 –

Singapore has controls and safeguards to ensure that information exchanged by competent authorities is used only for the purpose, and by the authorities, for which the information was sought or provided, unless prior authorisation has been given by the requested competent authority. Competent authorities follow established principles set out in their SOPs, or in line with international frameworks (Egmont Group for STRO, INTERPOL for LEAs).

Criterion 40.7 –

Competent authorities maintain appropriate confidentiality for any request for co-operation and the information exchanged, consistent with both parties' obligations concerning privacy and data protection (S77 of the CDSA, S3 of the Statutory Bodies and Government Companies (Protection of Secrecy) Act, s5(1)(e-f), OSA). LEAs have SOPs in place to ensure the safeguarding of information received from foreign counterparts. Competent authorities may refuse co-operation in case a counterpart is not able to protect the information effectively.

Criterion 40.8 –

Competent authorities can conduct inquiries on behalf of their foreign counterparts and exchange with their foreign counterparts all information that would be obtainable by them if such inquiries were being carried out domestically. STRO is able to conduct inquiries on behalf of its foreign counterparts and exchange financial intelligence that it is able to obtain (e.g. information supplied by reporting entities, pursuant to S5(3), CDSA)), or which is available in its database (S48, CDSA and Egmont Group's frameworks). As set out in the SOPs, LEAs are also able to conduct inquiries on behalf of counterparts (even in the absence of ML investigations) and share relevant information.

Exchange of Information between FIUs

Criterion 40.9 –

Singapore's FIU (STRO) has an adequate legal basis for providing co-operation on ML, PO and TF (S48, CDSA). Information can be shared regardless of the nature of the counterpart FIU (administrative, law enforcement, judicial/other), provided it is relevant to an investigation by that foreign authority into a foreign ML, associated predicate or TF offence. Since 2019, STRO is able to exchange information with all FIUs in the Egmont Group without a need for an LOU/MOU as long as basic safeguards of confidentiality are guaranteed in line with the Egmont Principles for Information Exchange between FIUs. As of July 2024, STRO has also concluded 42 MOUs and nine LOUs, including non-Egmont members.

Criterion 40.10 –

In line with its internal guidelines, when requested, STRO must provide feedback to foreign counterparts on the use and usefulness of the information exchanged within two weeks. Singapore reports that STRO regularly engages with counterparts to inform them of the outcome of the analysis conducted.

Criterion 40.11 –

STRO is authorised to exchange all information accessible or obtainable directly or indirectly by it, and any other information which it has the power to obtain or access, directly or indirectly, at the domestic level, with its foreign counterparts in line with R.29 (S48, CDSA). This includes information that STRO is able to obtain or access (S5(3), 45(1), 60, 61, 62 and 68(1), CDSA; S200 Casino Control Act, S17 PSPM Act, S74A Pawnbrokers Act 2015, S 28L(4) of the FSM Act). As well, STRO is able to access and exchange information directly accessible from SPF databases or requested from other enforcement units.

Criterion 40.12 –

Singapore ensures that LEAs like SPF (CAD) are able to take immediate action directly to suspend a transaction that is suspected of being related to money laundering, predicate offences or terrorist financing, in response to a relevant request from a foreign jurisdiction. Singapore provided case studies indicating this occurs in a timely manner (i.e. within a few hours from receiving the request).

STRO does not have the powers to suspend transactions, as this power is provided to LEAs like SPF, CPIB or CNB only (Part 4, S35, CPC) (see c 4.3). When STRO receives a transaction suspension request, it will undertake preliminary analysis to assess whether there is sufficient information indicating assets are proceeds of crime, and subject to the foreign counterpart's consent to share information, STRO will convey this to SPF(CAD) for action. If the competent authority having this power in the requesting countries are not counterparts, the request should be sent by SPF. This could involve some delays and is not fully aligned with the requirements of this criterion.

Exchange of information between financial supervisors

Since the 2016 MER, Singapore has not addressed the minor deficiency concerning the lack of legal basis to allow IPTO (Insolvency and Public Trustee's Office) under MinLaw to co-operate with its foreign counterparts. However, there is no specific impediment or prohibition preventing this co-operation from happening in practice, and financial supervisors can rely on established common law principles to engage in international co-operation, particularly concerning the confidentiality of information.

Criterion 40.13 –

MAS has an appropriate legal basis to provide co-operation with its foreign counterparts, irrespective of their nature or status (S17, S19(1)(b), and Part 4, FSMA).

Criterion 40.14 –

MAS has broad powers to obtain information domestically, including information held by FIs, and to exchange it with foreign supervisors in a manner proportionate to their respective needs (S 19(1), 20(1), FSMA).

Criterion 40.15 –

MAS is able to exchange information in criteria a to c when relevant for AML/CFT purposes, in particular with other supervisors that have a shared responsibility for FIs operating in the same group (S20, FSMA).

Criterion 40.16 –

MAS is able to conduct inquiries on behalf of foreign counterparts and provide any information in its possession (such as inspection reports), or instruct FIs to provide this information (S20, FSMA). MAS may also approve AML/CFT examinations of FIs in Singapore by foreign counterparts in order to facilitate effective group supervision (S26, FSMA).

Criterion 40.17 –

MAS is authorised to disseminate information exchanged only with the prior permission of the requested financial supervisor and has controls and safeguards in place to ensure that information is used appropriately. It is unclear whether this information covers both supervisory and non-supervisory purposes. (SOP for International Co-operation for AML/CFT Supervisory Purposes).

Exchange of information between law enforcement authorities

Criterion 40.18 –

Nothing prevents LEAs from exchanging domestically available information with foreign counterparts for intelligence or investigative purposes relating to ML, associated predicate offences or TF (see c.40.2(a)). This includes for example information obtained through screenings in existing databases (e.g. travel records) and publicly accessible information (such as company registration, land ownership and information obtained on a voluntary basis). In practice, information-sharing with foreign counterparts happens through INTERPOL, as well as a network of SPF attachés posted abroad, bilateral relations and engagement with accredited foreign police forces, secondment of SPF forces to Interpol. Other platforms (e.g. IACCC and RILO) are also used. Information can also be shared through engagement in a joint investigation with foreign counterparts.

Criterion 40.19 –

LEAs are able to:

Sub-criterion 40.19(a) - exchange domestically available information for intelligence or investigative purposes and co-operate with foreign counterparts to identify and trace criminal property and property of corresponding value, and in support of the freezing, seizing, and confiscation of such property through the formal MLA process. There is no obstacle to sharing domestic information with foreign counterparts (see c.40.18).Where required, this information can be exchanged through platforms such as ARIN-AP.

Sub-criterion 40.19(b) - commence domestic investigations or proceedings based on such information received from foreign counterparts, in appropriate cases. Singapore provided case studies showing this occurs in practice.

Criterion 40.20 –

Law Enforcement authorities:

Sub-criterion 40.20(a) - are able to spontaneously share relevant information regarding criminal property and property of corresponding value with foreign counterparts without a prior request. LEAs do this by leveraging on different platforms, such as INTERPOL, Egmont, ARIN, as well as direct bilateral relationships. Singapore provided case studies showing this occurs in practice.

Sub-criterion 40.20(b) - are able to spontaneously identify and trace criminal property and property of corresponding value if they suspect that such property relating to a foreign investigation may be located in Singapore drawing on their domestic powers (see R.4). Singapore provided case studies showing this occurs in practice.

Criterion 40.21 –

LEAs are able to assist their foreign counterparts in conducting inquiries and obtaining information using the powers bestowed upon them through domestic legislation (see R.3, and S21-22-34-39-111, CPC). To do so, LEAs in counterpart countries should send a bona fide request containing reliable and sufficient information on the foreign predicate offence committed and its nexus to a possible ML offence in Singapore. If this threshold is not met, LEAs will only provide information obtained through screenings in existing databases, publicly available information, and information obtained on a voluntary basis. Agreements that Singapore is party to governing such law enforcement co-operation govern restrictions on the type of information that can be shared and how it can be used. For example, LEAs must abide by international principles such as the INTERPOL's Rules on the Processing of Data, and/or the Protocol of Co-operation concerning the sharing of information between IACCC members. As set out in various SOPs of LEAs, the exchange of information is for investigation purposes only and is conducted on the basis of reciprocity and the ability of foreign counterparts to safeguard data confidentiality.

Criterion 40.22 –

LEAs are able to form joint investigative teams to conduct cooperative investigations with their foreign counterparts. Singapore provided case studies showing this occurs in practice.

Criterion 40.23 –

Sub-criterion 40.23(a) – Singapore takes part in multilateral networks to better facilitate rapid and constructive international co-operation in asset recovery. Singapore is an active contributor (including as a steering group member) in ARIN-AP. The SPF has utilised INTERPOL's Global Rapid Intervention of Payments (I-GRIP) to intercept illegal proceeds of CEF, including virtual assets transferred through hosted wallets in more timely and systematic manner. STRO is an Egmont Member since 2002. CNB is part of a range of networks/ participants in various drug related platforms. Singapore is also a founding member of Internation Anti-Corruption Co-ordination Centre (IACCC) since 2017, which seeks to co-ordinate global law enforcement responses to allegations of grand corruption and facilitate the timely exchange of information.

Sub-criterion 40.23(b) - Singapore joined ARIN-AP in 2017 (see above as well).

Exchange of information between non-counterparts

Criterion 40.24 –

Singapore permits competent authorities to exchange information indirectly with non-counterparts, while making clear for what purpose and on whose behalf the request is made. MAS can share information, upon request, with other domestic authorities for their investigation, enforcement action or supervisory action, or provide this information spontaneously to a domestic authority (S22, S25, FSMA). However, while the

provisions seem to limit the scope of assistance to only AML/CFT supervisory purposes (S19.1 (b) FSMA), Singapore provided case studies showing that MAS is able to provide assistance, subject to adequate confidentiality safeguards, when requested for purposes other than supervision or take supervisory action.

> ***Weighting and conclusion –*** Competent authorities are able to provide a broad range of international co-operation, both spontaneously and upon request, in relation to ML, predicate offences and TF. However, shortcomings with respect to R.5 have a cascading impact on the scope of international co-operation that can be provided. It is also unclear to what extent the scope of co-operation provided by MAS is limited to supervision or supervisory action. STRO's reliance on LEAs to suspend transactions means that, when requested, it may not be able to provide immediate assistance, particularly for non-counterparts. These are all minor shortcomings.
>
> Recommendation 40 is rated **Largely Compliant**.

Annex B. Technical compliance shortcomings

The Recommendations presented in green have been subject to a full assessment, reflecting either amendments to the FATF Standards or substantive changes made by the country to its legal, regulatory, or operational frameworks since its last mutual evaluation. The remaining Recommendations are based on pre-existing information from the country's most recent assessments and have not been reassessed in this review.

Recommended actions	Rating	Factor(s) underlying the rating
1) Assessing risks & applying a risk-based approach	Largely compliant	• The existing mechanism cannot ensure comprehensive and up-to-date risk understanding, nor systematically consider overall risk landscape in allocating supervisory resources across sectors with varying risk levels.
2) National co-operation and co-ordination	Compliant	• All criteria are met.
3) Money laundering offence	Compliant	• All criteria are met.
4) Confiscation and provisional measures	Largely compliant	• The application of provisional measures can be done for up to one year, which is unduly long and inconsistent with an emergency measure.
5) Terrorist financing offence	Largely compliant	• Criminal sanctions for legal persons are too low to be sufficiently dissuasive
6) Targeted financial sanctions related to terrorism and terrorist financing	Largely compliant	• In relation to asset freezing, there is no explicit provision to clarify that the prohibition against dealing requires that the subject not be given prior notice, and that the prohibition extends to property that is owned "wholly or jointly" by a designated person or entity. There are no provisions under the laws governing TF TFS related to bona fide rights of third parties.
7) Targeted financial sanctions related to proliferation	Largely compliant	• There is no explicit provision in accordance with the exemptions under the UNSCRs.
8) Non-profit organisations	Compliant	• All criteria are met.
9) Financial institutions secrecy laws	Compliant	• All criteria are met.
10) Customer due diligence	Compliant	• All criteria are met.
11) Record-keeping	Compliant	• All criteria are met.
12) Politically exposed persons	Compliant	• All criteria are met.
13) Correspondent banking	Compliant	• All criteria are met.
14) Money or value transfer services	Compliant	• All criteria are met.
15) New technologies	Largely compliant	• The SGD 1 500 threshold is higher than the FATF Standard threshold for capturing accurate information (EUR/USD 1 000).
16) Wire transfers	Largely compliant	• The threshold of SGD 1 500 is higher than the FATF Standard threshold for capturing accurate information about (EUR/USD 1 000).
17) Reliance on third parties	Compliant	• All criteria are met.
18) Internal controls and	Compliant	• All criteria are met.

foreign branches and subsidiaries		
19) Higher-risk countries	Largely compliant	• The required enhanced CDD does not provide for a sufficient wide range of measures that are proportionate to the risks in all instances.
20) Reporting of suspicious transactions	Compliant	• All criteria are met.
21) Tipping-off and confidentiality	Compliant	• All criteria are met.
22) DNFBPs: customer due diligence	Compliant	• All criteria are met.
23) DNFBPs: other measures	Largely compliant	• 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.
24) Transparency and beneficial ownership of legal persons	Partially compliant	• The alternative approach for BO related to VCCs is not based on a documented decision that factors in risk, context and materiality. • There are gaps in relation to verification requirements and accuracy of BO information.
25) Transparency and beneficial ownership of legal arrangements	Partially compliant	• Obligations are placed on trustees and trustee equivalents to obtain and hold a range of basis and BO information on the trust and wakafs, but LTC trustees do not have to verify the accuracy of this information (on the natural person) when one of the parties is a legal person or legal arrangement. • There is not adequate, accurate and up-to-date information on the basic and BO of the trusts or other similar legal arrangements, trustees and trust assets accessible efficiently and in a timely manner by competent authorities.
26) Regulation and supervision of financial institutions	Compliant	• All criteria are met.
27) Powers of supervisors	Compliant	• All criteria are met.
28) Regulation and supervision of DNFBPs	Largely compliant	• There are minor deficiencies in the dissuasiveness and proportionality of sanctions for lawyers and law practice entities.
29) Financial intelligence units	Largely compliant	• There is a minor deficiency with the lack of safeguards to preserve STRO's operational independence.
30) Responsibilities of law enforcement and investigative authorities	Compliant	• All criteria are met.
31) Powers of law enforcement and investigative authorities	Compliant	• All criteria are met.
32) Cash couriers	Largely compliant	• LEAs are able to retain the CBNI for a time that appears unreasonable.
33) Statistics	Compliant	• All criteria are met.
34) Guidance and feedback	Compliant	• All criteria are met.
35) Sanctions	Largely compliant	• The maximum penalty for lawyers and law practice entities remains insufficient and is not proportionate and dissuasive.
36) International instruments	Compliant	• All criteria are met.
37) Mutual legal assistance	Compliant	• All criteria are met.
38) Mutual legal assistance: freezing and confiscation	Compliant	• All criteria are met.
39) Extradition	Compliant	• All criteria are met.
40) Other forms of international co-operation	Largely compliant	• It is unclear to what extent the scope of co-operation provided by MAS is limited to supervision or supervisory action. • STRO's reliance on LEAs to suspend transactions means that, when requested, it may not be able to provide immediate assistance, particularly for non-counterparts.

Glossary of acronyms

Acronym	Definition
3B$ Case	SGD 3 Billion Case in 2023
AC3N	AML Case Co-ordination and Collaboration Network
ACIP	AML/CFT Industry Partnership
ACIP CSI	ACIP Case-Specific Information Taskforce
ACRA	Accounting and Corporate Regulatory Authority
AGC	Attorney General Chambers
AMLD	AML Department of the Monetary Authority of Singapore
AML/CFT SC	AML/CFT Steering Committee
ASEAN	Association of Southeast Asian Nations
AUM	Assets Under Management
BEC	Business Email Compromise
CAD	Commercial Affairs Department
CBMT	Cross-Border Money Transfer
CDD	Customer Due Diligence
CDP	Central Depository Pte Ltd
CDSA	Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992
CEA	Council for Estate Agencies
CEF	Cyber-enabled Fraud
CFTB	Counter-Financing of Terrorism Branch
CIS	Collective Investment Scheme
CLG	Companies limited by guarantee
CMRs	Cash Movement Reports
CNB	Central Narcotics Bureau of Singapore
COC	Commissioner of Charities
COSMIC	Collaborative Sharing of ML/TF Information & Cases
CPIB	Corrupt Practices Investigation Bureau
CSPs	Corporate Services Providers
CTRs	Cash Transaction Reports
DD	Deputy Director
dCMP	Digital capital markets product
DPTSPs	Digital payment token service providers
DTSPs	Digital Token Services Providers
EAM	External Asset Managers
EFI	Eligible Financial Institution
ESC	Egmont Secure Channel
FICG	Financial Intelligence Consultative Group
FIN-IR	Financial Intelligence Report
FRFCP	Foreign Charitable Purposes
FSM	Financial Services and Markets
GRA	Gambling Regulatory Authority
HNWI/UHNWI	High-net Worth Individual/Ultra High-net Worth Individual
IAC	Inter-Agency Committee
ICA	Immigration and Checkpoints Authority
IFC	International Financial Centre
IMC-CT	Inter-Ministry Committee on Counter Terrorism
IMC-EC	Inter-Ministry Committee on Export Controls
IMC-Scams	Inter-Ministry Committee on Scams
IMC-TD	Inter-Ministry Committee on Terrorist Designation
ISA	Internal Security Act
ISD	Internal Security Department

ISTRA	Inter-Agency STR Analytics Taskforce
JOG	Joint Ops Group
LARA	Legal Arrangements Risk Assessment
LEAs	Law Enforcement Agencies
LLP	Limited Liability Partnership
LPEs	Law Practice Entities
LPRA	Legal Persons Risk Assessment
LTCs	Licensed Trust Companies
MACMA	Mutual Assistance in Criminal Matters Act 2000
MAS	Monetary Authority of Singapore
MER	Mutual Evaluation Report
MHA	Ministry of Home Affairs
MINDEF	Ministry of Defence
MinLaw	Ministry of Law
MLA	Mutual Legal Assistance
MMB	Mosque Management Board
MOF	Ministry of Finance
MOM	Ministry of Manpower
MPA	Maritime and Port Authority of Singapore
MTI	Ministry of Trade and Industry
MUIS	Majlis Ugama Islam Singapore
NARS	National Asset Recovery Strategy
NAVIGATE	National AML Verification Interface for Government Agencies' Threat Evaluation
NRA	National Risk Assessment
NSCFT	National Strategy for Countering the Financing of Terrorism
Project POET	Project Production Order Electronic Transmission project
PS	Permanent Secretary
PSMDs	Precious Stones and Precious Metal Dealers
PSPs	Payment Service Providers
PTC	Private Trust Company
SEI	Spontaneous Exchange of Information
SGD	Singapore Dollar
SONAR	STRO Online Notices and Reporting Platform
SOP	Standard Operating Procedure
SPF	Singapore Police Force
SPRC	Security Policy Review Committee
STR	Suspicious Transaction Report
STRO	Suspicious Transaction Reporting Office
REA	Real Estate Agents
ROND	Register of Nominee Directors
RONS	Register of Nominee Shareholders
RORC	Register of Registrable Controllers
RTIG	Risk, Typologies Inter-Agency Group
TBML	Trade-based Money Laundering
TSOFA	Terrorism (Suppression of Financing) Act 2002
UFC	Unregistered Foreign Companies
URA	Urban Redevelopment Authority
VCC	Variable Capital Companies
WMS	Wakaf Masyarakat Singapura
WoG	Whole of Government
WoS	Whole of Society

www.fatf-gafi.org

May 2026

Mutual Evaluation of Singapore - Anti-money laundering and countering the financing of terrorism and proliferation financing measures

In this report: a summary of the anti-money laundering (AML)/countering the financing of terrorism (CFT)/counter-proliferation financing (CPF) measures in place in Singapore at the time of an on-site visit in July 2025.

The report analyses the level of effectiveness of Singapore's AML/CFT/CPF system, the level of compliance with the FATF 40 Recommendations and provides recommendations on how the system could be strengthened.