

**NATIONAL ANTI-MONEY LAUNDERING STRATEGY  
SINGAPORE  
2024**

**CONTENTS**

**1. INTRODUCTION .....3**

**2. WHOLE-OF-SOCIETY COORDINATION AND COLLABORATION .....7**

**3. LEGAL AND REGULATORY FRAMEWORK .....11**

**4. INTERNATIONAL COOPERATION .....18**

**5. PREVENT .....20**

**6. DETECT.....25**



**7. ENFORCE.....28**

**8. CONCLUSION .....30**

**TABLE OF ACRONYMS.....31**

## 1. INTRODUCTION

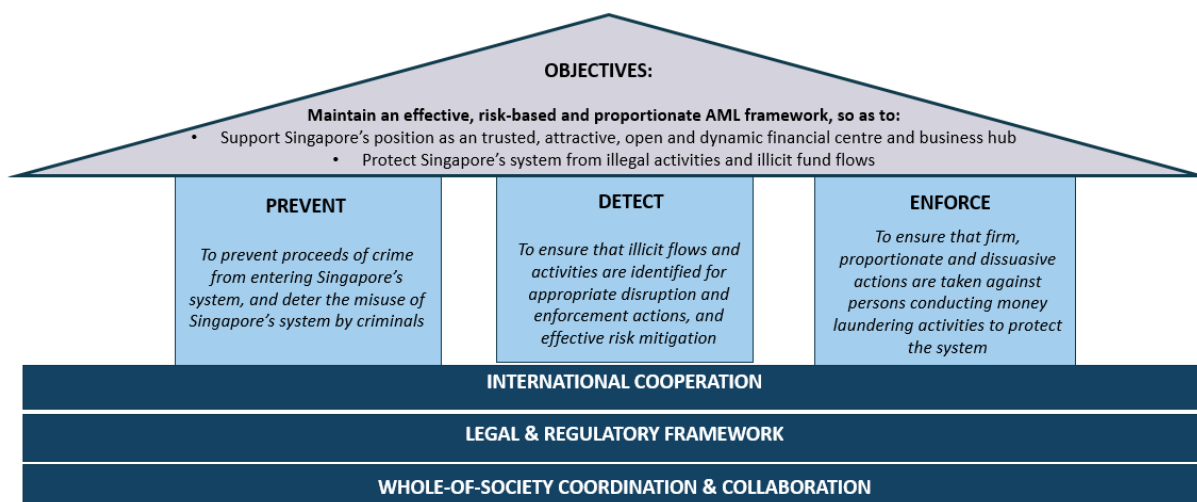
- 1.1 As an international business, financial and trading centre, Singapore is exposed to the risks of transnational money laundering (ML) as criminals seek to exploit our economic openness, financial system and business infrastructure to launder and integrate illicit funds and assets.
- 1.2 Having a robust anti-money laundering (AML) system and framework protect Singapore’s system from illegal activities and illicit fund flows and reinforces Singapore’s reputation as a trusted international financial centre and business hub. **Combatting ML is thus of national importance to Singapore.**
- 1.3 In 2016, Singapore published a National Policy Statement on Money Laundering/Terrorism Financing (ML/TF)<sup>1</sup>, which laid out Singapore’s policy objectives to detect, deter and prevent ML, associated predicate offences and terrorist financing; and protect the integrity of our financial system from illegal activities and illicit funds. The 2016 National Policy Statement further set out the objectives and principles for achieving these policy objectives. Guided by these objectives and principles, Singapore has continued to enhance our AML framework in response to the changing environment and risk landscape and our AML efforts have shown success over the years.
- 1.4 **This National AML Strategy document expands on the 2016 National Policy Statement, and provides an update on Singapore’s AML approach.** It takes into account key ML risks observed by agencies over the years, including the updated Money Laundering National Risk Assessment (ML NRA) which synthesised observations on ML risks over the years, as well as other risk assessments and reviews.
- 1.5 As set out in the updated ML NRA, Singapore faces increasingly complex ML risks, in tandem with geopolitical and macro-economic developments, the use of sophisticated structures, and technological advancements. The key findings of the ML NRA are summarised in the table below.

KEY ML THREATS	
 <b>Fraud</b> , particularly cyber-enabled fraud	 <b>Corruption</b> , originating from abroad
 <b>Organised Crime</b> , especially illegal online gambling associated with foreign organised criminal groups	 <b>Tax Crimes</b> , originating from abroad
	 <b>Trade-based money laundering</b>
OTHER NOTABLE ML THREATS	
 <b>Environmental Crime</b>	 <b>Drug-related offences</b>
 <b>Cyber-crime</b>	
HIGHER ML RISK SECTORS	
<i>Inherent exposure to key ML threats, and cross-border transactions/customers, despite stronger controls</i>	
 <b>Banks pose highest ML risks to Singapore</b>	
 <i>Abused through their roles as professional / financial intermediaries, exposure to cross-border transactions, and/or placement in high value assets, while taking into account controls in place</i>	
<ul style="list-style-type: none"> <li>• Corporate Services Providers</li> <li>• Real Estate</li> <li>• Casinos</li> <li>• Licensed Trust Companies</li> <li>• Precious stones and precious metal dealers</li> </ul>	<ul style="list-style-type: none"> <li>• Digital Payment Token Services Providers</li> <li>• Payment Institutions, with cross border money transfer services</li> <li>• External Asset Managers</li> </ul>

For more details on the ML threats and risks in Singapore, please refer to the ML NRA (<https://www.mas.gov.sg/publications/monographs-or-information-paper/2024/money-laundering-national-risk-assessment>), as well as other relevant publications which the authorities publish from time to time.

<sup>1</sup> Please refer to (<https://www.mas.gov.sg/publications/monographs-or-information-paper/2016/national-policy-statement>)

1.6 Taking into consideration the observations in the ML NRA, this National AML Strategy provides the blueprint of Singapore’s approach to address the identified ML threats and risks and sets out the actions which Singapore has taken and will be taking to further enhance our AML framework. **Singapore’s National AML Strategy seeks to maintain an effective, risk-based and proportionate AML framework, through three inter-dependent, horizontal Building Blocks and three Pillars, summarised in the diagram below.**



1.7 The details of the policy statements and actions which Singapore has taken and will be taking, under each of the Building Blocks and Pillars in the National AML Strategy are elaborated in the following chapters. The forward-looking actions which Singapore will be taking against ML risks are summarised in the table below.

BUILDING BLOCKS	ACTIONS AHEAD
<p><b>Whole-of Society Coordination and Collaboration</b>  <i>Singapore adopts a whole-of-society approach to combat ML, with the Government and private sector entities each having important roles to play.</i></p>	<p><b>(1) Further strengthen sensemaking and information-sharing mechanisms within and among government agencies</b></p> <ul style="list-style-type: none"> <li>a) Develop a Whole-of-Government (WOG) data sharing interface, the National AML Verification Interface for Government Agencies Threat Evaluation (NAVIGATE)</li> <li>b) Establish an AML Sensemaking workgroup to oversee operations-technology and capability development across government agencies.</li> </ul> <p><b>(2) Continue to deepen channels for data sharing amongst and with private sector entities</b></p>
<p><b>Legal &amp; Regulatory Framework</b>  <i>Singapore has a strong and transparent AML legal &amp; regulatory framework, which is consistent with international standards and best practices.</i></p>	<p><b>(3) Continue to develop and maintain a robust AML legal and regulatory framework</b></p> <p><b>(4) Clarify requirements to ensure consistent baseline in AML/CFT requirements across sectors</b></p>

<p><i>Singapore implements risk-based and proportionate AML requirements, to ensure collective efforts to prevent and deter the system from being misused for illicit activities and laundering of illicit funds</i></p>	
<p><b>International Cooperation</b>  <i>Singapore authorities actively cooperate with their international and regional counterparts, through formal and informal channels to achieve law enforcement and supervisory objectives for AML matters.</i></p>	<p><b>(5) Continue to leverage on international cooperation and provide timely and quality assistance to actively tackle ML activities</b></p> <p><b>(6) Enhance Singapore’s legal framework and processes to improve Singapore’s ability to provide and request for assistance in international criminal cooperation</b></p> <ul style="list-style-type: none"> <li>a) Amendments to the Mutual Assistance in Criminal Matters Act (MACMA)</li> </ul>
<p><b>PILLARS</b></p>	<p><b>ACTIONS AHEAD</b></p>
<p><b>Prevent</b>  <i>Singapore implements robust and risk-based supervisory frameworks on Financial Institutions (including Digital Payment Token Services Providers), Designated Non-Financial Businesses and Professions, and Non-Profit Organisations, to ensure effective implementation of requirements under the AML regulatory framework.</i></p> <p><i>Singapore seeks to prevent misuse of companies for illicit purposes, and promote transparency of legal persons and legal arrangements.</i></p>	<p><b>(7) Continue to enhance effectiveness of risk-based supervision</b></p> <p><b>(8) Continue to engage and uplift the capabilities of AML/CFT obligated entities</b></p> <p><b>(9) Enhance beneficial ownership transparency for legal persons and legal arrangements</b></p> <ul style="list-style-type: none"> <li>a) Review and develop next phase of beneficial ownership framework for legal persons, through collaboration with industry partners</li> <li>b) Enhance beneficial ownership framework for trusts through amendments to the Trustees Act</li> </ul> <p><b>(10) Continue to implement risk-based measures to prevent at-risk companies from being abused</b></p> <ul style="list-style-type: none"> <li>a) Continue pre-incorporation checks on companies</li> <li>b) Active monitoring and strike-off of inactive companies</li> </ul>
<p><b>Detect</b>  <i>Singapore performs active risk surveillance for timely detection of illicit activities, emerging threats and risks, and effective risk mitigation</i></p>	<p><b>(11) Continue to enhance detection capabilities and tools across public and private sectors</b></p> <ul style="list-style-type: none"> <li>a) Enhance training to strengthen agencies’ sense-making capabilities [<i>complements NAVIGATE and AML sensemaking workgroup</i>]</li> <li>b) Continued review of effectiveness of surveillance tools and information sharing mechanisms, including review of COSMIC (Collaborative Sharing of Money Laundering/Terrorism Financing Information &amp; Cases)</li> </ul>

<p><b>Enforce</b>  <i>Singapore adopts a multi-pronged approach in identifying ML activity, and rigorously investigates all leads to uncover possible ML offences, and takes dissuasive and proportionate actions against ML activity, including that relating to foreign crimes</i></p>	<p><b>(12) Prioritise law enforcement outcomes in areas of key risks and transnational complex ML cases</b> <i>[complements enhancements in operational coordination and collaboration, including through the AML Case Coordination and Collaboration Network (AC3N)]</i></p> <p><b>(13) Continue to prioritise asset recovery</b></p> <p><b>(14) Enhance AML penalty frameworks in real estate and legal sectors, to ensure penalties are dissuasive and proportionate</b></p>
--	---

## 2. WHOLE-OF-SOCIETY COORDINATION AND COLLABORATION

Policy statement:

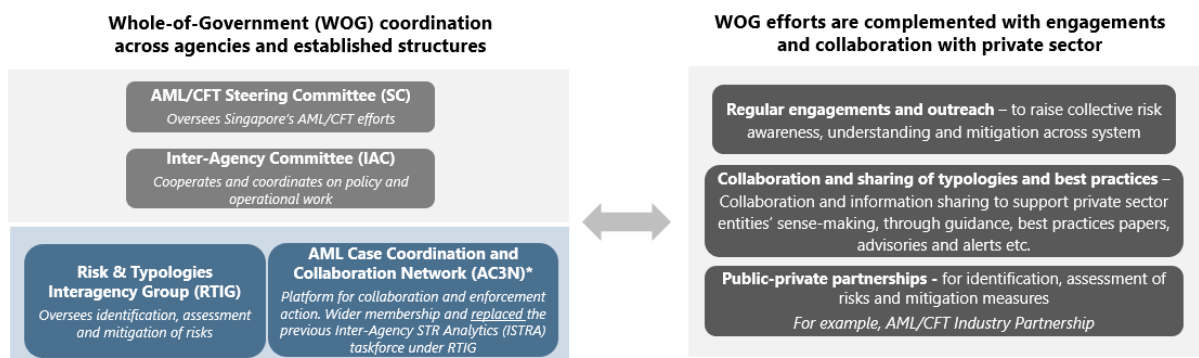
**Singapore adopts a whole-of-society approach to combat ML, with the Government and private sector entities each having important roles to play.**

2.1 International typologies and cases observed in Singapore have shown that ML is increasingly complex, facilitated by greater inter-connectivity and technological advancements. Criminals, especially international crime syndicates, may abuse different structures, and launder illicit funds and assets through multiple sectors to “layer” or disguise their origin, before integrating these proceeds into all parts of the legitimate economy. **Combatting ML thus requires the close coordination and collaborative effort of all stakeholders in the ecosystem.**

Strategy in Action:

2.2 Singapore’s whole-of-society approach against ML comprises (i) established structures across government agencies to maintain close policy and operational coordination and cooperation in order to identify and assess ML risks, and (ii) established partnerships, close engagement and collaboration with the private sector entities. This is summarised in diagram 1 below.

Diagram 1: Summary of structures and mechanisms:



*\*AC3N replaced the previous ISTRA mechanism which was set up in 2018). Please refer to paragraph 2.7 below for more information.*

WOG structures and coordination:

2.3 Singapore’s AML efforts are led by the AML/CFT Steering Committee (SC), which comprises the Permanent Secretary of the Ministry of Home Affairs (MHA), the Permanent Secretary of the Ministry of Finance (MOF), and the Managing Director of the Monetary Authority of Singapore (MAS). The AML/CFT SC sets Singapore’s policy objectives and directions for combatting ML and ensures that the various government agencies have effective mechanisms in place to cooperate and coordinate with one another, and to strengthen Singapore’s resilience against criminal abuse.

2.4 The AML/CFT SC is supported by the AML/CFT Inter-Agency Committee (IAC). The IAC is the main operational body that facilitates the coordination and implementation of Singapore’s AML policy. The

SC and IAC are further supported by the Risk Typologies Inter-Agency Group (RTIG), which is the main working level body tasked to review ML risks at the government level. The IAC and RTIG comprise all operational, law enforcement, regulatory, supervisory and policy agencies involved in AML/CFT work in Singapore. Through the IAC and RTIG, agencies also share information such as emerging ML threats and trends, Financial Action Task Force (FATF) typologies, best practices and other developments.

2.5 These established inter-agency structures are also supplemented by ad-hoc committees that undertake targeted reviews of our AML/CFT framework. For example, arising from a recent major ML case, an inter-ministerial committee (IMC) was set up, comprising Political Office Holders across multiple Ministries, to review Singapore's AML framework<sup>2</sup>.

2.6 The participation of senior level leadership and investment of significant resources into AML work in Singapore over the years demonstrate Singapore's strong political support and commitment towards combatting ML.

2.7 At the operational level, the Inter-Agency Suspicious Transaction Report Analytics Taskforce (ISTRA) was formed in 2018 under the auspices of the RTIG, to facilitate the development, prioritisation, and coordination of significant ML cases across agencies, including law enforcement and supervisory authorities. ISTRA enabled better identification of complex and sophisticated forms of ML activities by (a) leveraging on data analytics for more focused detection of suspicious networks; and (b) providing a channel for WOG coordination to mitigate the risks arising from these suspicious networks.

- Arising from the IMC review, the ISTRA mechanism has been replaced by AC3N. With wider membership and higher level of oversight, AC3N allows for even more effective and coordinated investigative, supervisory and enforcement actions across agencies.
- Through AC3N, sector supervisors will also gain deeper insights into risks affecting their specific sectors and drive risk-based supervisory efforts.
- Please refer to paragraphs 2.15 and 2.16 below for further actions which Singapore will be taking to strengthen the sensemaking and information-sharing mechanisms across the ecosystem.

2.8 Singapore has also put in place strategies, operational guidelines, and procedures to facilitate the inter-agency structures and effective functioning of our AML system. Beyond the formal and established inter-agency structures, AML/CFT agencies work closely together on a bilateral and regular basis. For example, law enforcement agencies (LEAs) and sector supervisors regularly engage each other to exchange risk information and discuss mitigation actions. Secondments of officers between agencies also enhance partnerships.

*Collaboration and engagement with private sector:*

2.9 The effectiveness of Singapore's AML framework does not rest on the efforts of government agencies alone. The agencies engage private sector entities (especially in higher-risk sectors identified in ML NRA) closely to raise awareness of ML risks and share information for effective implementation of risk mitigation measures.

---

<sup>2</sup> The IMC's review focused on five key areas: (a) How to better prevent money launderers from misusing corporate structures, (b) How financial institutions can enhance their controls and collaborate more effectively with one another and the authorities to identify and flag suspicious transactions, (c) How other gatekeepers in the system, like corporate service providers, real estate salespersons and estate agencies, and precious stones and precious metals dealers can better guard against money laundering risks, including the adequacy of the existing regulatory framework over these players, (d) How to better centralise and strengthen monitoring and sense-making capabilities across government agencies to detect suspicious activities; and (e) How to strengthen enforcement levers and capabilities to enable firm and decisive actions against money launderers, including depriving them of ill-gotten proceeds.

The IMC's findings and recommendations were published on 4 Oct 2024. For more details, please refer to (<https://www.mas.gov.sg/-/media/mas-media-library/news/media-releases/2024/imc-report.pdf>)



- 2.10 As outlined in the ML NRA, the agencies have established public-private partnerships including the AML/CFT Industry Partnership (ACIP), Alliance of Public Private Cybercrime Stakeholders (APPACT) and Anti-Corruption Partnership Network (ACPN)<sup>3</sup>, ACIP has set up working groups, comprising a range of experts across the industry, to look into key industry risk concerns such as the misuse of legal persons, virtual assets, and Trade-Based Money Laundering (TBML), and to explore the use of data analytics to combat financial crime. Over the years, ACIP has produced Best Practices Papers<sup>4</sup> which raise industry awareness and promote best practices to identify and mitigate key ML/TF risk concerns in Singapore.
- 2.11 The Anti-Scam Centre (ASC)<sup>5</sup> is another example of strong public-private partnership. Set up in 2019, the ASC serves as a nerve centre for tracing and disrupting the flow of illicit funds in the financial system. Through the ASC, private sector stakeholders such as banks work with the SPF, to coordinate real time disruption and freezing of funds. In 2020, ASC launched Project FRONTIER, working closely with partner banks, FinTech companies, online marketplaces, and other stakeholders to disrupt illicit fund flows by swiftly freezing bank accounts and mitigating victims' losses. Today, this network comprises over 100 stakeholders, including cryptocurrency firms and telecommunications companies. In 2022, the ASC was expanded to form the Anti-Scam Command (ASCom), to improve strategic oversight on all anti-scam efforts, including upstream prevention and public education, strengthen international cooperation, and enhance the efficiency of SPF's overall response to scams.
- 2.12 Authorities regularly share and exchange information with private sector entities to highlight typologies, emerging risks and intelligence on specific cases. For instance, a case-specific information sharing mechanism was established by the Commercial Affairs Department (CAD), MAS and ACIP members to share information on specific cases with relevant financial institutions (FIs), who are then able to work together, and with CAD to develop the case. One example is the Agritrade case (further details in *Box Story 1* of the ML NRA) where the FIs were able to exchange relevant information to support CAD's investigations, resulting in successful outcomes.
- 2.13 For a wider reach to the industry, sector supervisors have also established working relationships with industry associations, which facilitate engagements with the private sector. For example, MAS and CAD have regularly participated in industry events organised by the Association of Banks (Financial Crime Seminar), Association of Certified Anti-Money Laundering Specialists, etc. to discuss with the industry on key trends observed as well as challenges faced by the industry. MAS had also collaborated with the Singapore Trustees Association to develop a best practices paper on managing ML/TF risks associated with complex trust structures<sup>6</sup>.

### **Actions Ahead:**

- 2.14 Given the increasing complexity of ML threats, it is critical that **Singapore continues to adopt a whole-of society approach to combat criminal and ML activities. Stakeholders cannot work in silos.**
- 2.15 Following the IMC's review of Singapore's AML framework, **Singapore will be further strengthening the sensemaking and information-sharing mechanisms within and among the government agencies,** through the following:

---

<sup>3</sup> Please refer to section 4.6 of the ML NRA for more information on ACIP, APPACT and ACPN.

<sup>4</sup> Please refer to (<https://www.mas.gov.sg/regulation/anti-money-laundering/amlcft-industry-partnership-acip>) for the papers produced by ACIP.

<sup>5</sup> Please refer to Singapore's Law Enforcement Strategy to Combat Money Laundering at (<https://go.gov.sg/leaamlstrategy2024>) for more information.

<sup>6</sup> Please refer to (<https://www.sta.org.sg/industry-best-practice-paper/>)

- a) **Development of a WOG data sharing interface**, NAVIGATE, which will allow agencies to seamlessly screen against one another's databases and expeditiously assess entities of concern for ML risks; and
- b) **Establishment of an AML Sensemaking workgroup**, led by MHA and SPF, and comprising agencies involved in AML sensemaking efforts such as MAS and ACRA, to oversee the Government's operational policies, data sharing processes and capabilities in sense-making. This AML Sensemaking working group will support WOG sense-making efforts, by ensuring that the agencies' policies, processes and capabilities are up-to-date, and robust against emerging and sophisticated ML typologies. This AML Sensemaking workgroup will complement the case coordination work overseen by AC3N and the data-sharing on NAVIGATE.

2.16 Together with AC3N, these actions will facilitate timelier and more comprehensive sensemaking of ML risks, detection of illicit activities across the government agencies, as well as strengthen Singapore's efforts to disrupt and take dissuasive and deterrent enforcement actions against ML. **Singapore will also continue to deepen channels for data sharing amongst and with private sector entities.**<sup>7</sup>

2.17 In line with our whole-of-system approach against ML and ensure vigilance across the ecosystem, Singapore will continue to raise awareness of ML risks, and engage high value goods dealers who are currently unregulated<sup>8</sup> to highlight how they can mitigate ML risks and their obligations to file suspicious transaction reports (STRs). Singapore will monitor changes in ML risks and consider appropriate responses (including if specific sectors should be regulated or supervised more closely).

---

<sup>7</sup> Please refer to Chapter 6 for further information on Singapore's actions in relation to detection capabilities and tools across the public and private sector.

<sup>8</sup> Taking into account the typologies and cases observed, the authorities will start the engagements with the motor dealers sector given the susceptibility of vehicles being misused for ML purposes and the relatively higher value of vehicles in Singapore.

### 3. LEGAL AND REGULATORY FRAMEWORK

*Policy statement:*

***Singapore has a strong and transparent AML legal and regulatory framework, which is consistent with international standards and best practices.***

- *Singapore reviews our AML legal and regulatory framework on an ongoing basis, to keep pace with changing risk landscape and criminal typologies, and to ensure that our framework remains relevant and effective.*
- *Singapore's strong legal and regulatory framework is supported by a strong rule of law and an independent and efficient judiciary.*

***As part of the AML regulatory framework, Singapore implements risk-based and proportionate AML requirements to ensure collective efforts to prevent and deter the system from being misused for illicit activities and laundering of illicit funds.***

- 3.1 Singapore's AML legal framework is underpinned by the Corruption, Drug Trafficking, and Other Serious Crimes (Confiscation of Benefits) Act (CDSA). The CDSA criminalises the laundering of criminal benefits, sets out requirements for reporting suspicious transactions, and provides for the investigation and confiscation of such benefits. The CDSA is complemented by the MACMA for Singapore to provide a wide range of assistance to other jurisdictions on the basis of reciprocity, without the need for a bilateral mutual legal assistance treaty. LEAs who are involved in AML work (including SPF, CAD and CPIB) have extensive investigative powers under the Criminal Procedure Code (CPC) and are able to request relevant information from individuals and organisations. This enables LEAs to take swift action to investigate offences and prevent dissipation of illicit assets.
- 3.2 The overarching AML legal framework works in hand with the regulatory framework which imposes AML/CFT requirements on obligated private sector entities (including FIs and designated non-financial businesses and professions (DNFBPs), and non-profit organisations (NPOs)). The frameworks also give sector supervisors powers to monitor compliance and take actions for breaches of such requirements.

**Strategy in Action:**

- 3.3 **Singapore keeps abreast of AML developments and regularly reviews the effectiveness of our AML legal and regulatory framework.** We seek to ensure that our legal and regulatory framework remains relevant, effective and are in line with international standards and best practices. We seek to provide thought leadership and actively participate at international and regional AML-standard setting or discussion fora including the FATF<sup>9</sup>, the Asia-Pacific Group on Money Laundering (APG), the Financial Stability Board and Basel Committee on Banking Supervision, INTERPOL, and the Egmont Group.

---

<sup>9</sup> Singapore has served in various leadership roles at the FATF, including as the Co-Chair of the FATF's Policy and Development Group, member of the FATF Steering Group, and most recently the FATF President (from July 2022 to June 2024). Through such active involvement, Singapore collaborates closely with fellow AML/CFT policy makers and experts to drive and develop the international AML/CFT agenda and standards.

AML legal framework:

3.4 Singapore regularly reviews our legal framework and has strengthened our AML laws and legislative levers over the years. Key enhancements to our AML legal framework since 2019 are summarised in Table 1 below.

**Table 1: Key enhancements in Singapore’s AML legal framework**

Legislation	Year	Amendments
CDSA	2018	<ul style="list-style-type: none"> <li>• Introduction of a new ML offence to criminalise the possession or use of property reasonably suspected of being criminal proceeds, if the accused cannot satisfactorily account for it.</li> <li>• Amendments to allow Courts to decide on ML cases involving overseas crimes on the basis of evidence presented by the Prosecution, without having to rely on foreign governments or experts.</li> <li>• Increase in maximum fines for ML offences committed by legal persons; and</li> <li>• Empower STRO (Singapore’s Financial Intelligence Unit) to exchange information under an international arrangement, subject to there being an undertaking to ensure reciprocity as well as safeguards to protect the confidentiality of information shared and control their specific use<sup>10</sup>.</li> </ul>
	2023	<ul style="list-style-type: none"> <li>• Amendments to mitigate the abuse Singapore’s system for laundering of funds, especially in relation to cyber-enabled fraud. These amendments cover new ML offences including rash and negligent money laundering. It also identified four situations where the person can be liable for ML offence including allowing a third party to operate his payment account without taking reasonable steps to find out the purpose of this arrangement. This would enable LEAs to prosecute persons for a ML offence at lower levels of culpability.</li> <li>• The offence of the possession of a controlled drug under section 8(a) of the Misuse of Drugs Act 1973 was added to the First Schedule of the CDSA with effect from September 2023. It enables CNB to conduct and initiate concurrent ML and financial investigation and proceedings, even when an accused person’s drug trafficking charge is reduced to one for the possession of a controlled drug.</li> </ul>
	2024 <sup>11</sup>	<ul style="list-style-type: none"> <li>• Amendments aimed at tackling ML cases arising from foreign predicate offences where criminal benefits might have been</li> </ul>

<sup>10</sup> This has allowed STRO to exchange financial intelligence with more than 170 overseas counterpart financial intelligence units which are members of the Egmont.

<sup>11</sup> Legislative changes have been passed in Parliament, and provisions will come into force and be in effect by early 2025.

		<p>transferred through multiple banks accounts in foreign jurisdictions before entering Singapore. This includes the removal of the need for the Prosecution to show as a physical element of the offence that the properties allegedly laundered are benefits of drug dealing or criminal conduct. It will be sufficient for the Prosecution to prove beyond a reasonable doubt that the money launderer knew or had reasonable grounds to believe that he was dealing with criminal proceeds.</p> <ul style="list-style-type: none"> <li>• Amendments to allow AML/CFT supervisors, such as the Council for Estate Agencies and the Accounting and Corporate Regulatory Authority, to have access to suspicious transaction reports filed by their respective regulated entities.</li> <li>• Introduction of a Third Schedule to the CDSA, designating foreign serious environmental crimes as ML predicate offences. This will allow LEAs to initiate ML investigations if it is suspected that monies in Singapore are derived from such crimes committed overseas</li> </ul>
Computer Misuse Act (CMA)	2018	<ul style="list-style-type: none"> <li>• Amendments to pave the way for the operationalisation of the Cybersecurity Act 2018 and enhance LEAs' ability to pursue cybercrime. This serves to tackle the increasing scale and transnational nature of cyber threats and the evolving tactics of cyber criminals, and empowers investigators where computer-related evidence is involved. In the same year, the Criminal Reform Justice Act 2018 and the Evidence (Amendment) Act 2018 were passed in the Parliament and empowers relevant investigators to access, secure and safeguard evidence on computers, regardless of whether the evidence is stored on a computer inside or outside Singapore.</li> </ul>
	2023	<ul style="list-style-type: none"> <li>• Criminalisation of the disclosure and obtaining or dealing in national digital identity (or Singpass)<sup>12</sup> credentials to facilitate criminal activities. These amendments seek to curb the abuse of Singpass by deterring individuals from enabling or facilitating the commission of criminal activities such as fraud and ML by others and to protect citizens and businesses who depend on Singpass as our national digital identity.</li> </ul>
Online Criminal Harms Act (OCHA)	2023	<ul style="list-style-type: none"> <li>• Introduction of levers to enable authorities to more effectively deal with online activities that are criminal in nature. Such offences include ML and specified predicate offences. With OCHA, the Government may issue directions against specified criminal offences, proactively prevent cyber-enabled fraud and malicious cyber activities through requiring designated online services to comply with Codes of Practice and Directives.</li> </ul>

<sup>12</sup> Singpass stands for Singapore Personal Access, which is Singapore's national digital identity. Users can use Singpass to transact with Government agencies and private sector organisations. Currently, Singpass has more than 4.5 million users, covering 97% of Singapore Citizens and Permanent Residents aged 15 and above. Source: [www.smartnation.gov.sg](http://www.smartnation.gov.sg).

Free Trade Zone (FTZ) Act  Regulation of Imports and Exports Act (RIEA)	2023	<ul style="list-style-type: none"> <li>Enhancements to regulation and control of goods that flow through our FTZs. Amendments include the introduction of a licensing regime for FTZ operators, and prescribing data provision requirements for FTZ operators and cargo handlers on goods flowing through the FTZs. These amendments enhance Customs' oversight of the entities operating within the FTZs and ability to detect illicit activities taking place in the FTZs.</li> </ul>
	2024 <sup>13</sup>	<ul style="list-style-type: none"> <li>Amendments to allow Customs, to share trade data with STRO, to develop richer financial intelligence to tackle ML/TF/PF risks.</li> </ul>
Income Tax Act (ITA)  Goods and Services Tax Act (GSTA)	2018	<ul style="list-style-type: none"> <li>Enhancements in investigation powers for IRAS officers, such as the powers of arrest and forced entry when investigating tax crimes.</li> </ul>
	2020	<ul style="list-style-type: none"> <li>In 2020, these powers were further enhanced under the GST Amendment Act 2020, allowing IRAS officers to seize goods suspected to be used to commit an offence under the GSTA (instrumentalities of crime). Such powers enhance IRAS' ability to combat and disrupt the commission of tax offences.</li> </ul>
	2024 <sup>14</sup>	<ul style="list-style-type: none"> <li>Amendments to allow IRAS, to share tax data with STRO, to develop richer financial intelligence to tackle ML/TF/PF risks.</li> </ul>

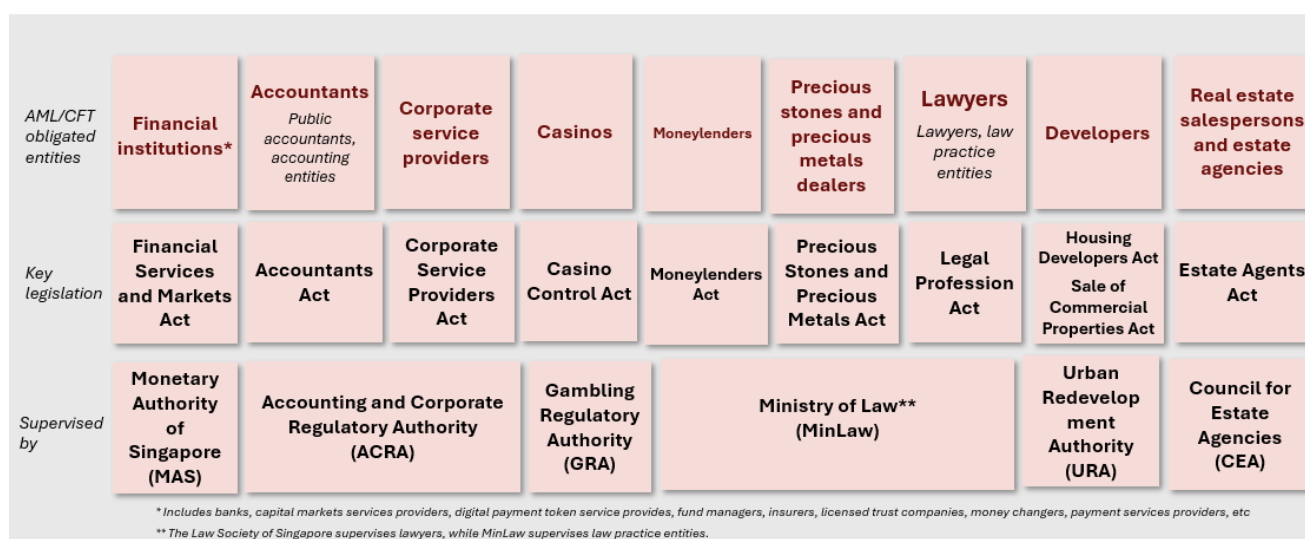
AML regulatory framework:

- 3.5 Under the AML regulatory framework, sector supervisors oversee the robust implementation of the AML/CFT requirements across the ecosystem. Under the sector specific legislation, sector supervisors have powers to supervise and take actions against their respective sectors. Please refer to diagram 2 below for a summary of the AML/CFT obligated entities, the respective sector supervisors, and key legislation for the relevant sectors. Singapore's approach relation to the implementation of these AML/CFT requirements by the sector supervisors is further elaborated in Chapter 5.
- 3.6 Sector supervisors of FIs, DNFBPs and NPOs impose AML/CFT requirements on their respective sectors, in line with FATF standards and international best practices. These include: (i) identifying and verifying customers, beneficial owners, and beneficiaries (where relevant); (ii) conducting ongoing monitoring and regular customer due diligence (CDD), with enhanced customer due diligence (ECDD) measures for higher risk customers; (iii) conducting screening to ensure compliance with AML/CFT (including for counter proliferation financing) requirements; and (iv) prompt filing of suspicious transaction reports (STRs). Details of the AML/CFT controls implemented within each of the sectors are highlighted in the ML NRA.

<sup>13</sup> Legislative changes have been passed in Parliament, and provisions will come into force and be in effect by early 2025.

<sup>14</sup> Legislative changes have been passed in Parliament, and provisions will come into force and be in effect by early 2025.

*Diagram 2 – Summary of AML/CFT obligated entities and sector supervisors:*



3.7 Sector supervisors regularly review the requirements in the AML regulatory framework to ensure their continued relevance and effectiveness in mitigating ML/TF risks. In response to the changing ML threats and risk environment, Singapore has introduced the following key changes to the AML/CFT requirements on specific sectors, set out in [Table 2](#) below.

***Table 2: Summary of key changes to AML/CFT requirements on specific sectors***

Sector	Enhancements
Digital Payment Token Services Providers (DPTSPs)	<ul style="list-style-type: none"> <li>In 2020, MAS introduced a regulatory framework for persons that provide digital payment token<sup>15</sup> services in Singapore. Such persons are required to obtain a licence under the Payment Services Act<sup>16</sup> and comply with AML/CFT requirements. Taking into account further changes to FATF Standards applicable to DPTSPs and emerging use cases, MAS introduced amendments to the Payment Services Act in 2024.</li> <li>In 2022, the Parliament passed the Financial Services and Markets Act, which provided the legislative framework to regulate digital token service providers created in Singapore that carry on a business of providing digital token service outside Singapore<sup>17</sup>. Such licensees will be subject to AML/CFT requirements.</li> </ul>
Precious Stones and Precious Metals Dealers (PSMDs)	<ul style="list-style-type: none"> <li>PSMDs were brought within the AML/CFT framework in 2019 and are supervised by MinLaw. AML/CFT requirements including CDD and ECDD obligations, record keeping, and ongoing monitoring requirements were imposed on PSMDs. In addition to the requirement to file STRs, PSMDs are also subject to a cash</li> </ul>

<sup>15</sup> Digital Payment Tokens, together with digital capital market product tokens, refer to virtual assets as defined in the FATF standards. Entities that conduct regulated activities in relation to digital capital market product tokens are already required to be licensed under the Securities and Futures Act, and to comply with AML/CFT requirements.

<sup>16</sup> Virtual assets services providers, as defined in FATF standards, include DPTSPs. The scope of DPT services that fall under the scope of the Payment Services Act are aligned with international standards set out by the FATF. Details on the scope of activities can be found in the First Schedule of the Payment Services Act.

<sup>17</sup> The regulatory framework is expected to come into force by end June 2025.

	<p>transaction reporting regime for transactions in cash or cash equivalents above S\$20,000 (designated transactions).</p> <ul style="list-style-type: none"> <li>• In November 2023, MinLaw enhanced requirements for PSMDs to conduct CDD measures for transactions involving payment received in digital payment tokens or gold above S\$20,000, to address the evolving ML/TF/PF risks inherent in the payment mode.</li> <li>• In May 2024, the requirements were further enhanced to capture under the regulatory ambit all precious products, as stipulated in the Precious Stones and Precious Metals (PSPM) Act, priced above S\$20,000 regardless of the value attributable to the PSPM, to better address the evolving risk of higher valued precious products which may otherwise not be captured under the PSPM Act. Consequently, PSMDs are now required to conduct CDD and file cash transaction reports on transactions involving a broader range of precious products.</li> </ul>
Casinos	<ul style="list-style-type: none"> <li>• Casinos are supervised by the Gambling Regulatory Authority of Singapore (GRA), and AML/CFT requirements applied to Casinos since the introduction of the Casino Control Act and Casino Control (Prevention of Money Laundering and Terrorism Financing) in 2006 and 2009 respectively<sup>18</sup>. Given the higher exposure to cash transactions and higher risk customers, casinos are required to file cash transaction reports in addition to STRs.</li> <li>• In 2024, GRA amended the Casino Control Act to tighten requirements for casino operators to conduct CDD checks for the detection and prevention of ML/TF/PF, by lowering the threshold to cover single cash transactions or deposits involving S\$4,000 or more (from thresholds for single cash transactions involving S\$10,000 or more or deposits into a deposit account involving S\$5,000 or more).<sup>19</sup></li> </ul>
Real estate developers	<ul style="list-style-type: none"> <li>• The real estate sector is supervised by the Council for Estate Agencies (CEA) (for real estate agents and salespersons) and the Urban Redevelopment Agency (URA) (for real estate developers). The AML/CFT requirements for real estate agents and salespersons are imposed under the Estate Agents (Prevention of Money Laundering and Financing of Terrorism) Regulations. The development and sale of uncompleted private properties are regulated under the Housing Developers (Control and Licensing) Act (HDCLA) and Sale of Commercial Properties Act, both administered by the Controller of Housing (COH).</li> <li>• In June 2023, AML/CFT requirements for developers were introduced under the Housing Developers (Anti-Money Laundering and Terrorism Financing) Rules 2023 and Sale of Commercial Properties (Anti-Money Laundering and Terrorism Financing) Rules 2023, to further strengthen the AML/CFT framework in the real estate sector. Under the AML/CFT</li> </ul>

<sup>18</sup> The two Singapore casinos were opened in 2010.

<sup>19</sup> Legislative changes have been passed in Parliament, and provisions will come into force and be in effect by early 2025.



	requirements, developers are required to carry out CDD checks on purchasers, including ECDD for higher-risk customers, ensure proper record keeping relating to these checks and implement adequate programmes and measures to prevent ML/TF activities.
Corporate Service Providers (CSPs)	<ul style="list-style-type: none"> <li>• The CSP sector is supervised by the Accounting and Corporate Regulatory Authority (ACRA).</li> <li>• In July 2024, the Corporate Service Providers Bill and Companies and Limited Liability Partnerships (Miscellaneous Amendments) Bill were passed to enhance the regulatory framework for CSPs and the transparency of legal persons. Key changes include expanding the scope of entities that will be regulated as CSPs and increasing the fines for AML/CFT breaches for CSPs, including individuals who own or manage such CSPs. It will also be an offence for individuals to provide nominee directorship services by way of business unless the appointments are arranged by a CSP. CSPs will also be required to be satisfied that these individuals they arrange to act as nominee directors are fit and proper.<sup>20</sup></li> </ul>

**Actions Ahead:**

- 3.8 **Singapore will continue to review our AML legal and regulatory framework** to ensure that we have the appropriate tools and levers to address changing risks, trends and developments, and ability to take proportionate and dissuasive actions against criminal and ML activities.
- 3.9 While Singapore has imposed AML/CFT requirements in line with FATF standards and international practices, sector supervisors have observed uneven implementation of the controls in some areas. **To ensure a consistent baseline in AML/CFT requirements across sectors, sector supervisors will be clarifying the requirements for real estate salespersons, estate agencies, developers, lawyers and law practice entities to conduct CDD and ongoing monitoring of their clients.** In particular, we will make clear the need to identify and take reasonable measures to verify the identities of the individuals<sup>21</sup> that their clients may be acting on behalf of. The AML/CFT requirements of the real estate sector will also be further enhanced to ensure that CDD checks are conducted on both buyers and sellers of properties.
- 3.10 The other legislative changes related International Cooperation and the implementation of sector-specific AML requirements are further described in *Chapter 4* on International Cooperation and *Chapter 5* on Prevent pillar respectively.

<sup>20</sup> Legislative changes have been passed in Parliament, and provisions will come into force and be in effect by early 2025.

<sup>21</sup> In addition to identifying and verifying the identities of the ultimate beneficial owners of businesses, which is already required.

#### 4. INTERNATIONAL COOPERATION

Policy statement:

**Singapore authorities actively cooperate with their international and regional counterparts, through formal and informal channels to achieve law enforcement and supervisory objectives for AML matters.**

- *Singapore seeks international cooperation to pursue criminals and their assets, especially in relation to cases related to significant cross-border ML threats or sectors with higher ML risks.*
- *Singapore provides timely and constructive information and assistance, in relation to requests by other countries.*

4.1 Given the transnational nature of ML activities, international cooperation is a critical aspect of Singapore's response to combat ML as well as the effectiveness of our AML framework. Singapore is keenly aware that criminals can exploit Singapore's well-connected infrastructure and payment networks to launder illicit assets. As highlighted in the ML NRA, Singapore faces significant ML risks arising from foreign ML threats (such as cyber-enabled fraud, organised crime, corruption, and TBML). In particular, authorities have observed an increase in layering of funds across multiple jurisdictions, facilitated by technological developments and use of complex structures. International cooperation is thus one of the key building blocks in Singapore's AML strategy.

Strategy in Action:

4.2 **Singapore's international cooperation efforts in AML is focused on two key dimensions – (i) participation in and contribution to the development of international standards, at various international and regional fora, and (ii) the provision of and request for assistance via formal and informal channels.**

4.3 Singapore participates actively in international fora, including the FATF and the APG. Singapore is an active member of the FATF and one of the founding members of the APG, and most recently, held the FATF Presidency from July 2022 to June 2024. Through such active involvement, Singapore collaborates with fellow AML/CFT policy makers and experts to, *inter alia*, drive and develop international AML/CFT agenda and standards. We also contribute actively to the work of other international financial crime fighting bodies, such as the Egmont Group and INTERPOL, which has facilitated cooperation, and the sharing of information and intelligence with Singapore's key partners.

4.4 Singapore has a comprehensive framework which enables Singapore to provide a wide range of assistance to other jurisdictions on the basis of reciprocity without the need for bilateral MLA treaties. The Attorney General's Chambers (AGC) is Singapore's Central Authority and works closely with LEAs and other competent authorities in making and responding to requests for MLA and extradition. AGC has put in place clear and efficient processes, as well as a specialised team to process the requests, and improve the timeliness and quality of responses provided to foreign counterparts.

4.5 Singapore also has an effective extradition regime, with a wide network of extradition partners, including declared Commonwealth jurisdictions and bilateral and multilateral treaty partners. In 2022, Singapore enhanced our extradition regime to adopt a threshold approach for determining whether

an offence is extraditable<sup>22</sup>. This replaced the positive list approach, where only offences described in a list would be extraditable. In recent years, Singapore has successfully extradited individuals for ML-related offences.

- 4.6 Apart from formal international cooperation channels, authorities proactively use other forms of informal cooperation channels such as global law enforcement, FIU and supervisory networks, to pursue cross-border joint investigations, exchange information and participate in operational platforms. For example, Singapore is a member of the Asset Recovery Interagency Network – Asia Pacific (ARIN-AP) and INTERPOL Expert Working Groups on financial crime. In January 2024, Singapore joined the Steering Group of ARIN-AP, demonstrating our commitment to leverage these networks to pursue transnational ML cases. LEAs, STRO and other competent authorities (such as MAS and IRAS) have also cooperated and exchanged information with their foreign counterparts on a bilateral basis.
- 4.7 In particular, STRO has participated in initiatives to facilitate sharing of intelligence and collaboration with international partners. For example, STRO is an active member of the Financial Intelligence Consultative Group (FICG), a regional body comprising FIUs from Southeast Asia, New Zealand, and Australia which aims to strengthen collaboration on AML/CFT by prioritising and addressing regional risks and facilitating the sharing of intelligence. STRO has also co-led a project under the FICG, along with the FIUs from Malaysia (UPWBNM) and Indonesia (PPATK), to develop a regional fraud response mechanism to enhance operational collaboration expediting information sharing on illicit funds flow to combat cyber-enabled fraud in the region.

**Actions Ahead:**

- 4.8 **Singapore will continue to leverage on international cooperation and provide timely and quality assistance to actively tackle ML activities.** Arising from our ongoing reviews, **Singapore will be implementing enhancements in our legal framework to enhance Singapore’s ability to cooperate in ML cases.** In particular, the MACMA will be amended to improve Singapore’s ability to provide and request for assistance in international criminal cooperation (including empowering Singapore LEAs to take statements from witnesses and suspects in relation to requests relating to foreign criminal investigations).

---

<sup>22</sup>The Extradition Act now provides that an offence is extraditable as long as it has a maximum punishment of two years' imprisonment or more, and is not on a list of excluded offences.

## 5. PREVENT

- 5.1 The Prevent pillar of Singapore's AML Strategy seeks to proactively prevent criminals from establishing themselves in Singapore and deter illicit funds from entering Singapore's system. As highlighted in *Chapter 3* above, AML/CFT requirements are applied through a range of entities from the financial and non-financial sectors which are at the frontlines of the fight against ML as they deal directly with persons, structures, and assets in commercial, business relationships and transactions.

***Policy statement:***

***Singapore implements robust and risk-based supervisory frameworks on FIs (including DPTSPs<sup>23</sup>), DNFBPs, and NPOs, to ensure effective implementation of the requirements under the AML regulatory framework.***

***Strategy in Action:***

- 5.2 Sector supervisors supervise the relevant sectors based on a risk-based approach, taking into account the risk profile and activities of the relevant sectors. The risk-based approach is a cornerstone of Singapore's AML framework to manage ML risks arising from the sectors' activities, monitor the entities' compliance with the sectoral AML/CFT requirements, and ensure that risk-based and proportionate measures are implemented.
- Sector supervisors conduct risk surveillance and engage their respective sectors to review and enhance the effectiveness of their risk based AML/CFT controls.
  - Adopting a robust risk-based approach allows sector supervisors to calibrate supervisory attention and intensity of supervision based on risk and allocate more resources to higher risk areas. Where weaknesses are observed, supervisors follow-up closely with entities to ensure that remedial actions are taken.
  - Where the AML/CFT obligated entities breach the requirements, sector supervisors have powers to take actions against the entities. Please refer to *Chapter 7 below* for further information on enforcement and penalty frameworks under which such actions may be taken.

Details of risk-based approach adopted by sector supervisors are elaborated in the ML NRA.

- 5.3 The implementation of the AML/CFT requirements and supervision of the sectors, are supported by regular outreach and engagement by the sector supervisors as well as STRO to share risk observations, emerging risks and typologies. Sector supervisors also provide guidance to the sectors on implementation of AML/CFT requirements. For example, MAS has published a number of guidance papers to share key supervisory observations, related to the key issues and risks noted in the financial sector, or other key risk or emerging ML/TF risk areas identified as part of MAS' risk surveillance. Other sector supervisors such as ACRA (for corporate services providers), CEA (for real estate salespersons), MinLaw (for lawyers and precious stones and precious metals dealers), have been conducting outreach sessions on ML/TF risks, latest typologies, red flags in suspicious transactions and provide guidance to help their regulated entities better understand and comply with their AML/CFT obligations. In relation to Singapore's updated ML NRA, the sector supervisors have also actively disseminated and shared information on the key findings to raise the industry's collective risk awareness.

---

<sup>23</sup> Virtual assets services providers, as defined in FATF standards, include DPTSPs.

- 5.4 Sector supervisors also regularly seek feedback from their regulated entities to ensure that our AML regulatory framework remains a robust and proportionate one, that does not unduly stifle legitimate financial and business activities.

**Actions Ahead:**

- 5.5 Given the increasing complexity and fast changing methods and typologies adopted by criminals, all sectors will have to remain vigilant. It is important for Singapore to strengthen our collective defences across the AML/CFT obligated entities through robust implementation of AML measures to prevent and deter illicit funds from being integrated into our system. **Sector supervisors will continue to enhance risk-based supervision, in conjunction with the enhancements in WOG sense-making and coordination mechanisms** (described in *Chapter 2* above).
- 5.6 To further support the AML/CFT obligated entities in the implementation of the requirements in the AML regulatory framework (described in paragraph 5.3 above), **sector supervisors will provide more guidance on AML practices to set clearer waterlines, including in relation to client risks assessments, source of fund and source of wealth checks and prompt filing of STRs.** Sector supervisors will also continue to raise awareness of risks amongst their regulated entities and collaborate with them to strengthen Singapore's collective defences against ML.
- 5.7 **Sector supervisors will work with their respective sectors to enhance the quality and accessibility of training to uplift the capabilities and support AML/CFT obligated entities to better identify ML/TF risks and take preventive actions.** For instance, CEA will be enhancing training for real estate agents and salespersons, by mandating AML/CFT courses and working with course providers to enhance the quality of training and make it more accessible

**Policy statement:**

***Singapore seeks to prevent misuse of companies for illicit purposes, and promote transparency of legal persons and legal arrangements.***

- 5.8 Legal persons (such as companies) have been observed to be misused in ML cases and a risk area of focus since 2017. Relative to legal persons, legal arrangements (such as trusts) have featured in fewer instances in in ML cases. In the cases where legal arrangements do feature in investigations, they are used as part of a complex structure, interspersed with layer(s) of companies, and often involving cross-jurisdictional elements. The opacity of such complex structures helps to conceal the ownership of illicitly obtained funds or assets. This is consistent with international typologies. Given Singapore's role as an international business hub and risk observations by agencies, the misuse of legal persons and complex structures involving legal arrangements remains a focus area in Singapore's AML framework.

**Strategy in Action:**

- 5.9 Over the years, Singapore has taken active steps to strengthen defences to prevent the misuse of legal persons and arrangements. These include:
- Through ACIP, authorities worked with the private sector (including banks, CSPs and consultants) to raise industry risk awareness and monitor the risks related to legal persons. A dedicated Legal Persons and Arrangements Workgroup (LPA WG), comprising representatives from banks and competent authorities was also set up with the aim of strengthening the

industry's understanding of risks associated with the misuse of legal persons and arrangements, identifying emerging typologies and risks involving legal persons and arrangements, best practices for mitigating such risks, and developing risk products for dissemination.

- MAS and ACIP have issued a number of guidance and best practices papers to highlight typologies and best practices for FIs to highlight legal persons risks and typologies observed, and for FIs to identify and prevent misuse of legal persons.<sup>24</sup>
- Agencies have also worked closely together to exchange information and to take enforcement actions and disruption measures in cases where legal persons or legal arrangements were misused. Please refer to *Case study 6* and *Box Story 9* in the ML NRA for examples of such cases.

#### Legal persons:

5.10 Since 2020, ACRA has managed a central beneficial ownership (BO) register for companies, which is accessible by competent authorities for the enforcement of any written law in Singapore. ACRA conducts regular inspections to ensure that companies file their BO information in a timely manner. ACRA continues to strengthen the effectiveness of the central BO register, including taking measures to ensure greater accuracy of the BO information maintained. In July 2024, Singapore amended the Companies Act and Limited Liability Partnerships Act to enhance corporate transparency of Singapore Companies and other legal persons<sup>25</sup>. Companies are also required to identify, maintain, and lodge the identities of any nominee directors and nominee shareholders, and their nominators, and to file this information with ACRA. The nominee status of any director and shareholder will be publicly accessible and the identities of their nominators will be available to competent authorities.

5.11 ACRA has been stepping up its oversight of corporate service providers. Such providers could be engaged for services related to the incorporation of companies and arranging for persons to act as nominee directors.

- ACRA subjects CSPs found to have facilitated the misuse of companies, including the setting up of shell companies, to more intensive supervisory scrutiny. ACRA has stepped up its enforcement efforts on CSPs.
- ACRA has also been actively monitoring and striking off inactive companies to address key threats and risks arising from shell companies. ACRA, in collaboration with other agencies, will step up their efforts to strike off inactive companies.
- In 2024, the CSP Act was introduced to enhance the regulatory framework for CSPs to (i) expand the regulatory scope to include Singapore-based entities that provide corporate services, (ii) increase penalties for non-compliance by CSPs of their AML/CFT/CPF obligations. This includes holding senior management of such firms liable for such breaches, under certain circumstances, and (iii) requiring that individuals can only act as a nominee director by way of business if the nominee directorship was arranged by a CSP<sup>26</sup> and that the CSP ensures the individuals they arrange to act as nominee directors are fit and proper.

---

<sup>24</sup> For example, MAS has issued papers on (a) Effective Practices to Detect and Mitigate the Risk from Misuse of Legal Persons (June 2019), (b) Effective Use of Data Analytics to Detect and Mitigate ML/TF Risks from the Misuse of Legal Persons (June 2023), (c) Strengthening AML/CFT Controls on Risks of Misuse of Legal Persons/ Arrangements and Complex Structures (August 2023). ACIP has issued industry best practices papers on (i) misuse of legal persons (May 2018), and (ii) managing ML/TF/PF risks associated with receiving referrals from corporate services providers (February 2024).

<sup>25</sup> These amendments include (i) requirements for all new companies to maintain information on their beneficial owners from the date of their incorporation, instead of the previous requirement to only do so within the first 30 days of incorporation, (ii) requirements for companies to verify and update their beneficial owners' information on an annual basis, and (iii) increase in the maximum fine for offences related to registers was increased from \$5,000 to \$25,000, to ensure that the information on the registers are kept up-to-date.

<sup>26</sup> Unless the individual is the sole proprietor of a registered CSP.

### Legal arrangements:

- 5.12 Singapore has taken various steps to prevent the misuse of legal arrangements, including by raising awareness on the ML risks posed by legal arrangements and imposing AML/CFT controls on trustees and trust companies. Sector supervisors also take proactive steps to ensure that trustees comply with the requirements; under the Trustees Act (for express trusts covered by Part 7) and requirements under MAS' AML/CFT Notice (for licensed trust companies (LTCs)).
- In particular, LTCs are subject to MAS' risk-based supervision. As noted in the ML NRA, LTCs are assessed to be a higher ML risk sector. Given the higher ML risks posed by the sector, MAS had placed greater supervisory focus the licensed trust companies over the years and stepped-up supervision arising from risks highlighted by surveillance inputs.
  - MAS also published several guidance papers that are relevant to the LTCs, including the following: (i) "Guidance to Capital Markets Intermediaries on Enhancing AML/CFT Frameworks and Controls" in January 2019; (ii) "Circular on Money Laundering and Terrorism Financing Risks in the Wealth Management Sector" in March 2023; and (iii) "Strengthening AML/CFT controls on risks of misuse of legal persons/arrangements and complex structures" in August 2023. In addition, MAS regularly engages with the LTCs through industry events and townhall sessions to clarify MAS' supervisory expectations on managing ML/TF risks relevant to the LTC sector.
  - The trust industry associations, the Singapore Trustees Association (STA) and The Society of Trust and Estate Planning, have been active in engaging trust practitioners and uplifting AML/CFT standards by setting out relevant industry guidance.
  - In line with the risk-based approach to supervision, for the private trusts managed by non-professional trustees, MinLaw has set up a whistleblowing mechanism for trustees' failure to comply with their record-keeping requirements in the Trustees Act to be reported. Any reports will then be investigated and followed-up upon by MinLaw.

### Actions Ahead:

- 5.13 To further enhance Singapore's understanding of risks related to legal persons and legal arrangements, and raise collective risk awareness, Singapore had conducted deep dive assessments on the risk posed by legal persons and legal arrangements. These risk assessments were published on 30 Oct 2024<sup>27</sup>, and the sector supervisors will continue to raise awareness and engage entities to ensure that their controls address the misuse of legal persons and legal arrangements.
- 5.14 Singapore will **undertake the following actions to enhance beneficial ownership transparency and prevent companies and legal arrangements from being abused for ML purposes.**
- a) **ACRA will continue to build on its efforts and develop the next phase of Singapore's beneficial ownership framework for legal persons.** This includes collaborating with industry partners to study whether BO information could serve as a useful additional source of information that could aid AML/CFT obligated entities (such as banks), in combatting ML, while considering the sensitive nature of the data.
  - b) **ACRA will continue to implement risk-based measures to prevent at-risk companies from being abused.** In particular, ACRA will continue screening prospective companies on a risk-based approach when they apply for incorporation. Where there are clear indicators of illegitimate activities by a prospective company and its individuals, ACRA will reject the

---

<sup>27</sup> The legal persons national risk assessment and legal arrangements national risk assessments can be found at (<https://www.mas.gov.sg/regulation/anti-money-laundering/ml-tf-pf-risk-assessments>).

incorporation where there is sufficient evidence. Further, ACRA will actively monitor and strike off inactive companies (especially those with higher risk profiles) to address key threats and risks arising from shell companies.

- c) **MinLaw will be amending the Trustees Act** to ensure compliance with the revised FATF standards, and to improve the effectiveness of the AML framework on trust beneficial ownership. The upcoming amendments will propose, amongst others, an increase in the maximum penalty for breaches of the Trustees Act and the Trustees (Transparency and Effective Control) Regulations from S\$1,000 to S\$25,000 and provision for the power of composition.



## 6. DETECT

*Policy statement:*

***Singapore performs active risk surveillance for timely detection of illicit activities, emerging threats and risks, and effective risk mitigation.***

- *The timely detection of illicit activities by government agencies and private sector facilitates the implementation of risk mitigation measures through the whole-of-society approach.*

- 6.1 As an international financial centre and business hub, a high volume of funds is processed through Singapore's ecosystem. **The ability to detect and pick up ML and illicit activities supports timely and effective mitigation, disruption, and enforcement actions.** The STR regime serves as a key tool for detection of suspicious activities. As Singapore's Financial Intelligence Unit, the STRO analyses and enriches information from STRs, and produces financial intelligence reports that are disseminated to relevant law enforcement agencies and sector supervisors. These reports provide actionable intelligence for relevant authorities to take the appropriate actions. The STR regime is complemented by the cash transaction reporting regime for specific higher risk sectors, the cross-border cash reporting regime (CBCRR)<sup>28</sup>, for the detection and investigation of ML and TF, as well as ongoing monitoring and surveillance conducted by government agencies and the private sector entities to identify anomalous activities.
- 6.2 As criminal methods and typologies are constantly changing as criminals seek to find new ways to move or disguise their illicit funds as legitimate, Singapore needs to be up to date and remain vigilant to enhance our detection capabilities and processes.

**Strategy in Action:**

- 6.3 As highlighted in *Chapter 2* on Whole-of-Society coordination and collaboration, Singapore has in place established mechanisms (such as RTIG and AC3N) for sharing information between government agencies, and with private sector entities (such as through ACIP). The enhancements related to AC3N and NAVIGATE will allow agencies to more effectively detect transactions and persons that pose ML concern to Singapore.
- 6.4 To facilitate the detection of ML risks, anomalous transactions or networks, Singapore has enhanced our framework to enable sharing of information and intelligence across agencies. In August 2024, legislative amendments were made to (i) allow more AML/CFT supervisors to have access to STRs filed by their respective sectors which will enable sector supervisors to better detect risks and suspicious transactions or networks in their respective sectors, and (ii) enable IRAS and Customs to share tax and trade data respectively with STRO, which will enable STRO to augment its analyses and provide richer intelligence to LEAs and supervisors. This will allow for better detection of various offences, including tax and trade-based ML, in line with Singapore's key ML threats.
- 6.5 At the bilateral level, agencies have also implemented structured data exchange targeted at specific risks and typologies, to facilitate timely detection/intervention against ML. This enables agencies that have complementary roles in preventing ML to share early risk indicators and undertake quicker joint

---

<sup>28</sup> Under the CBCRR, individuals are required to declare cross border movements of physical cash and bearer negotiable instruments (CBNI) that are above the FATF-prescribed threshold of S\$20,000.

targeted action on such entities. For example, ACRA and MOM have enhanced their bilateral data exchange, to address the risks related to bad actors legitimising their identity in Singapore through the use of work passes and corporate structures. The data focuses on higher risk entities which may be in breach of existing regulations, including their attributes and their compliance history. Leveraging on data analytics, both agencies will identify potential misuse of companies for fraudulent work pass applications and other violations of MOM and ACRA regulations for supervisory and enforcement follow ups.

**6.6 Government agencies have been actively leveraging on technology and data analytics to enhance detection and surveillance capabilities, to support detection of ML networks and sharpen supervisory attention on higher risk areas.** Some examples of these developments include:

- Since 2018, STRO has embarked on a digital transformation journey through the launch of its online data collection platform SONAR (STRO's Online Notices and Reporting Platform). STRs are submitted digitally via SONAR using a standardized template, allowing data to be collected via structured fields. This paved way for the use of data analytics to process, triage and disseminate STRs. In 2022, STRO enhanced analytics and data management system to equip STRO with capabilities to process large volumes of reports, automatically triage and disseminate STRs based on thematic business rules. This improved STRO's analysis as well as the quality of financial intelligence disseminated to LEAs and sector supervisors for follow-up, and also better supported Singapore's international cooperation efforts.
- LEAs have been exploring the use of technology, including data analytics, to improve the detection of ML networks. Please refer to Singapore's Law Enforcement Strategy to Combat Money Laundering<sup>29</sup> for more information on the LEA's leverage on digitalisation and technology to enhance effectiveness of investigations.
- MAS has used data analytics, coupled with information from other sources and intelligence from domestic and foreign AML/CFT counterparts, to identify concerning networks of suspicious actors and activities, and to facilitate pro-active and targeted supervisory follow ups to address risk concerns.

6.7 Beyond government agencies, private sector entities have developed and implemented tools (including the use of data analytics) and mechanisms to further strengthen sensemaking and detection across the ecosystem. Within the financial sector, MAS has been strongly encouraging FIs to develop their data analytics capabilities. The integration of technological solutions into FIs' day-to-day controls and processes enables more effective ongoing monitoring and proactive detection of anomalies in transactions or customer behaviours, enabling better detection of bad actors and prompt disruption or risk mitigation actions to be taken. MAS had intensified engagements with FIs over the past few years, to encourage industry to put necessary IT and data infrastructure in place to support the development and implementation of technological solutions to enhance their risk detection and prevention capabilities.

6.8 ACIP has also set up a Data Analytics Workgroup for banks to discuss and share insights on the adoption and implementation of analytics for AML/CFT purposes. ACIP had issued two papers<sup>30</sup> to share more broadly with the private sector on data analytics methods adopted. Over the past few years, MAS has observed an increased adoption of data analytics techniques for financial crime purposes amongst the FIs, especially the banks. This has also enabled them to file STRs more effectively and efficiently. As FIs continue to improve the quality and timeliness of filing STRs, our LEAs have been provided with better

---

<sup>29</sup> Please refer to (<https://go.gov.sg/leaamlstrategy2024>) for Singapore's Law Enforcement Strategy to Combat Money Laundering

<sup>30</sup> Please refer to ([Industry Perspectives – Adopting Data Analytics Methods For AML/CF \(Nov 2018\)](#)) and ([Industry Perspectives on Best Practices – Leveraging on DA and ML Methods for AMLCFT \(Mar 2024\)](#)).

leads which they can act upon more quickly. MAS<sup>31</sup> has sought to more quickly share pertinent risk information<sup>32</sup> with the broader industry via advisories, improving our financial system's defences.

- 6.9 To further strengthen analysis of transactions and detection of anomalous activities in the financial system, Singapore launched COSMIC in April 2024, for participant banks to share risk information with each other if the customer's profile or behaviour displays certain or combinations of indicators of suspicion or "red flags" indicative of potential illicit activities. This will enable the banks to conduct sharper analysis of customer activities, and close information gaps that criminals may exploit to conduct illicit transactions through a network of entities with accounts in different FIs, and to enhance detection of illicit networks and actors across the sector. For a start, information sharing on COSMIC will be among six major commercial banks in Singapore, to allow for agile implementation to achieve platform stability and focus on key risks arising from (a) misuse of legal persons, (b) misuse of trade finance for illicit purposes, and (c) proliferation financing. Information from COSMIC, including material networks of suspicious actors, is being integrated into MAS' overall surveillance framework to target higher risk activities in the financial system for supervisory intervention as well as WOG mitigation measures.
- 6.10 The insights observed from the use of data analytics and technological tools used by government agencies and the private sector entities in turn feed into the coordination mechanism structures described above in Chapter 2 (e.g. via the RTIG and ACIP mechanisms) and where appropriate, enforcement actions to be taken.

#### **Actions Ahead:**

- 6.11 As highlighted in *Chapter 2* above, Singapore will be enhancing our mechanisms and processes for sharing of information and sense-making within and between the government agencies. **The establishment of the NAVIGATE platform and AML Sense-making workgroup, will strengthen Singapore's ability to detect ML activities – please refer to *paragraph 2.15* above for more information.** Complementing the enhancements in WOG mechanisms, the SPF will lead training across agencies, to level-up agencies' sensemaking capabilities, in particular, to effectively harness technology and data analytics.
- 6.12 **Authorities will continue to review the effectiveness of the surveillance tools and information sharing mechanisms (including COSMIC).** As such information-sharing represents a new paradigm in the fight against financial crime, MAS plans to expand COSMIC in phases, with the initial phase to last for two years. After the initial phase of two years, MAS will evaluate whether to expand COSMIC's coverage to more focus areas and FIs. In line with recommendations arising from the IMC review, Singapore will continue to explore ways to deepen channels for data sharing among and with private sector entities.

---

<sup>31</sup> As relevant and sometimes in conjunction with other agencies such as CAD.

<sup>32</sup> On emerging typologies and bad actors

## 7. ENFORCE

- 7.1 Singapore takes a firm and clear stance against ML. This is reflected in the strong legal framework which empowers law enforcement authorities to take firm enforcement actions against entities and individuals involved in ML activities. The key LEAs in Singapore which are directly involved in investigating ML are the SPF (including CAD), CNB, and CPIB<sup>33</sup>.
- 7.2 In addition to the powers of LEAs, sector supervisors have a wide range of tools available, to take action against breaches of AML/CFT requirements within their respective sectors.

*Policy statement:*

***Singapore adopts a multi-pronged approach in identifying ML activity, rigorously investigates leads to uncover possible ML offences, and takes proportionate and dissuasive actions against ML activity, including that relating to foreign predicate offences.***

**Strategy in Action:**

- 7.3 As elaborated in the Detect pillar, detection of illicit activities supports authorities in taking timely and effective enforcement actions. Information and intelligence from various sources (including STRs, Cash Transaction Reports (CTRs), Cash Movement Reports (CMRs), and other information) are analysed by STRO to support the detection and investigation of ML, terrorism financing and associated predicate offences. ML enforcement agencies would investigate where there is reason to suspect ML offences. To this end, clear operating procedures are in place to provide guidance on the identification of ML and referral of investigations by agencies to LEAs involved in investigating ML. In line with Singapore's key ML threats, LEAs prioritise the investigation of complex, transnational ML cases, including ML perpetrated by professional and syndicated money launderers.
- 7.4 Singapore has also been regularly reviewing and enhancing the legal framework under the CDSA (described in *Chapter 3* above), to equip LEAs with appropriate powers and tools to take actions against money launderers, in view of changing risk landscape. In addition, to address risks related to cross border movements of cash, Singapore has enhanced our CBCRR, by mandating the electronic submission of CBCRR declarations for travellers entering and leaving Singapore and increasing the composition fines imposed for CBCRR offences by threefold, which aligns our measures with international comparisons.
- 7.5 In addition to imposing dissuasive sanctions in the form of fines and custodial sentences, asset recovery has been and will continue to be a key tenet of Singapore's approach against ML and other crimes. Asset forfeiture serves as a crucial and powerful deterrent, as it deprives criminals of their illicit gains and hits the heart of crime. To this end, Singapore has implemented a comprehensive framework for seizure and confiscation of criminal proceeds. Singapore has also published a National Asset Recovery Strategy to make clear Singapore's asset recovery processes and roles of various stakeholders. Further details of Singapore's asset recovery framework and processes are set out in the National Asset Recovery Strategy launched in June 2024.<sup>34</sup>

---

<sup>33</sup> SPF investigates money laundering in relation to predicate offences under its own charge such as fraud and illegal gambling, and case referrals from other agencies investigating serious offences under the CDSA. CNB has an embedded Financial Investigation Team that investigates money laundering related to drug offences, whereas CPIB investigation officers across all CPIB investigation units are trained to investigate money laundering arising from bribery-related predicate offences.

<sup>34</sup> Please refer to (<https://file.go.gov.sg/nationalassetrecoverystrategy2024.pdf>) for the National Asset Recovery Strategy.

- 7.6 To reflect Singapore’s firm stance against ML activities, AML/CFT supervisors in Singapore have implemented robust penalty frameworks for AML/CFT obligated entities which are at the frontlines dealing with transactions and customers, and taken actions where breaches are identified. The penalties are reviewed periodically to ensure that they remain dissuasive and deterrent. For instance, the CSP Act has been amended in 2024 to increase penalties for CSPs and their senior management who breach their AML obligations. CSPs that are non-compliant with their obligations to detect and prevent ML will now face a fine of up to S\$100,000 – a four-fold increase from the previous financial penalty of S\$25,000. The senior management of CSPs can also be held liable for such breaches under certain circumstances<sup>35</sup>, and face a fine of up to S\$100,000.

**Actions Ahead:**

- 7.7 As highlighted in *Chapter 2* on whole-of-society coordination and collaboration, arising from the IMC’s recommendations, Singapore will enhance operational coordination and collaboration across agencies on complex ML cases through AC3N, which would help triage and prioritise enforcement outcomes for specific complex cases. Through AC3N, LEAs and sector supervisors will review and coordinate actions with a whole-of-system lens and bolster Singapore’s collective AML defences.
- 7.8 Singapore will continue to take a firm stance against persons who abuse our system for ML. **Singapore will prioritise law enforcement outcomes in key risk areas and transnational complex ML cases**, as noted in the ML NRA. Please refer to Singapore’s Law Enforcement Strategy to Combat Money Laundering, which elaborates on the approach and focus areas of key LEAs in combatting ML.
- 7.9 LEAs will also leverage on asset recovery as a key tool to deprive criminals for the illicit gains and remove the financial incentive for laundering their monies through Singapore. As articulated in Singapore’s National Asset Recovery Strategy, **asset recovery has and will continue to be a key priority of Singapore’s AML framework**.
- 7.10 Arising from the IMC recommendations and in line with ongoing efforts to review Singapore’s AML framework, **CEA, URA and MinLaw will clarify or enhance the AML penalty frameworks for their respective sectors** (namely, real estate salespersons and estate agencies, property developers, lawyers and law practice entities), to ensure that the sanctions are dissuasive and proportionate, and meted out are in line with the severity of the breaches and culpability of persons involved.

---

<sup>35</sup> For example, if they knew or ought reasonably to have known that the offence would be or is being committed but failed to take all reasonable steps to prevent or stop the commission of that offence.

## **8. CONCLUSION**

- 8.1 Singapore remains firmly committed to combatting ML. This National AML Strategy will guide Singapore's actions ahead, as we seek to maintain an effective AML framework so as to protect our hard-earned reputation as a trusted and well-governed international financial centre and business hub. We will continue to monitor and identify emerging and changing risks and take a risk-based and proportionate approach to implement measures that are targeted against the abuse of our system while remaining welcoming to legitimate businesses and investments in Singapore.

## TABLE OF ACRONYMS

AC3N	AML Case Coordination and Collaboration Network
ACIP	AML/CFT Industry Partnership
ACPN	Anti-Corruption Partnership Network
ACRA	Accounting and Corporate Regulatory Authority
AGC	Attorney General's Chambers
AML	Anti-Money Laundering
APG	Asia-Pacific Group on Money Laundering
APPACT	Alliance of Public Private Cybercrime Stakeholders
ARIN-AP	Asset Recovery Inter-Agency Network Asia Pacific
BO	Beneficial Owner
CAD	Commercial Affairs Department
CBCRR	Cross-Border Cash Reporting Regime
CBNI	Cash and bearer negotiable instruments
CDD	Customer Due Diligence
CDSA	Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992
CEA	Council for Estate Agencies
CFT	Countering the Financing of Terrorism
CMA	Computer Misuse Act 1993
CMR	Cash Movement Report
CNB	Central Narcotics Bureau
COH	Controller of Housing
COSMIC	Collaborative Sharing of Money Laundering/Terrorism Financing (ML/TF) Information & Cases
CPF	Counter Proliferation Financing
CPIB	Corrupt Practices Investigation Bureau
CSP	Corporate Service Provider
CSP Act	Corporate Service Providers Act 2024
CTR	Cash Transaction Report
DA	Data analytics
DNFBP	Designated Non-Financial Businesses and Professions
DPTSP	Digital Payment Token Service Provider
ECDD	Enhanced Customer Due Diligence
FATF	Financial Action Task Force
FI	Financial Institution
FIU	Financial Intelligence Unit
FTZ	Free Trade Zone
FTZA	Free Trade Zones Act 1966
GRA	Gambling Regulatory Authority
GSTA	Goods and Services Tax Act 1993
HDCLA	Housing Developers (Control and Licensing) Act 1965
IAC	AML/CFT Inter-agency Committee
IMC	Inter-Ministerial Committee
IRAS	Inland Revenue Authority of Singapore
ISTRA	Inter-Agency Suspicious Transaction Report Analytics Taskforce
ITA	Income Tax Act 1947
LEA	Law Enforcement Agency
LTC	Licensed Trust Company

MACMA	Mutual Assistance in Criminal Matters Act 2000
MAS	Monetary Authority of Singapore
MHA	Ministry of Home Affairs
MinLaw	Ministry of Law
ML	Money Laundering
MLA	Mutual Legal Assistance
ML NRA	Money Laundering National Risk Assessment
MOF	Ministry of Finance
MOM	Ministry of Manpower
NAVIGATE	National AML Verification Interface for Government Agencies Threat Evaluation
NPO	Non-profit Organisation
OCHA	Online Criminal Harms Act 2023
PF	Proliferation Financing
PSMD	Precious Stones and Precious Metals Dealer
PSPM	Precious Stones and Precious Metals
PSPM Act	Precious Stones and Precious Metals (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing) Act 2019
RFA	Registered Filing Agent
RIEA	Regulation of Imports and Exports Act 1995
RTIG	Risk and Typologies Inter-Agency Group
RQI	Registered Qualified Individual
Singpass	Singapore Personal Access
SC	AML/CFT Steering Committee
SONAR	STRO's Online Notices and Reporting Platform
SPF	Singapore Police Force
STA	Singapore Trustees Association
STR	Suspicious Transactions Report
STRO	Suspicious Transactions Reporting Office
TBML	Trade-Based Money Laundering
TF	Terrorism Financing
URA	Urban Redevelopment Authority
VASP	Virtual Asset Service Provider
WOG	Whole-of-Government