2024 • SINGAPORE

TERRORISM FINANCING NATIONAL RISK ASSESSMENT

Singapore's key terrorism financing (TF) risk areas

MINISTRY OF HOME AFFAIRS

MOF
MINISTRY OF FINANCE
SINGAPORE

MAS
Monetary Authority of Singapore

INTRODUCTION

OBJECTIVES

1. **The 2024 Terrorism Financing (TF) National Risk Assessment (NRA) is a product of Singapore's continuous review of our TF risks and updates our earlier TF NRA published in 2020.** The refreshed TF NRA reflects our collective experience and observations since our last review, with particular consideration of the rapid growth of the digital economy in Asia spurred by the COVID-19 pandemic. This NRA presents the latest overview of Singapore's TF risk environment, captures key terrorism and TF developments at the local, regional, and global levels - including potential spillovers from the ongoing Israel-Hamas conflict - and identifies the key corresponding risk areas within Singapore's National Countering the Financing of Terrorism (CFT) system. The refreshed TF NRA informs law enforcement agencies (LEAs), financial intelligence units (FIUs), regulators/supervisors, policy makers, and the private sector on Singapore's latest and emerging TF threats, risks, and vulnerabilities. This will enable them to adopt a targeted and risk-focused approach when updating and implementing CFT strategies and risk mitigation measures.

APPROACH

2. **In Singapore, the Risks and Typologies Inter-Agency Group (RTIG), led by the Ministry of Home Affairs (MHA) and the Monetary Authority of Singapore (MAS), oversees the identification, assessment, and mitigation of TF risks at the whole-of-government (WOG) level.** The RTIG comprises all relevant supervisory, regulatory, law enforcement, policy agencies, as well as Singapore's FIU, the Suspicious Transaction Reporting Office (STRO). The work of the RTIG is overseen by the Anti-Money Laundering (AML)/CFT Steering Committee.[1] During the process of refreshing the TF NRA, the supervisory, regulatory, policy, and operational agencies reviewed the significance of TF threats identified in the 2020 TF NRA and identified new TF typologies of concern that have emerged in subsequent years.

3. **Singapore has proactively reached out to foreign governments, international bodies, and industry players to complement our understanding of Singapore's TF risks and typologies of concern.** In March 2024, Singapore conducted a consultation exercise via the secure Egmont Group network to survey our TF risk assessment with members of the Financial Action Taskforce (FATF) and other high-risk jurisdictions with a potential TF nexus to Singapore. This initiative strengthened and deepened Singapore's understanding of our

[1] The AML/CFT Steering Committee is co-chaired by the Permanent Secretaries of the Ministry of Home Affairs and the Ministry of Finance, and the Managing Director of MAS.

latest TF risks from the perspectives of external jurisdictions and the impact of global and regional terrorism and TF developments on Singapore's TF threats and vulnerabilities.

4. Singapore also referred to key TF-related studies developed by the FATF, including those from Singapore's FATF Presidency from July 2022 to June 2024, to enhance our understanding of the latest TF typologies and their manifestation in the Singapore context. This includes the FATF report published in October 2023 on TF crowdfunding. Additionally, Singapore conducted industry consultation sessions with key Financial Institutions (FIs) via the AML/CFT Industry Partnership (ACIP),[2] with the most recent session in May 2024. These sessions included briefings on the latest TF typologies and threats to Singapore, and emerging TF trends and typologies observed by LEAs. The consultation also provided an opportunity for the industry to provide feedback on emerging TF typologies that they had observed and discussed potential mitigating measures to address these risks.

[2] The AML/CFT Industry Partnership is co-chaired by MAS and the Commercial Affairs Department of the Singapore Police Force. Established in 2017, this public-private partnership brings together the financial sector, LEAs, and other government entities to collaboratively identify, assess, and mitigate key TF risks facing Singapore. It allows LEAs to leverage the insights of FIs on TF risks, as well as the financial background and financing methods employed by local radicalised individuals. For more details, please refer to https://www.mas.gov.sg/regulation/anti-money-laundering/amlcft-industry-partnership-acip

METHODOLOGY

5. **The methodology applied in the refreshed 2024 TF NRA is based on guidance published by the FATF**[3] and considers a range of qualitative and quantitative data. TF risks are a function of threats, vulnerabilities, and consequences. The TF NRA was refreshed through the following process:

Examination of the Overall Terrorism/TF Threat

Singapore thoroughly examined and identified the terrorist groups that posed the most significant terrorism threat to Singapore and the region, as well as the primary ways these groups were financed. Singapore considered key international developments such as the ongoing Israel-Hamas conflict and tensions in the Middle East, along with their potential terrorism and TF spillovers to the region and Singapore. The TF threats to different sectors of the Singapore economy were thoroughly analysed, taking into account emerging international typologies, and substantiated by information from TF investigations and financial intelligence, including Suspicious Transaction Reports (STRs), Requests for Assistance (RFAs), and Mutual Legal Assistance (MLA) requests. These findings were further validated through insights gleaned from participation in FATF, regional CFT projects, and surveillance of regional and international TF typologies of concern.

Analysis of Sectors' TF Vulnerabilities

Regulators and supervisors reviewed the vulnerability assessments of their respective sectors, considering their sector's key TF threats and how certain products, services, and activities might be exploited for TF purposes, as well as industry feedback. The latest TF threats in the respective sectors were compared with those identified in the 2020 TF NRA.

[3] The FATF's TF Risk Assessment Guidance Project, published on 5 July 2019.

Evaluation of TF Risks of Various Sectors

Similar to the 2020 TF NRA, Singapore evaluated the risk of terrorists and terrorist groups exploiting a particular sector for TF as a function of the sector's TF threats and vulnerabilities (after implementing mitigating measures) and where the consequences were deemed severe. The following matrix was used to derive the 2024 TF risk ratings of the various sectors: H (High), MH (Medium High), ML (Medium Low), or L (Low).

Risk Ratings		Vulnerabilities			
		L	ML	MH	H
Threats	H	MH	MH	H	H
	MH	MH	MH	MH	H
	ML	ML	ML	MH	MH
	L	L	L	ML	ML

KEY TERRORISM FINANCING THREATS

6. **Singapore's key TF threats stem from: (i) terrorist groups such as the Islamic State of Iraq and Syria (ISIS), Al-Qaeda (AQ), and Jemaah Islamiyah (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.** Far-right extremism is also a growing security concern in many countries worldwide. While it has not currently gained significant traction in Southeast Asia, its anti-Islam and anti-immigration rhetoric may resonate with some individuals here. In assessing the TF threats arising from these areas, key TF activities such as the raising, moving, storing, and using of financial resources for terrorism purposes have been considered in the refreshed TF NRA.

TERRORIST GROUPS

ISLAMIC STATE OF IRAQ AND SYRIA (ISIS)

7. **PERSISTENT THREAT OF ISLAMIC TERRORIST GROUPS: ISIS'S INFLUENCE BEYOND CONFLICT ZONES |** Although ISIS has lost several senior leaders since 2022, a new generation of leaders has emerged who are undeterred by the possibility of being killed during the attacks. This new leadership intends to expand ISIS's reach and carry out attacks in non-conflict zones. In April 2023, reports indicated that ISIS might be positioning itself for a resurgence in Syria, where international counter-terrorism efforts may be compromised due to strained relations between major powers over the war in Ukraine.[4]

8. **ISIS'S CONTINUED PRESENCE IN SOUTHEAST ASIA AND THEIR UTILISATION OF SOCIAL MEDIA |** Within Southeast Asia, ISIS remains the primary terrorism threat. The central message of defending oppressed Muslims propagated by ISIS continues to gain traction on social media platforms in the region. For instance, supporters widely shared translations of ISIS spokesman Abu Umar al-Muhajir's September 2022 speech, urging global supporters, including those in Southeast Asia, to continue fighting for ISIS's cause. Singapore remains a prized target for ISIS and is frequently featured in their propaganda. For example, in June 2023, Southeast Asian ISIS supporters on social media called for retaliatory attacks following the death of Islamic State East Asia Province leader Abu Zacharia. They also circulated a poster depicting several government leaders in Southeast Asia, including Singapore's then-President Halimah Yacob, as targets.

9. **RENEWED EASE OF TRAVEL FOR FOREIGN TERRORIST FIGHTERS** | There has not been a significant exodus of Southeast Asian foreign terrorist fighters (FTFs) from conflict zones to their home countries since 2020. This was partly due to repatriation challenges and COVID-19 travel restrictions from 2020 to 2022. However, the easing of pandemic-era travel restrictions has made it easier for pro-ISIS elements to return to their home countries and networks, potentially facilitating attacks in their home countries and in the region. Those who remain in overseas conflict zones also pose a security concern due to their ability to remotely direct terror activities in Southeast Asia.

10. **TF TYPOLOGIES |** Following its retreat in 2018, ISIS is believed to have smuggled approximately US$400 million out of Iraq and Syria using established criminal and *hawala*[5] networks, as well as experienced financial facilitators. Its core structure continues to provide resources to its affiliates, including those in Southeast Asia, albeit at a reduced level. Known means of transfers involve cash couriers, money remittances, bank transfers, virtual currencies, and online transactions.

11. Funds raised, moved, and transferred to support terror activities by terrorists and/or individuals within the region could originate from legitimate and illegitimate sources. Legitimate sources may include salaries and charities, which are sometimes abused by terrorist actors. Illegitimate sources may involve criminal proceeds.

[4] MHA's Singapore Terrorism Threat Assessment Report 2023, published on 24 July 2023 (https://www.mha.gov.sg/docs/default-source/default-document-library/singapore-terrorism-threat-assessment-report-2023.pdf))

[5] Hawala is an informal and anonymous value-transfer system that relies on a network of brokers to send money to various locations instantaneously and frequently without a paper trail. An individual transfers money from one location to another by depositing money with a local agent, who then informs their counterpart abroad to pay the recipient; the two agents settle their accounts later. As Hawala operates outside traditional banking systems, it lacks regulation and oversight, making it easily exploitable by terrorism/TF actors.

AL-QAEDA AND JEMAAH ISLAMIYAH ELEMENTS

12. There are indications that **Al-Qaeda and Jemaah Islamiyah have been rebuilding through their "long game" strategy** and may resume planning large-scale attacks, necessitating the movement and raising of funds.

13. **AL-QAEDA (AQ) |** Far from being a spent force, AQ has adopted a "long-game strategy" of building local alliances and socialising local communities through its regional affiliates. In January 2019, the United Nations (UN) reported that AQ remains resilient and active, and is, in some regions such as Afghanistan, stronger than ISIS.

14. **JEMAAH ISLAMIYAH (JI) |** The AQ-aligned JI poses a long-term security concern to the region. Since 2019, Indonesian authorities have undertaken rounds of pre-emptive strikes against the JI and arrested key JI leaders. While JI has been lying low, it continues to quietly sow ground support for the establishment of an Islamic caliphate in the region.

15. **TF TYPOLOGIES |** Despite the ongoing crackdown, JI is expected to persist with its outreach activities through its network of schools, mosques, and non-profit organisations (NPOs) to raise funds, recruit new members, and foster ground support for its long-term objective of establishing an Islamic state in the Southeast Asian region.

RADICALISED INDIVIDUALS

16. **DETECTION OF RADICALISED INDIVIDUALS IN SINGAPORE | Singapore continues to detect radicalised individuals from both the local and foreign worker populations.** In recent years, the majority of self-radicalised individuals detected in Singapore have been supporters of ISIS. Among them, Singapore has convicted 13 individuals for TF offences from 2016 to-date.[6] All of their TF activities related to the raising and/or moving of funds out of Singapore using fairly unsophisticated channels and methods (e.g., through remittance agents) to support terrorist activities abroad.

17. **RADICALISED SINGAPOREANS |** Since the rise of ISIS, there has been a corresponding increase in the number of self-radicalised Singaporeans detected. The primary driver of this threat continues to be online radicalisation. As of June 2023, 37 self-radicalised Singaporeans have been dealt with under the Internal Security Act (ISA) and other terrorism-related legislation.[7] For instance, Singaporean A, who was arrested by the Malaysian Special Branch (MSB) and deported to Singapore, was detained under the Terrorism (Suppression of Financing) Act 2002 (TSOFA)[8] for his support of ISIS in September 2021.

Box Story 1 – Singaporean Convicted of TF

Singaporean A was convicted and sentenced to 3 years and 10 months' imprisonment under the TSOFA in September 2021. The Singaporean, a businessman based in Malaysia, was arrested by the MSB in 2019 and handed over to Singapore's Internal Security Department (ISD) for investigation into his terrorism-related activities. Singaporean A was a close associate of Malaysian B, a Syria-based ISIS militant, and had, while in Malaysia, provided money to Malaysian B totalling RM1,500 (approximately S$576) and US$351.75 (approximately S$450) in 2013 and 2014, respectively. Some of this money was remitted to Malaysian B's contacts in a third country via a licensed remittance company in Singapore. Singaporean A was aware of Malaysian B's intention to travel to Syria to become an FTF and Malaysian B's membership in an ISIS-affiliated group called Jabhat al-Nusra.

18. Singapore continues to detect a small number of self-radicalised Singaporeans intending to travel abroad and fight alongside terrorist organisations. For instance, Singaporean C detained under the ISA, had intended to travel to Gaza to join Hamas's military wing and carry out knife attacks against Jews in Singapore in 2021.

19. **RADICALISED FOREIGN WORKERS |** Singapore continues to detect radicalisation among foreigners working and living in Singapore. The significant foreign worker community's presence could also enable terrorist groups to use Singapore as a base for terrorism fundraising among their own nationals here, or as a conduit for TF purposes.

Box Story 2 – Bangladeshi National Convicted of TF

In February 2022, a Bangladeshi construction worker in Singapore was convicted and sentenced to two years and eight months' imprisonment under the TSOFA. He used his debit card to send money totalling S$891 on 15 occasions in support of overseas online fundraising campaigns for Syria-based organisations. He was

[6] As of May 2024.
[7] The ISA allows the Government to detain or impose Restriction Orders on individuals who pose a threat to Singapore's national security, which includes involvement in terrorism-related conduct.
[8] Singapore's main legislation to counter terrorism financing.

aware that these funds could be used to benefit Hayat Tahir Al-Sham (HTS), a United Nations Security Council designated terrorist entity , which was fighting to establish an Islamic caliphate in Syria.

20. **TF TYPOLOGIES |** The main TF modalities observed from known cases include self-funding from individuals' salaries or savings and transfers via licensed money remittances. The amounts involved in these TF cases are generally small. Our investigations also revealed that none of the cases were linked to organised crime, as Singapore remains inhospitable for organised crime groups.[9]

21. **Singapore's relative affluence means that locals and migrant workers in Singapore potentially possess greater resources and have access to more channels to raise or move funds for terrorism-related activities.** For instance, self-radicalised individuals who have been convicted for TF offences since the publication of the 2020 TF NRA include a local businessman and a foreign worker who possessed sufficient discretionary funds to contribute toward terrorist activities.

22. The Singapore authorities conducted a study to better understand the risks posed by self-radicalised individuals and the financial behaviour of terrorist actors.

Box Story 3 – Key Findings of the Financial Study of Radicalised Individuals in Singapore

The financial study on radicalised Singaporeans was conducted in two phases. Government agencies formulated preliminary insights in the first phase and corroborated with financial institutions in the second phase.

The first phase involved analysing the radicalised individuals' financial background and their methods of financing, including raising, moving, and using funds. It was observed that a vast majority of the radicalised individuals did not engage in or planned to engage in TF activities. This could be due to the following reasons:

(i) Many individuals were interrupted early in their radical trajectories before developing concrete plans to secure funding.

(ii) Some individuals were likely consumed by practical challenges, such as bypassing border security checks, especially after Türkiye clamped down on the flow of foreign terrorist fighters, or in linking up with ISIS in Syria; and/or

(iii) The actual cost of travelling to conflict zones was not prohibitively high and did not require fundraising.

Among those who tried or planned to raise funds, **self-funding from legitimate or existing income sources** was the most used method. Those who gave money for terrorism purposes or to terrorism-linked individuals, predominantly used licensed remittance agents. The sums involved were small and did not involve complex or suspicious transaction patterns. To date, there have been no instances of individuals leveraging newer forms of cross-border fast payment systems (e.g., Singapore-Thailand PayNow-PromptPay, Singapore-Malaysia NETS-DuitNow QR code payment linkages) for TF purposes.

[9] Singapore remains inhospitable for organised crime groups. We frequently mount operations to disrupt organised crime threats. Our capabilities are further enhanced through legislative tools such as the Organised Crime Act, and the establishment of dedicated units to combat organised crimes, such as the Organised Crime Branch in the Criminal Investigation Department of the Singapore Police Force.

In the second phase of the study, authorities leveraged the CFT Operational Group set up under ACIP. Involving FIs, including remittance agents, allowed Singapore authorities to deepen our understanding of the financial behaviour of terrorist actors by identifying commonalities and patterns in their financial transactions.

SUMMARY OF TF THREAT

23. **Similar to the 2020 TF NRA, our latest assessment concludes that the TF threat of raising and moving funds for terrorists and terrorist activities overseas remains pertinent in Singapore's context.** Self-radicalised individuals continue to pose the most salient TF threat to Singapore. However, we do not discount the possibility of a terrorist attack occurring in Singapore. We remain cognisant of the global terrorism and TF threats posed by terrorist groups such as ISIS, AQ, and JI, especially in light of the continued ideological influence these groups have over radicalised individuals in Singapore, as well as international and regional conflicts that may fuel new motivations for terror. In the next segment, we will discuss how these terrorism threat actors may seek to exploit various sectors in Singapore to raise and move funds for terrorists and terrorist activities overseas.

24. **Law enforcement agencies, STRO, and supervisory authorities in Singapore remain vigilant against emerging and potential TF typologies.** For instance, with the proliferation of digital payment services in Asia following the COVID-19 pandemic (e.g., cross-border fast payment systems), there is an increased risk that terrorists, terrorist organisations, and their supporters may exploit the convenience of these new online transaction channels or virtual currencies/assets to further their terrorist causes. To address this threat, STRO regularly shares relevant TF red flag indicators with the private sector to enhance their awareness and detection of suspicious TF activities.

25. A country's vulnerability to TF is closely tied to its TF threats and contextual factors. In the case of Singapore, **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**.

TERRORISM FINANCING VULNERABILITIES AND RISKS

AREAS AT RISK OF BEING EXPLOITED FOR TF

26. This section elaborates on the key sectors in Singapore that terrorists, terrorist organisations, and sympathisers may target to raise, move, or use funds for terrorist purposes. Sectors not delineated in this report are assessed to present a low risk for TF. This assessment is based on their limited exposure to TF threats and vulnerabilities while considering established TF typologies and existing AML/CFT controls.

UPDATES SINCE 2020

27. **The key TF risk areas identified in 2024 closely resemble those identified in 2020, with money remittances and banks identified as sectors posing the highest TF risks**. Moreover, emerging TF risks have been identified in **new cross-border fast payment systems and online fundraising**, considering Singapore's high internet penetration, and prevalence of online banking, and the global surge in digital economy driven by the COVID-19 pandemic. While most TF activities still occur through fiat and traditional sectors, there is a growing risk of virtual assets being utilised by international terrorist groups.[10] As a result, TF risks associated with **Digital Payment Token (DPT) service providers have been elevated from Medium-Low to Medium-High risk, necessitating increased industry vigilance against this evolving threat.**

Sectors at Risk of Being Exploited for TF	2020 TF NRA	2024 TF NRA
Money remittances, including: - Unlicensed money remittances - Cross-border online payments **(emerging area since 2020)**	**High**	**High**
Banks, including: - New cross-border fast payment systems **(emerging area since 2020)**	**Medium-High**	**Medium-High**
DPT service providers **(increased risk since 2020)**	**Medium-Low**	**Medium-High**
Non-profit organisations, including: - Online fundraising **(emerging area since 2020)**	**Medium-Low**	**Medium-Low**
Cross-border cash movement	**Medium-Low**	**Medium-Low**
Precious stones and precious metal dealers	**Medium-Low**	**Medium-Low**
Other AML/CFT regulated sectors not featured in the report (e.g., Real estate)	**Low**	**Low**

Table 1: Comparison of TF Risk Assessments in 2020 and 2024

[10] See FATF's Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers, June 2023.

MONEY REMITTANCES

HIGH RISK

KEY EXPOSURES TO TF THREAT AREAS

28. Terrorist financiers are known to utilise money remittance (cross-border money transfer service provider) channels for transferring funds across borders. International typologies further suggest the use of remittance channels, including *hawalas*, to facilitate the flow of funds for TF.

UPDATES SINCE 2020

29. **TF threats have manifested within this sector in Singapore.** There has been **one TF conviction** since 2020 involving the movement of funds through licensed money remittance agents by a local sympathiser to support terrorism-related activities abroad.

30. Based on investigations and cases prosecuted by law enforcement agencies, **there have been no instances of unlicensed money remittances being exploited for TF activities in Singapore thus far**. Nevertheless, the Singapore authorities remain vigilant to such risks, considering overseas reports of TF abuse in this sector.

KEY VULNERABILITIES

31. **DEMOGRAPHICS OF USERS AND TRANSACTIONS WITH COUNTRIES/ECONOMIES MORE EXPOSED TO TERRORISM/TF RISKS |** Money remittances often provide cost-effective and efficient remittance services compared to banks, making them popular among Singapore's sizeable foreign migrant worker population. Some of the countries in the region that local remittance agents frequently transact with are known to have higher exposure to terrorism/TF risks.

32. The demographic profile of users and the established transaction corridors involving countries in the region more exposed to terrorism/TF risks heighten Singapore's vulnerability. There is an increased risk of foreign terrorism-related actors exploiting Singapore as a base to raise funds among both locals and foreign populations.

UPDATES SINCE 2020

33. The Singapore authorities have observed that donations to foreign online fundraising campaigns typically traverse traditional payment channels, including payment service providers, bank transfers, or digital banking platforms such as credit and debit cards. MAS and MHA have intensified efforts to raise awareness among the payment and banking sectors to the TF risks associated with donations to foreign online fundraising campaigns. These efforts involve engagement sessions where red flag indicators and suspicious entities are

shared, sensitising the sectors to the potential risk of TF abuse through Singapore's banking and payment systems by foreign online fundraising platforms.

34. **DISPARITIES IN TF DETECTION CAPABILITIES ACROSS THE SECTOR** | Through MAS's robust supervision of licensed remittance agents in Singapore, [11] industry players have enhanced their level of TF risk awareness and AML/CFT controls over the years. MAS has sustained its efforts to promote greater consistency and improvements across the sector.

35. Some established players, representing a significant proportion of the total transaction volume in the sector,[12] have implemented advanced data analytics capabilities in their control measures to monitor transactions and detect TF-related red flags. However, smaller-scale remittance agents may lack the resources to employ similarly advanced tools, typically relying on more conventional know-your-customer and screening control measures to detect TF activities. Known local TF cases to-date have shown that TF transactions often involve small transaction amounts and originate from legitimate sources such as salaries and business profits. This is in line with international trends and presents challenges for remittance agents in identifying potential TF cases.

UPDATES SINCE 2020 - MITIGATING MEASURES

36. MAS will continue to engage industry players to further strengthen their awareness of their TF risks and AML/CFT obligations. For instance, a TF thematic review of remittance agents and banks was conducted in 2020 to assess their understanding of TF risks and the effectiveness of their controls in detecting and deterring TF-related fund flows.

37. Subsequently, a Guidance Paper containing the findings of the review was published in 2023. This Paper outlined best practices from industry players, including the use of more sophisticated monitoring capabilities to detect and trace fund flows linked to terrorist activities, as well as promptness of response to authorities' information requests and directions. Additionally, in 2022, a joint MAS-CAD industry engagement session with payment service providers, including remittance agents, was held to raise awareness of licensees' obligations under the TSOFA and to share MAS's supervisory expectations and observed good practices. As part of MAS's ongoing supervision, it continues to identify vulnerable money remittance agents and subject them to supervisory checks.

HIGH RISK

38. **USE OF UNLICENSED MONEY REMITTANCES** | The Payment Services Act 2019 (PS Act) criminalises the operation of unlicensed money remittances. Despite this, Singapore recognises the existence of an unlicensed money remittance sector. Typically, these entities do not adhere to existing AML/CFT obligations such as customer due diligence, transaction monitoring, STR filing, and record keeping. There is a demand among Singapore's migrant worker population for such services due to their affordability compared to licensed money remittances and their relative convenience. Customers rely on them for various reasons, including a limited access to formal banking channels, cultural preferences, and the desire to evade currency control and tax obligations.

[11] Remittance agents refer to cross-border money transfer service providers in Singapore that are licensed under the Payment Services Act.
[12] As of April 2024, there are 195 licensed remittance agents in Singapore.

39. The main customers of these unlicensed money remittances are the large migrant workforce in Singapore. Most law enforcement cases involving unlicensed money remittance services concern transactions to the home countries of Singapore's major migrant worker populations. Some of these countries have been identified as high-risk TF jurisdictions by the Singapore authorities. **However, to date, there have been no observed TF linkages in the operations of unlicensed money remittances.**

UPDATES SINCE 2020 - MITIGATING MEASURES

40. Singapore remains vigilant to the sector's susceptibility to TF abuse and recognises the need to manage risks arising from the use of unlicensed money remittances in Singapore. The Singapore authorities have adopted a multi-pronged approach, including:

(a) Upstream prevention efforts through user-centric outreach and education programmes conducted in partnership with community partners such as the Migrant Workers' Centre and migrant worker dormitories. These efforts aim to highlight the importance of using licensed remittance agents.

(b) Increased access to licensed alternatives such as licensed remittance services and licensed digital payment services. This includes locating licensed remittances in situ at the migrant worker dormitories, especially during the COVID-19 pandemic.

(c) Proactive detection and investigation of unlicensed operators based on intelligence gathered by authorities.

BANKS

MEDIUM-HIGH RISK

KEY EXPOSURES TO TF THREAT AREAS

41. Terrorist financiers are known to use the banking sector to raise and move funds into and out of the Southeast Asian region. These typologies are extensively documented both regionally and globally due to the prevalence of banks and the ease of conducting transactions through them.

42. Based on investigations and cases prosecuted by law enforcement agencies to date, **banks in Singapore have not been exploited for TF activities. However, a small amount of funds/assets relating to persons of interest could have been initially deposited with the banks**. Nevertheless, we remain vigilant to the risk of Singapore's banking system being used as a conduit by terrorists and their financiers, given our position as an international financial centre. Singapore is also mindful of the risk of radicalised individuals using our banking system to provide funds for terrorism-related activities abroad, particularly due to the typically small amounts involved and the difficulty in distinguishing those amounts from legitimate transactions.

KEY VULNERABILITIES

43. **STATUS AS AN INTERNATIONAL FINANCIAL CENTRE |** Singapore's status as an international financial centre exposes us to large international money flows. Additionally, our geographical proximity to countries with active terrorist activities or terrorist groups makes us vulnerable to being used as a conduit for TF purposes. The sophisticated and interconnected banking system in Singapore, coupled with a wide range of accessible and efficient online financial services, further increases the risk of exploitation for illicit purposes. The TF vulnerability of the banking sector is assessed to have remained largely unchanged since the 2020 TF NRA, as the proportion of total wire transfer flows to and from high TF risk countries has remained consistent.

UPDATES SINCE 2020

44. **The exposure of banks in Singapore to customers posing higher TF risks, including from sectors such as foreign charities and NPOs,[13] remains low**. To date, there have also been no known TF cases suggesting that the new cross-border fast payment systems (e.g., PayNow-PromptPay, NETS-DuitNow QR code payment linkages) have been exploited to support overseas terrorism-related activities.

[13] Foreign NPOs and charities has been traditionally identified as a higher risk sector for TF, based on international typologies and academic research. For instance, there has been known involvement of NPOs in TF activities in the Southeast Asian region, many of which appeal for donations to help families of terrorists who have been incarcerated or killed during counter-terrorism operations. NPOs have also been known to be used as conduits in the region for funds received from the ISIS central command in the Middle East, to support ISIS-inspired terrorist groups. See section on NPOs for additional details.

45. **CHALLENGES IN DETECTING TF DUE TO SMALL TRANSACTION AMOUNTS AND SIMILARITY TO LEGITIMATE TRANSACTIONS |** The vast majority of banking transactions are intertwined with daily activities, including receiving salaries, paying bills, and saving money. Funds moved or stored by a terrorist or a sympathiser may appear legitimate until they are used to support terrorism-related activities. Moreover, local TF cases have revealed that radicalised individuals and sympathisers often engage in transactions involving small amounts, funding terrorism-related activities from legitimate sources such as salaries or savings. Consequently, distinguishing these transactions from individuals' legitimate financial activities becomes challenging in the absence of additional intelligence or indicators.

UPDATES SINCE 2020 - MITIGATING MEASURES

46. While the banks in the Singapore ecosystem generally have well-developed TF risk awareness and AML/CFT control measures, MAS recognises the importance of continued engagements with the banks. This involves regular dialogues with MAS and law enforcement agencies, participation in industry events to familiarise banks with the latest TF risks and typologies, and encouraging banks to adopt risk mitigation measures in response to continually evolving TF typologies.

DIGITAL PAYMENT TOKEN SERVICE PROVIDERS

MEDIUM-HIGH RISK

KEY EXPOSURES TO TF THREAT AREAS

47. DPTs, also known as virtual assets/currencies, have emerged as a potential means for terrorist financiers, particularly tech-savvy militants. to raise and move funds across borders. Recognised international typologies include using DPT service providers (DPTSPs) to solicit DPTs online, followed by transferring these tokens through multiple transactions within a brief period to a wallet address associated with extremist platforms.

UPDATES SINCE 2020

48. **Presently, there is no strong evidence indicating widespread utilisation of DPTs for TF across the Southeast Asian region**.[14] This could partly stem from the unavailability of technological advancements in areas afflicted by terrorism due to the lack of financial technology infrastructure and poor internet connectivity.[15]

49. Despite this, global typologies suggest a growing risk of virtual assets being exploited to facilitate TF activities, although fiat currencies remain dominant. There are indications that terrorists and terrorist groups are looking to make greater use of virtual currencies to support their illicit agendas in the wake of the COVID-19 pandemic. The Singapore authorities continue to closely monitor this evolving domain.

50. Singapore's status as a FinTech hub has attracted DPT service providers, and our high digital literacy facilitates the adoption of DPTs. While there are no known domestic TF cases involving DPTs, Singapore is cognisant of the higher TF risks originating from the increasing presence of DPT service providers. The higher TF risks are driven by the anonymity, speed, and cross-border nature of transactions facilitated by DPTSPs. Furthermore, there is a risk of licensed DPTSPs engaging with unregulated or inadequately regulated DPTSPs beyond Singapore's jurisdiction.[16] Compounding this risk is the "sunrise issue" – the uneven global implementation of the Travel Rule in the DPT sector. Hence, it is imperative for authorities and stakeholders to maintain vigilance over potential TF risks in this sector and closely monitor developments.

[14] RSIS Southeast Asia Report 2020, page 9: "Indonesia's Financial Intelligence Unit informed that PayPal and Bitcoin are often used by militants to move funds to avoid detection by the authorities. The source of money via PayPal had originated from Bitcoin. However, the scale of their usage may be limited to tech-savvy militants only."

[15] RSIS Southeast Asia Report 2020, page 24: "Technological innovations for finances are unavailable in Mindanao due to the absence of infrastructure in financial technologies and poor internet connectivity."

[16] For instance, the US authorities' settlement with Binance Holdings Ltd and its affiliates in November 2023 highlights that there remain inherent risks for virtual assets and virtual assets service providers globally. In its press release, US authorities noted apparent violations of multiple sanctioned programmes, and "the violations include failure to implement and report suspicious transactions with terrorists – including Hama's Al-Qassam Brigrades, Palestinian Islamic Jihad (PIJ), Al Qaeda, and the ISIS – ransomware attackers, money launderers, and other criminals." See: https://home.treasury.gov/news/press-releases/jy1925

KEY VULNERABILITIES

51. **ANONYMITY, SPEED, AND CROSS-BORDER NATURE OF TRANSFERS ASSOCIATED WITH DPTS |** DPTs are particularly vulnerable to TF abuse due to several factors:

(i) the potential anonymity they offer;
(ii) the convenience they provide as a near-instantaneous value transfer medium; and
(iii) the cross-border nature of the transactions.[17]

Features that enhance anonymity, such as mixers, tumblers, Internet Protocol anonymisers, and privacy coins make DPTs more appealing for TF, as they enable terrorists and their financiers to conceal their identities, counterparties, and physical locations. Their cross-border capability and the ability to make high-value transactions quickly make DPTs a more attractive option for raising or moving assets compared to conventional methods. However, these same characteristics pose significant challenges for law enforcement agencies in tracing and detecting DPT transactions related to TF activities.

UPDATES SINCE 2020

52. **LACK OF CONSISTENCY IN AML/CFT CONTROLS AND TF RISK UNDERSTANDING DUE TO MORE NASCENT AND FAST-CHANGING INDUSTRY, BOTH GLOBALLY AND LOCALLY |** Since the 2020 TF NRA, MAS has stepped up its supervisory and engagement efforts. MAS has also organised and participated in a series of industry engagement sessions to raise the industry's awareness of ML/TF risks in the lead-up to the enactment of the PS Act.

53. Additional guidance was issued to the industry in 2021 to facilitate effective implementation of AML/CFT controls.[18] Robust AML/CFT-focused licensing checks have been instituted to uphold standards across the sector.

MITIGATING MEASURES

54. **LEGISLATIVE CONTROLS |** DPTSPs in Singapore are subject to licensing under the PS Act and corresponding AML/CFT regulations, which came into effect on 28 January 2020 and are aligned with international standards, including FATF's recommendation 15 on value transfers. Licensed DPTSPs are required to collect and screen originator and beneficiary details before executing transfers and to transmit originator and beneficiary information to the next DPTSP when executing transfers. Following industry consultation in May 2023, additional enhancements were made to the AML/CFT regulations for DPTSPs on 2 April 2024 to further align our regime to international standards and practices.[19]

55. MAS has applied a risk-based approach in its supervision of DPTSPs, which includes inspections to examine the sector's effectiveness in combatting TF. This is complemented by MAS's surveillance of the DPT sector to identify areas or entities of higher risks and proactively detect entities that may be operating or providing DPT services illegally without a license, as well as ongoing outreach and engagements to raise the industry's TF risk awareness.

[17] FATF's Guidance for a Risk-Based Approach to Virtual Assets also affirms that virtual assets have characteristics such as increased anonymity, which may make them more susceptible to abuse by criminals, money launderers, and terrorist financiers.
[18] MAS published Strengthening AML/CFT Controls of Digital Payment Token Service Providers in March 2021, which provides an overview of MAS' AML/CFT requirements and supervisory expectations for the Digital Payment Token (DPT) sector.
[19] Please refer to https://www.mas.gov.sg/regulation/notices/psn02-aml-cft-notice---digital-payment-token-service

NON-PROFIT ORGANISATIONS

MEDIUM-LOW RISK

KEY EXPOSURES TO TF THREAT AREAS

56. **International and regional typologies have shown that terrorist financiers are known to use non-profit organisations (NPOs) to raise, move, and use funds.** International aid flowing into the ISIS-liberated areas of Iraq and Syria could present opportunities for ISIS to generate funds. Additionally, Singapore's proximity to jurisdictions with active terrorist threats and activities make us vulnerable to cross-border movements of people and funds for TF. Within the region, pro-ISIS groups and JI have reportedly raised funds through supporters working in Muslim charities and *dakwah* centres, though not necessarily with the knowledge or approval of the organisations involved.

UPDATES SINCE 2020

57. Beyond the possible diversion of legitimate funds for TF purposes due to weak internal controls, the sector is also witnessing the emergence of online fundraising movements that solicit donations from sympathisers for the families of jihadists, terrorist detainees, and martyrs. With the rapid growth of the digital economy and social media in Asia, especially following the COVID-19 pandemic, many NPOs and cause-based entities are turning to online platforms for fundraising activities, including those supporting TF causes. Notably, there have been numerous incidents of fundraising activities for humanitarian causes and Hamas via online platforms following the outbreak of the Israel-Hamas conflict in October 2023.

58. The local NPO sector comprises 3,471 entities.[20] These are predominantly registered charities, but also include a number of Companies Limited by Guarantee (CLGs), mosques, and societies. These NPOs fall under the regulatory purview of the Commissioner of Charities (COC), Accounting and Corporate Regulatory Authority (ACRA), Majlis Ugama Islam Singapore (MUIS), and Registry of Societies (ROS) respectively.

59. **Singapore's NPO sector is largely domestically oriented.** Registered charities are required by legislation to conduct activities that are wholly or substantially beneficial to the community in Singapore.

[20] As at 31 December 2022.

UPDATES SINCE 2020

60. **Only three out of ten charities in Singapore engage in some form of overseas work, make donations, and/or provide funding or services to beneficiaries outside Singapore.[21] These activities comprise less than 2% of the total expenditure of charities from 2020 to 2022.** An even smaller proportion of charities within this group conduct these activities in higher-risk jurisdictions and/or near conflict zones outside of Singapore. Mosques assist the fundraising efforts of Rahmatan Lil Alamin Foundation (RLAF), a registered charity under the purview of the COC, to support humanitarian relief efforts for people affected by natural disasters in the region. Aside from supporting such efforts through RLAF, mosques do not raise or donate funds to any person or entity outside Singapore. CLGs and societies, which are not part of the charity sub-sector, are even more domestically focused and typically do not engage in fundraising for foreign causes.

61. **Thus far, there has been no indication of foreign funding flowing into Singapore via our local NPO sector to support domestic terrorism-related activities, nor funds raised by local NPOs being moved to fund terrorism-related activities abroad.** Nevertheless, the Singapore authorities are aware of the possibility that funds raised in Singapore for charitable purposes, particularly for humanitarian relief use in or near conflict and other crisis zones, could be diverted for TF purposes. **To date, there have been no TF convictions of NPOs under the TSOFA**.

KEY VULNERABILITIES

62. Given that funds from local NPOs could potentially be diverted for TF purposes, the charity sub-sector, which has relatively more exposure to overseas activities, is assessed to be more vulnerable to TF.

63. **VARIED LEVELS OF AWARENESS OF EMERGING TF RISKS |** Findings from Ministry of Culture, Community, and Youth (MCCY)/Charity Unit (CU)'s 2024 survey indicate a higher level of awareness of the risk of TF abuse among charities since the last vulnerability assessment conducted in 2018. However, the level of TF risk understanding still varies. Larger charities tend to demonstrate a better understanding of and experience in risk management, while smaller charities may have less expertise but are nevertheless eager to learn about appropriate measures to protect themselves against potential TF abuse. Additionally, the lean and transient nature of the workforce in the charity sector may also impact the sustainability of training on TF awareness and risk management.

64. There is therefore an opportunity to further enhance the level of awareness and understanding of TF risks among registered charities. The COC continues to collaborate with various partners to conduct webinars and training sessions to increase the charities' awareness and understanding of TF risks. More charities are also keen to leverage such platforms to enhance their understanding of the risks of TF abuse and the mitigating measures that may be taken to safeguard themselves.

65. In general, charities recognise that the sector is at risk of TF abuse, and are able to identify the prevalent methods in which charities could be abused for TF activities. These include diversion of charitable funds or resources, support for recruitment, abuse of programming, false representation, or sham charities, as well as affiliation with terrorist activities. However, given the evolving risk environment, charities that have not periodically assessed their risks of TF abuse may not be as sensitive to emerging risks that could increase their

[21] Based on a survey conducted by the COC in 2024, as part of Singapore's Vulnerability Assessment for the NPO sector and the disclosures of overseas expenditure made by charities in the financial years ended 2020 – 2022.

susceptibility to TF abuse. Charities that have yet to conduct any TF risk assessment are recommended to do so to gain a better understanding of their exposure to TF risks.

UPDATES SINCE 2020 – ONLINE FUNDRAISING

66. **The growth of online fundraising activities in recent years, driven by the rapid expansion of the digital economy in Asia, particularly due to the COVID-19 pandemic, has significantly expanded their global reach.** This growth leverages advancements in payment methods, including digital transactions and DPTs, and outreach methods, such as the explosive growth of online and social media platforms. As the variety and ease of payment methods increase alongside the broader audience for online causes, the risk of terrorist financiers exploiting online fundraising for TF purposes also increases. They may siphon funds from legitimate online charitable appeals (though not necessarily with the knowledge of the appeal starter) or conduct TF fundraising **under the guise of online charitable appeals**.

67. While many of these causes are legitimate and admirable, terrorist financiers have been known to exploit this by disguising their own TF fundraising activities as humanitarian efforts. Donors to these causes may be unaware and unable to distinguish between fraudulent TF crowdfunding and genuine humanitarian crowdfunding, thus become unwitting facilitators of TF activities.

68. Singapore has encountered **one TF case involving contributions to foreign terrorist activities via foreign online fundraising platforms (refer to Box Story 2)** to date and remains highly vigilant to the risks posed by this emerging typology. This takes into consideration Singapore's high internet penetration rate and connectivity with the global economy, which have enabled foreign online fundraising campaigns to draw donations from Singapore. We cannot underestimate the ability of terrorist groups, such as ISIS, to disseminate their propaganda activities through the internet, including rallying their overseas-based supporters and sympathisers for funds.

69. **EVIDENTIAL CHALLENGES IN PROVING INTENT OF TF DONORS |** Terrorist financiers sometimes operate online fundraising campaigns or charities under the pretence of humanitarian causes. Hence, willing TF donors can knowingly contribute to TF causes through these campaigns or charities but subsequently feign ignorance when investigated to avoid prosecution. Additionally, some online fundraising platforms may allow anonymous donations and have weak donor identification measures in place. Law enforcement agencies could therefore face greater challenges in prosecuting willing TF donors under such circumstances.

70. To address this evidential difficulty, the TSOFA provides that an offence is made out if the offender has "reasonable grounds to believe" that the funds provided would be used for TF purposes. Even if a TF donor claims ignorance of how his donated funds would be used, he could still be prosecuted if there are sufficient red flags indicating that donations to the specific campaign or charity would be applied to TF purposes. Adopting such a test has allowed Singapore to successfully mount prosecutions against donors who contributed to online fundraising campaigns or foreign charities for TF purposes, purportedly providing support to humanitarian causes.

71. **PROSECUTING CITIZENS FOR TF CROWDFUNDING ACTIVITIES CONDUCTED OVERSEAS |** Given the global reach of crowdfunding activities and social media platforms, there is a possibility of funds being sent out of Singapore in support of foreign TF crowdfunding causes. However, as long as the act of sending the funds occurs in Singapore, prosecution is still possible under the TSOFA.

Furthermore, Section 34 of the TSOFA ensures that the legislation has extraterritorial reach – any citizen of Singapore who donates to foreign TF causes can still be prosecuted under the TSOFA, even if the offence is committed overseas, as exemplified in Box Story 1.

MITIGATING MEASURES

72. **INCREASING TF RISK AWARENESS AND UNDERSTANDING AMONG CHARITIES |** Some charities have implemented training programmes for their staff and volunteers to raise awareness and understanding of TF risks. The COC has also collaborated with various partners, including legal professionals and law enforcement agencies, to conduct webinars aimed at enhancing TF risk understanding among charities.

73. During targeted outreach sessions to the charity sector, the COC, in collaboration with MHA, briefed participants on the latest terrorism threats to Singapore and TF risks specific to the NPO sector. This included discussion of regional NPOs that reportedly served as conduits to channel funds to terrorist groups. The Singapore authorities also emphasised the importance of conducting due diligence checks on foreign partners and beneficiaries when charities engage in overseas activities. Charities are also reminded of the legal obligation under TSOFA to provide information on property and financial transactions with a nexus to terrorists or TF activities to the Singapore Police Force (SPF) by lodging STRs.

UPDATES SINCE 2020

74. **INCREASING TF RISK AWARENESS AND UNDERSTANDING OF FOREIGN ONLINE FUNDRAISING CAMPAIGNS |** Singapore has observed that donations from Singapore to foreign online fundraising campaigns typically flow through **payment channels, including payment service providers, bank transfers, or digital banking routes** such as credit and debit cards. In response, MAS and MHA have intensified efforts to raise awareness among the payment and banking sectors regarding the TF risks associated with donations to foreign online fundraising campaigns. **While no manifestation of this risk has been observed in Singapore charities to date, they should nonetheless remain vigilant against the potential exploitation of online charitable fundraising campaigns for TF activities.**

75. **LEGISLATIVE CONTROLS |**The Charities Act requires all charities (except those exempted) to be registered with the COC. The COC may reserve the right to refuse registration or remove an institution from the register of charities if its registration or continued registration appears contrary to the public interest. Consequently, charities attempting to exploit the NPO sector for TF purposes can and will be deregistered by the COC.

76. Moreover, to ensure transparency and enable the public to differentiate between legitimate and false charities, the register of charities (including deregistered charities) is publicly accessible. Additionally, the Charities Act prohibits individuals convicted of terrorism or TF, whether in Singapore or overseas, from serving as governing board members, key officers, or trustees of any charity. **All fundraising appeals for charitable, benevolent, and philanthropic purposes in Singapore, whether conducted online or offline, and regardless of whether they support local or foreign causes, are regulated under the Charities Act and the Regulations.**

UPDATES SINCE 2020

77. To address the escalating TF risk associated with online fundraising, Singapore enacted the Online Criminal Harms Act (OCHA) in July 2023. This legislation empowers the Government to issue directions to online service providers, including social media platforms and online fundraising platforms, to prevent suspected criminal activities, such as terrorism or TF-related content, from engaging with or reaching users in Singapore. Consequently, this makes it harder for terrorist organisations to solicit funds from Singaporeans through foreign TF crowdfunding campaigns.

78. Our law enforcement agencies and STRO are actively forging strong partnerships with foreign counterparts, including through information exchange to facilitate the prosecution of TF crowdfunding activities in foreign jurisdictions. Additionally, the Singapore authorities have intensified public education campaigns aimed at encouraging individuals to donate to registered charities, thereby ensuring that their donations are used for genuine charitable causes.

79. **GUIDELINES AND REPORTING MECHANISMS ON THE DISBURSEMENT OF FUNDS, REPORTING OF SUSPICIOUS TRANSACTIONS, AND DUE DILIGENCE** | The varied levels of awareness of emerging TF risks among charities may impact the implementation of mitigating measures that are proportionate to the exposure of TF risks. Findings from the survey indicate that most charities have some measures to safeguard their organisations against TF abuse. The key measures include the conduct of due diligence checks on their stakeholders (e.g., governing board members, key officers, trustees, employees, volunteers, beneficiaries, and partners), transacting via regulated financial channels, and monitoring mechanisms to ensure that funds disbursed are used for the intended charitable purposes.

80. However, charities should remain informed of emerging risks and periodically review measures commensurate with their exposure to risks of TF abuse. Charities should conduct additional checks and formalise proper policies and procedures when they receive donations, disburse funds, or conduct activities in higher-risk jurisdictions, to mitigate the risks of misuse of charitable funds and resources for TF.

81. In addition, more charities should establish procedures to report suspicious transactions and activities and implement additional mitigating measures promptly. To aid charities in establishing these mitigating measures to safeguard against TF abuse, COC has initiated targeted outreach programmes and published AML/CFT guidance to educate charities on the methods through which the charity sector could be abused for terrorism and TF, emphasising the importance of conducting appropriate due diligence checks on donors, partners, and beneficiaries, and reinforcing the legal obligation under TSOFA to provide information on property and financial transactions with a nexus to terrorism/TF to the SPF by lodging STRs.

UPDATES SINCE 2020

82. In January 2018, COC introduced a *Code of Practice for Online Charitable Fund-Raising Appeals, advocating for* best practices to ensure legitimacy, accountability, and transparency of charitable appeals hosted on crowdfunding platforms in Singapore. This includes assessing risks associated with TF and establishing adequate systems, processes, and procedures to address such risks. Five major crowdfunding platforms in Singapore have committed to the Code of Practice,[22] collaborating closely with COC to undergo

[22] The platforms are: Give.asia, Giving.sg, Ray of Hope, SimplyGiving, and DeeDa. For more information on the Code of Practice and its best practices, please visit https://www.charities.gov.sg/Pages/Fund-Raising/Use-of-OFR-and-CFR/Code-of-Practice-for-Online-Charitable-FR.aspx#

voluntary periodic reviews of their systems and processes in 2021 and 2022 to evaluate their adherence to best practices. These platforms have shown receptiveness to the recommendations resulting from these reviews.

83. COC launched the *Terrorist Financing Risk Mitigation Toolkit for Charities* in February 2023 to increase awareness of TF abuse among charities and provide guidance for identifying, assessing, and mitigating TF risks systematically. In a survey conducted by COC in 2024, the majority of charities recognise the vulnerability of the charity sector to TF abuse. Approximately 70% of the surveyed charities demonstrated an understanding of the prevalent methods of charity abuse for TF purposes. Moreover, most charities have implemented mechanisms to monitor activities and utilisation of disbursed funds both within and outside Singapore.

84. As part of COC's regulatory measures to mitigate TF risks in the charity sector, stringent checks are conducted to verify the authenticity of applications for permits to raise funds for foreign charitable purposes. Non-compliance with these regulations carries severe penalties, including criminal conviction under the TSOFA.

CROSS-BORDER CASH MOVEMENT

MEDIUM-LOW RISK

KEY EXPOSURES TO TF THREAT AREAS

85. Terrorist financiers globally have been observed employing cash couriers to physically transport funds across borders to finance their activities. Unlike transactions within regulated sectors, cash transactions lack a digital trail.

86. These typologies are well documented in the region, perpetrated by cash-intensive economies with porous borders, loose maritime boundaries, and proximity to conflict zones. **These routes do not currently involve Singapore and there have been no indications of cross-border cash movement (CBCM)[23] related to TF in Singapore to date.[24]**

87. Nevertheless, Singapore is aware that our status as an international transport and transshipment hub, coupled with our geographical proximity to countries with active terrorist groups, makes us vulnerable to being used as a potential location for the pickup and transit of funds by cash couriers, particularly for foreign terrorist fighters travelling to conflict zones.

KEY VULNERABILITY

88. **Singapore maintains stringent border controls and a robust framework to detect illicit CBCM.** This is facilitated by strong collaboration and intelligence sharing among various law enforcement agencies, including the Immigration & Checkpoints Authority of Singapore (ICA), Singapore Customs, and the SPF. Nevertheless, our sectoral deep dive has identified the following vulnerability.

89. **The anonymity accorded to small amounts of money brought across borders poses a risk,** particularly concerning the funding of terrorist activities abroad. This risk persists, especially if individuals manage to leave Singapore without detection. International typologies also recognise that the small sums of money typically associated with terrorism often fall below the reporting threshold.[25]

[23] This analysis addresses the physical movement of cash and bearer negotiable instruments across Singapore's borders and does not encompass the cross-border movement of funds, including electronic transfers and domestic transactions.
[24] Based on the analysis of cases thus far, the typical purposes of CBCM include business transactions, gambling activities, and personal use. None of the Cash Movement Reports filed to-date have been linked to TF.
[25] Singapore's reporting threshold for CBCM is S$20,000, in line with the prevailing FATF standards.

MITIGATING MEASURES

90. To mitigate these risks, Singapore actively employs intelligence, data analytics, and imaging technology to detect such illicit activities at the checkpoints.

UPDATES SINCE 2020

91. To further enhance public compliance with the CBCM measures, ICA and SPF have introduced the electronic Cross-Border Cash Reporting Regime (e-CBCRR) declaration form, which has been integrated with the electronic Singapore Arrival Card (e-SGAC) since May 2024. This initiative complements the sanctions and punitive measures, such as fines and confiscations, that have been imposed on CBCRR offenders.

PRECIOUS STONES AND METALS DEALERS

MEDIUM-LOW RISK

KEY EXPOSURES TO TF THREAT AREAS

92. International and regional typologies indicate relatively few instances of terrorist financiers using precious stones, precious metals, and precious products (PS/PM/PPs) to move or raise funds for terrorism. However, PS/PM/PPs have high intrinsic value in a relatively compact form and tend to maintain or increase their value over time. This means that PS/PM/PPs could still serve as a viable store of value and accepted as an alternative currency.

93. Following Singapore's implementation of a cash transaction reporting regime for precious stones and metals dealers (PSMDs) in 2014, Singapore established a division within the Ministry of Law (MinLaw) to supervise PSMDs for AML/CFT measures under the Precious Stones and Precious Metals (Prevention of Money Laundering and Terrorism Financing) Act 2019 (PSPM Act), which took effect in April 2019. [26]

UPDATES SINCE 2020

94. The definition of precious products under the PSPM Act was amended in 2024 to update the definition of "precious product" to encompass any such product priced above a prescribed value.

95. This assessment encompasses the regulated dealers[27] of PS/PM/PPs as defined within the PSPM Act. [28] The sector has a diverse range of value-chain activities, including retailing in physical stores, online platforms, auctioning, wholesale/distribution, manufacturing, and second-hand goods dealing. **Locally, there are no known cases of PS/PM/PPs being used for TF activities to date.** Nevertheless, the inherent characteristics of the sector make it vulnerable to misuse for TF.

KEY VULNERABILITIES

96. **VARIED LEVELS OF AWARENESS OF TF RISKS AND AML/CFT CONTROLS** | MinLaw's supervision of the sector has led to improvements in the industry's awareness of TF risks and AML/CFT controls over the years, although such improvements are still lacking in some segments of the sector.

[26] As of 1 May 2024, the PSPM Act has been amended to the Precious Stones and Precious Metals (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing) Act 2019.
[27] Regulated dealing refers to the (a) manufacturing; (b) importing or possessing; (c) selling; (d) purchasing for resale of any precious stone, precious metal, or precious product; and (e) selling or redeeming asset-backed tokens.
[28] As of 1 April 2024, there were 2002 registered dealers in the PSMD sector, operating 2,566 outlets amongst them.

97. **DIFFICULTY IN TRACING SPECIFIC ITEMS |** The challenge of tracing specific items and the global market for PS/PM/PPs make it easier for terrorist financiers to exploit cross-border, multi-jurisdictional situations to obscure paper trails. This renders it more challenging for law enforcement agencies to conduct investigations.

UPDATES SINCE 2020

98. **ASSET-BACKED TOKENS[29] |** PS/PM/PPs are vulnerable to TF abuse as they can be used to back asset-backed tokens, which could potentially be exploited for terrorist funding activities. These instruments are subject to AML/CFT regulations under the PSPM Act, mandating PSMDs dealing with them to implement AML/CFT controls. Singapore has also taken additional steps to mitigate this risk by instituting controls for virtual assets (refer to DPT section).

MITIGATING MEASURES

99. To address these vulnerabilities, the PSPM Act mandates all PSMDs to implement AML/CFT controls during transactions. Additionally, MinLaw closely monitors and supervises higher-risk PSMDs to prevent TF abuse. This is supplemented by MinLaw's regular outreach initiatives and provision of guidance materials to enhance the sector's awareness of TF risks.

[29] "Asset-backed token" means a token, certificate, or other instrument supported by one or more precious metals, precious stones, or precious products, granting the holder entitlement to the respective precious metal, precious stone or precious product, or a portion thereof. However, it excludes:

(a) securities or derivatives contracts as defined in the Securities and Futures Act 2001;
(b) commodity contracts as defined in the Commodity Trading Act 1992;
(c) digital payment tokens as defined in the Payment Services Act 2019; and
(d) any token, certificate, or other instrument that may be prescribed.

CONCLUSION

100. **The global terrorism landscape undergoes constant evolution, leading to continual shifts in TF risks**, both on the international stage and domestically. Singapore acknowledges the necessity of sustained vigilance against both established and emerging threats, along with vulnerabilities pertaining to terrorism, particularly TF.

101. **Singapore has developed and implemented a comprehensive WOG approach to continually identify, monitor, and mitigate TF risks.** This approach involves sustained collaborations and close coordination with the private sector and academia to enhance our collective understanding of TF risks. The refreshed 2024 TF NRA articulates the latest key TF threats and vulnerable sectors in Singapore and considers significant developments since 2020. This report will assist the Singapore authorities in directing our national efforts against TF towards high-risk areas and refining our national CFT strategy, as delineated in the refreshed 2024 National Strategy for CFT published in July 2024. Furthermore, it furnishes private sector stakeholders with an updated overview of Singapore's TF risks and guidelines on how industry players should sustain vigilance against prevailing and emerging TF risks.

102. **Singapore acknowledges the global reach of terrorism and TF and remains committed to bolstering collaboration with foreign law enforcement, intelligence, regulatory, and supervisory counterparts in the international fight against terrorism and TF.** Singapore will also continue to actively contribute to regional and international initiatives aimed at enhancing our collective understanding of the prevailing and emerging TF risks and typologies. These include proactive engagements in international bodies such as the FATF, the Asia/Pacific Group on Money Laundering, the Egmont Group, the Financial Intelligence Consultative Group (FICG), and INTERPOL's Project PACIFIC Working Group.