

Anti-Money Laundering and Countering the Financing of Terrorism Guide for Companies Limited by Guarantee

Issued on 29 NOVEMBER 2024

TABLE OF CONTENTS

03

Introduction

10

How CLG-NPOs can be protected against ML/TF

04

Money laundering, terrorism financing, and the impact on NPOs, including CLG-NPOs

16

Appendix A: Red-flag indicators

07

Methods and risk of abuse of NPOs

Notes on version(s)

Version	Notes
1.0	Issued on 30 October 2015.
1.1 (Current)	Issued on 29 November 2024.

INTRODUCTION

- 1.1 This guide is prepared for directors, other officers, employees and relevant stakeholders of Companies Limited by Guarantee (CLGs) operating as non-profit organisations (NPOs) to manage the risks of potential abuse of the CLG-NPO for Money Laundering (ML), Terrorism Financing (TF) and other illicit purposes.
- 1.2 A CLG-NPO may be at risk of being abused for ML/TF or other forms of terrorist support by virtue of its characteristics or activities. This guide provides information about the types of risks faced and recommend practices that CLG-NPOs may adopt to identify and manage their exposure to such risks.
- 1.3 An NPO is defined by the Financial Action Task Force (FATF) as “*a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of ‘good works’*”¹.

¹ Per FATF Recommendation 8 Non-Profit Organisations

MONEY LAUNDERING, TERRORISM FINANCING, AND THE IMPACT ON NPOs, INCLUDING CLG-NPOs

Overview of the FATF and Singapore's commitment

- 2.1 Singapore is a member of the FATF, an inter-governmental body that leads global action to tackle ML, TF and proliferation financing (PF). The FATF researches how money is laundered and terrorism is funded, promotes global standards (known as FATF Recommendations) to mitigate the risks, and assesses whether countries are taking effective action.
- 2.2 As a member of the FATF, Singapore is committed to implementing the FATF Recommendations and is evaluated by FATF for our compliance with these Recommendations.

The nature, differences and impact of ML and TF

- 2.3 ML is the process in which illegitimate sources of property or proceeds are disguised in order to make it appear legitimate, so that criminals can enjoy the benefits of their crimes and avoid detection by competent authorities. TF is the financing of terrorist acts and of terrorists and terrorist organisations.
- 2.4 ML and TF share a common characteristic: both involve concealing the movement of funds. However, a key difference lies in the origin of these funds. While ML exclusively deals with proceeds of crime, TF can involve funds that originate from both legitimate and illegitimate sources. For instance, funds legitimately raised by a CLG-NPO could potentially be misused to support terrorist activities or terrorist organisations.
- 2.5 ML/TF activities have a detrimental impact on Singapore's economy and security. In an increasingly globalised economy, the impact of ML/TF may have far-reaching effects. With the expansion of both physical and electronic financial infrastructure, funds can easily move across borders, and ML/TF activities are becoming more and more sophisticated and challenging to detect. To help build and maintain Singapore's strong reputation as a well-regulated financial hub, everyone plays an important role in combating ML and TF.

The role of NPOs, including CLG-NPOs, in the global community and their vulnerability to being abused by terrorists


- 2.6 NPOs play a vital role in the world economy, complementing national economies and social systems by providing essential services. Their efforts not only complement the activities of governmental and business sectors in providing essential services, but also offer comfort and hope to those in need around the world.

- 2.7 Unfortunately, terrorists are exploiting the NPO sector to raise and move funds, provide logistical support, encourage terrorist recruitment, or otherwise support terrorist organisations and operations.
- 2.8 NPOs are at risk of abuse as they:
- enjoys public trust;
 - have access to considerable sources of funds, and in some contexts are cash-intensive; and
 - may have a global presence that provides a framework for national and international operations and financial transactions.
- 2.9 The misuse of NPOs not only facilitates terrorist activity but also undermines the confidence of donors and financial institutions, and jeopardises the integrity of NPOs.

AML/CFT Legislation in Singapore

- 2.10 The applicable Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) laws and regulations in Singapore include the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 (CDSA), the Terrorism (Suppression of Financing) Act (TSOFA) 2002 and the United Nations Regulations.
- CDSA: The CDSA criminalises the laundering of proceeds derived from drug trafficking, tax evasion and other serious offences. Under the CDSA, it is mandatory for any person to lodge a Suspicious Transaction Report (STR) if he knows or has reason to suspect that any property may be connected to a criminal activity. The failure to do so may constitute a criminal offence.
 - TSOFA: The TSOFA not only criminalises TF but also imposes a duty on a person to provide information pertaining to TF to the police. The failure to do so may constitute a criminal offence. Under the TSOFA, any person shall lodge a STR if he has possession, custody or control of any property belonging to any terrorist or if he has information about a transaction or any transaction in respect of, or any property belonging to any terrorists.²
 - UN Regulations: The UN Regulations prohibit dealing in funds or other assets of particular individuals and entities designated by the UN Security Council as contributing to a particular threat to, or breach of, international peace and

² First Schedule of TSOFA available from <https://sso.agc.gov.sg/Act/TSFA2002?ProvIds=Sc1-#Sc1->



security³, and impose a duty to provide information on prohibited transactions to the Singapore Police Force (SPF).

2.11 CLG-NPO, its directors, other officers and employees must comply with all applicable AML/CFT laws and regulations. It is a serious offence to commit or assist in ML or TF, and equally grave to tip off any impending or on-going investigations of suspicious criminal activities, as the penalties include heavy fines and jail sentences.

³ United Nations Security Council Consolidated List available from <https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list>

METHODS AND RISK OF ABUSE OF NPOs

How NPOs may be abused by money launderers and terrorist financiers

The abuse of NPOs for ML/TF may take place in various forms, given the diverse nature of NPOs. This includes, but not limited to, the following typologies:

3.1 Diversion of funds

This means that an NPO, or an individual acting on behalf of an NPO, diverts funds into known or suspected terrorist activities. For example, funds raised by NPOs for humanitarian programmes are diverted to support terrorism at some point through the NPO's business process. Both internal and external individuals may act as fundraisers to raise funds in the name of the NPO to support terrorist purposes, with or without the NPO's knowledge. An NPO might also be used to launder money or be used as a legitimate front to move funds from one place to another.

3.2 Affiliation with a terrorist entity

This means that an NPO or an individual acting on behalf of an NPO maintains operational ties with a terrorist organisation or its supporters. For example, individuals supporting terrorist organisations may work as staff of an NPO while maintaining contact with fellow terrorist representatives, with or without the NPO's knowledge. Affiliations can range from informal personal connections between NPOs directing officials and terrorists, to more formalised relationships between NPOs and terrorists. The resources and facilities of the NPO may be used or are used to create an environment which supports or promotes terrorism related activities.

3.3 Abuse of programming

This means that NPO-funded programmes meant to support legitimate humanitarian purposes are manipulated at the point of delivery to support terrorism. For example, an NPO may be established to advance religion and education in the jurisdiction in which it is operating. However, the NPO's activities could be manipulated by advancing philosophies designed to lend support to a terrorist organisation.

3.4 Support for recruitment

This means that NPO-funded programmes or facilities are used to create an environment which supports and/or promotes terrorism recruitment activities. For example, NPOs may be involved in transferring funds to terrorists, providing financial support to families of terrorists, organising and hosting events that support terrorists, and publishing materials supporting terrorism or terrorists. They may also

use their facilities to recruit and train individuals to engage in acts of terror, provide meeting places for terrorists, and host speakers that advocate terrorism.⁴

3.5 False representation or sham entities

This means that under the guise of charitable activity, an organisation or individual raises funds and/ or carries out other activities in support of terrorism. Terrorists may try to set up organisations as a sham front, raising funds, promoting causes and carrying out activities in support of terrorism. Companies may also be set up as a shell or front company to launder funds.

Case studies of NPOs which were abused

The following case studies from other countries illustrate how NPOs can be abused for TF purposes:

3.6 Diversion of funds by actors internal to NPOs (Collection phase)

A company was established with very broad commercial purposes. Numerous small deposits were made to the company's account by an individual who had signing authority on the account. These funds were immediately transferred to foreign-based companies. An investigation by the national financial intelligence unit revealed that the individual with signing authority was also a directing official of an NPO. It was suspected that the small deposits made into the company's account originated from fundraising by the NPO. Law enforcement information indicated that the NPO was known to have ties to a terrorist group. A second directing official of the NPO, who was also a manager of the company, also had ties to the terrorist group. The investigation concluded that the company was a front, being used as a conduit to transfer funds on behalf of the NPO linked to a foreign terrorist group.

3.7 Diversion of funds by actors internal to NPOs (Retention phase)

An NPO was raising funds supposedly for humanitarian relief in an area of conflict. The NPO used collection boxes outside religious institutions to solicit donations. The funds raised were held in a bank account. The founder of the NPO was suspected of diverting the funds to facilitate terrorism rather than using them for the stated humanitarian activities. A law enforcement investigation resulted in the arrest of the founder of the NPO for terrorism facilitation offences. The case is still under investigation. To date, although there have been no convictions, USD 60,000 in collected funds has been seized.

3.8 Diversion of funds by actors external to NPOs (Transfer phase)

An NPO was established to support charitable work in foreign areas of conflict. An investigation by the national financial intelligence unit, initiated by suspicious transaction reporting, revealed that locally collected funds were being transmitted to

⁴ 'Risk of Terrorist Abuse in Non-Profit Organisations' in FATF (2014), para.118 & 119, p.46.

foreign-based charitable organisations. The investigation also uncovered that, once the funds were received by the foreign-based charitable organisations, they were systematically passed on to persons or organisations which were part of, or affiliated with, a known terrorist organisation. While there were established connections between the foreign-based charitable organisations and the terrorist organisation, direct links between the NPO and the terrorist organisation could not be substantiated.

3.9 Abuse of Programming (Delivery of programmes phase)

An NPO was carrying out religious and educational activities domestically. Information provided by the national financial intelligence unit indicated that the NPO had received over USD 13,000 from a foreign organisation known to provide support to a foreign terrorist group. Subsequent open-source research indicated that the NPO's education programs espoused an ideology that was shared by several foreign terrorist groups. Concerns arose that this shared ideology was being exploited for recruitment for a terrorist organisation. The NPO was audited by the national regulator, and the audit found that the NPO could not account for the origin of much of its income and expenditures. Based on this, the NPO was deregistered.

3.10 False front

An NPO established as a cultural youth association was the recipient of several government grants. A law enforcement investigation into the operations of the NPO found that it was a front organisation for a terrorist group. The actual activities of the NPO included raising and managing funds for the terrorist group and disseminating the group's extremist message via the Internet. While the NPO had a formally constituted governing body, it was created and directed by members of the terrorist group. The principal individuals involved were arrested and the NPO and its website were shut down.

HOW CLG-NPOs CAN BE PROTECTED AGAINST ML/TF

- 4.1 This section outlines recommended measures for CLG-NPOs to mitigate against ML/TF risks. It is important to note that the implementation of these measures should be proportionate to the CLG-NPO's exposure to ML/TF risks. CLG-NPOs should be informed of emerging risks and periodically review their measures. CLG-NPOs should also consider the availability of resources when adopting these measures.
- 4.2 These recommendations are not exhaustive and CLG-NPOs should tailor their approach based on their ML/TF risk assessment and operational context.

Maintaining strong corporate governance and financial transparency

- 4.3 CLG-NPOs should maintain robust policies and procedures for financial management and have internal controls that promote transparency and accountability of funds, in order to safeguard against potential ML/TF risks. For example, a CLG-NPO should have proper internal control systems with proper procedures for key processes, such as procurement and payment, revenue and receipts, and a system to ensure proper delegation of authority and appropriate approval limits. There should be measures in place to ensure proper segregation of duties and adequate checks and balances, especially over financial matters such as the collection, handling of cash, depositing, transfer of funds and the issuing of receipts.
- 4.4 Formal written policies and procedures for key processes should be documented, implemented and adhered to.
- 4.5 CLG-NPOs are also encouraged to conduct regular reviews of their internal controls, policies and procedures, key charitable programmes and partnerships to protect themselves from ML/TF risks.
- 4.6 CLG-NPOs are reminded to keep complete financial records of income, expenses and financial transactions throughout their operations.

Knowing key donors, partners and beneficiaries

- 4.7 CLG-NPOs should carry out reasonable due diligence checks on their key donors, partners and beneficiaries. Resource permitting, CLG-NPOs should put in their best efforts to confirm the identity, credentials and good standing of these parties, while respecting donor confidentiality.
- 4.8 Due diligence should be undertaken by CLG-NPOs on a best efforts basis:
 - (a) before accepting funds from prospective donors, disbursing funds or providing support to prospective beneficiaries, or establishing working relationships with prospective representatives, agents, contractors, partners, suppliers or vendors;
 - (b) when suspecting ML/TF; or

(c) when doubting the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification.

4.9 Enhanced checks should be conducted when donors, beneficiaries or partners are located in high-risk jurisdictions and/or near conflict zones.

4.10 CLG-NPOs should stay informed of periodic updates to the following:

- a) the list of UN-designated individuals and entities subject to sanctions⁵;
- b) any list of designated terrorists and terrorist entities⁶;
- c) any AML/CFT guidance/circulars issued by the Office of the Commissioner of Charities (COC);
- d) any list of the business sectors/industries/activities which are susceptible to risks of ML/TF abuse;⁷ and
- e) any list of jurisdictions identified in the FATF's "black" and "grey" lists.⁸

4.11 To facilitate this, CLG-NPOs are highly encouraged to subscribe to the [Monetary Authority of Singapore Mailing List](#) and [IMC-TF Mailing List](#) for updates on designated persons and entities.

⁵ The lists of designated individuals and entities subject to sanctions by the UN Security Council may be found at: <https://www.mas.gov.sg/regulation/anti-money-laundering/targeted-financial-sanctions/lists-of-designated-individuals-and-entities>.

⁶ The lists of persons and entities designated as terrorists or terrorist entities by the Inter-Ministry Committee on Terrorist Designation (IMC-TD) may be found at: <https://www.mha.gov.sg/what-we-do/managing-security-threats/countering-the-financing-of-terrorism>.

⁷ CLG-NPOs may refer to Singapore's refreshed Terrorism Financing National Risk Assessment 2024 for more information about the TF risks of various sectors: <https://www.mha.gov.sg/mediaroom/press-releases/singapore-refreshes-the-terrorism-financing-national-risk-assessment-and-national-strategy-for-countering-the-financing-of-terrorism/>.

CLG-NPOs may also refer to Singapore's Money Laundering National Risk Assessment, which provides an overview of Singapore's key ML risks: <https://www.mas.gov.sg/publications/monographs-or-information-paper/2024/money-laundering-national-risk-assessment>.

⁸ FATF's "black" list sets out the high-risk jurisdictions that are subject to a call for action due to significant strategic deficiencies in their regimes to counter ML/TF or proliferation financing. FATF's "grey" list sets out the jurisdictions which are under increased monitoring by the FATF to address strategic deficiencies in their regimes to counter ML/TF or proliferation financing.

The lists of high-risk and other monitored jurisdictions (i.e. FATF's "black" and "grey" lists) may be found at: <https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html>.

Programme planning and monitoring

- 4.12 CLG-NPOs should establish documented and clear selection criteria for beneficiaries and the scope of activities conducted for their benefit. CLG-NPOs should always know what their funds are being accepted and used for, and regularly review the expenditure to ensure that funds are channelled towards causes which are in line with their objectives. For example, CLG-NPOs should be vigilant to ensure that their name is not being used to support persons or causes with which they are not familiar.
- 4.13 For overseas disbursements, CLG-NPOs should assess whether overseas activities are in line with their charitable objectives, establish written procedures for due diligence checks, reporting of suspicious activities and documented mechanisms to monitor usage of funds.
- 4.14 When partnering with other organisations on charitable projects, CLG-NPOs should have clear written agreements outlining the activities to be undertaken, establish documented mechanisms to monitor these activities and fund usage to ensure that the partnership agreement is complied with.
- 4.15 CLG-NPOs should monitor project performance on a regular basis by verifying the existence of beneficiaries and ensuring the receipt of funds. CLG-NPOs should also maintain detailed budgets and keep proper records of related purchases and expenses for each project. Where possible, conduct regular on-site inspections or visits. If on-site inspections or visits are not possible or not appropriate, CLG-NPOs should minimally request regular written progress reports from partners or beneficiaries to monitor project developments, especially those conducted in high-risk countries or regions near conflict zones.
- 4.16 All anomalies or discrepancies identified during on-going monitoring, as well as any red flag indicators that could be a warning sign of unusual activity that could be indicative of ML/TF⁹, shall be escalated to the relevant personnel and governing board members in a timely manner.
- 4.17 In such a case, the CLG-NPO shall carry out the necessary mitigation and/or rectification, which may include but are not limited to the termination of funding or partnership, promptly. The CLG-NPO may also take additional measures, where appropriate and necessary, to prevent the development of new projects and new practices, or the adoption of new technologies, which involve risks of ML/TF or proliferation financing¹⁰.

⁹ A non-exhaustive list of red flag indicators is set out in **Appendix A** below.

¹⁰ Proliferation financing refers to financing the proliferation of weapons of mass destruction which would pose a significant threat to international peace and security, as identified by the relevant United Nations Security Council Resolutions. The FATF has provided guidance on measures to combat proliferation

Conducting financial transactions through regulated financial channels

- 4.18 As far as possible, CLG-NPOs should ensure that transactions or fund transfers are conducted through regulated financial channels¹¹. This is particularly important for disbursement of funds beyond Singapore. Using regulated channels help minimise the potential diversion of funds for TF while the funds are in transit.
- 4.19 In circumstances where cash is the only possible way for CLG-NPOs to operate, such as in particularly remote regions where financial services are unavailable, it should be used appropriately in line with international and national laws and regulations, including cash declaration and/or cash disclosure requirements to promote greater transparency and accountability of the funds. CLG-NPOs should document the decision to allow the transfer of cash, making clear why it is in the interest of the charity to do so, and the steps taken to ensure the money reaches the intended recipient.
- 4.20 Where the use of a regulated financial or payment system is not feasible, particularly for cross-border transactions into conflict-affected areas, and informal Money or Value Transfer Services (MVTs) are the most viable option, CLG-NPOs should take appropriate measures to mitigate their TF risk by selecting an MVTs with sound systems and controls for managing TF risk. CLG-NPOs should also demonstrate that it is reasonable to do so and check the legitimacy of institutions or platforms to be used before proceeding with the transaction.

Training and Staffing

- 4.21 CLG-NPOs should ensure that the governing board members and employees are informed about training and information about AML/CFT matters.
- 4.22 All governing board members, key officers and employees should:
- Attend AML/CFT training and participate in outreach events such as webinars organised by COC and the Charity Council.

financing which the Charity may refer to: <https://www.fatf-gafi.org/en/publications/Financingofproliferation/Guidance-counter-proliferation-financing.html>.

¹¹ The Singapore Terrorism Financing National Risk Assessment 2024 highlighted that digital payment tokens have emerged as a potential means for terrorist financiers to raise and move funds across borders. 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. The Charity should thus exercise additional caution if it accepts donations in virtual assets. In particular, it should only accept such donations via digital payment token service providers that are licensed by the MAS and regulated for AML/CFT.

b) Use these opportunities to:

- Gain new tips, insights and best practices to strengthen governance capabilities,
- Enhance TF risk awareness specific to the NPO sector
- Learn about methods through which the NPO sector could be abused for terrorism and TF.

4.23 CLG-NPOs should implement clear reporting channels or systems for reporting suspicious activities and transactions within the organisations.

Reporting suspicious transactions to the STRO

4.24 A CLG-NPO should lodge a STR if there is a reasonable suspicion of ML or TF activities during the course of its administration or operations. STRs provide useful information to law enforcement authorities for the detection of criminal wrongdoings.

4.25 Under the CDSA and TSOFA, it is mandatory for CLG-NPO to lodge a STR if it has:

- reason to suspect that any property represents the proceeds of, or is connected to a criminal activity;
- possession, custody or control of property or information about any transaction (or proposed transaction) relating to any property belonging to terrorists; or
- information about any proposed transaction with respect to any property belonging to any terrorist or terrorist entity.

4.26 CLG-NPOs and their employees should file the STR electronically via STRO Online Notices and Reporting platform (SONAR). For more information regarding the filing of STR and SONAR, please refer to [SPF's website](#).

No tipping-off

4.27 It is prohibited to tip off any person in connection with any on-going investigation or proposed investigation under, or for purposes of, the TSOFA and the CDSA.

Fund raising for local charitable purposes

4.28 CLG-NPOs that wish to conduct public charitable fund-raising appeals and fall under the following categories:

- Registered and exempt charities under the Charities Act 1994
- Valid permit-holders raising funds for foreign charitable purpose approved by the COC

are exempted from having to apply for a House to House and Street Collections (HHSC) licence from the Police before they raise funds in public. However, they must submit details of the public fund-raising appeal via the Charity Portal at least seven (7) working days prior to the start of the appeal.

- 4.29 HHSC are licensed by the Police under the HHSC Act except for collections by or for the abovementioned groups which are exempted. For instance, public fund-raising appeals for a charitable cause and not for the benefit of any registered or exempt charity.
- 4.30 For more information on the HHSC licence, please visit the [Singapore Police Force's website](#).
- 4.31 There may be other permits or licences from other agencies which fund-raisers need to apply for in order to carry out a specific type of fund-raising activity. To find out more, please visit [GoBusiness Singapore](#).

Fund raising for foreign charitable purposes

- 4.32 If CLG-NPOs wish to conduct any fund-raising appeal for foreign charitable purposes, the organisation must apply to the COC for a permit.
- 4.33 To apply for the permit, CLG-NPOs must submit the application at least 30 days before the commencement of the fund-raising appeal. The CLG-NPO concerned must submit the following documents in its application:
- Proof that the beneficiary is a bona fide organisation in its country;
 - Letter from the beneficiary acknowledging that fund-raising activity is being held in its name; and
 - Governing instrument of the charity or intended beneficiary.

For more information, please refer to the [Charities Portal](#).

APPENDIX A: RED FLAG INDICATORS

5.1 The red flag indicators listed below are types of activities that can be suspicious. The occurrence of one or more of these indicators may be a warning sign of unusual activities that may be indicative of ML/TF, but it does not necessarily mean that it is indeed a suspicious activity. Further investigation should be carried out if any of these indicators are present. This list is non-exhaustive.

Donor Related Indicators:

- (a) The donor or beneficiary is unwilling to provide complete information about its beneficial owners or underlying beneficiaries.
- (b) Donations are made through third parties instead of the donor himself/herself without apparent legitimate purposes.
- (c) Donor sending funds in multiple transactions in small amounts and/or involving multiple parties.
- (d) Large donations are made using a personal account or the donor makes large contributions that appear to be more than the usual amount that particular profile(s) of the donor(s) would typically make.
- (e) Unusual request for refund of donations.
- (f) Donations involving virtual assets, especially where the ownership of the virtual assets cannot be easily traced to the donor(s).
- (g) Multiple small transactions to avoid triggering identification or reporting requirements.

Beneficiary Related Indicators:

- (h) Detection of ML/TF concerns over fund raisers/volunteers or beneficiaries (e.g. from adverse news, including TF-related sanctions measures from credible authorities).
- (i) No logical purpose in the financial transactions or there appears to be no link between the stated charitable activities of the beneficiary and the parties in the transaction.
- (j) Use of funds not consistent with the organisation's purposes.
- (k) A large number of donations made through fund transfers ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements, or foreign exchange transactions performed on behalf of beneficiaries.

Funds Related Indicators:

- (l) Funds are comingled with personal or private business funds.
- (m) Multiple accounts are used to collect and channel funds to a small number of beneficiaries, particularly in high-risk terrorist areas or transactions involving foreign currency, which are subsequently transferred to high-risk terrorist areas within a short period of time.

High-risk Areas Indicators:

- (n) Use of cash couriers to transfer funds into areas with known terrorist activity.
- (o) Funds are remitted, resources transferred and/or activities carried out to/in locations which are:
 - Countries designated by national authorities; and/or
 - FATF non-cooperative countries/territories; and/or
 - Areas where terrorist entities have a substantial presence.

5.2 CLG-NPOs should also refer to the list of red flag indicators that are relevant to the non-profit sector on the [SPF's website](#).

About Accounting and Corporate Regulatory Authority

The Accounting and Corporate Regulatory Authority (ACRA) is the regulator of business registration, financial reporting, public accountants, and corporate service providers. We are responsible for developing the accountancy sector and setting the accounting standards for companies, charities, co-operative societies, and societies in Singapore. ACRA fosters a vibrant and trusted business environment that enables innovation and growth and contributes towards making Singapore the best place for business.

For more information, please visit www.acra.gov.sg

