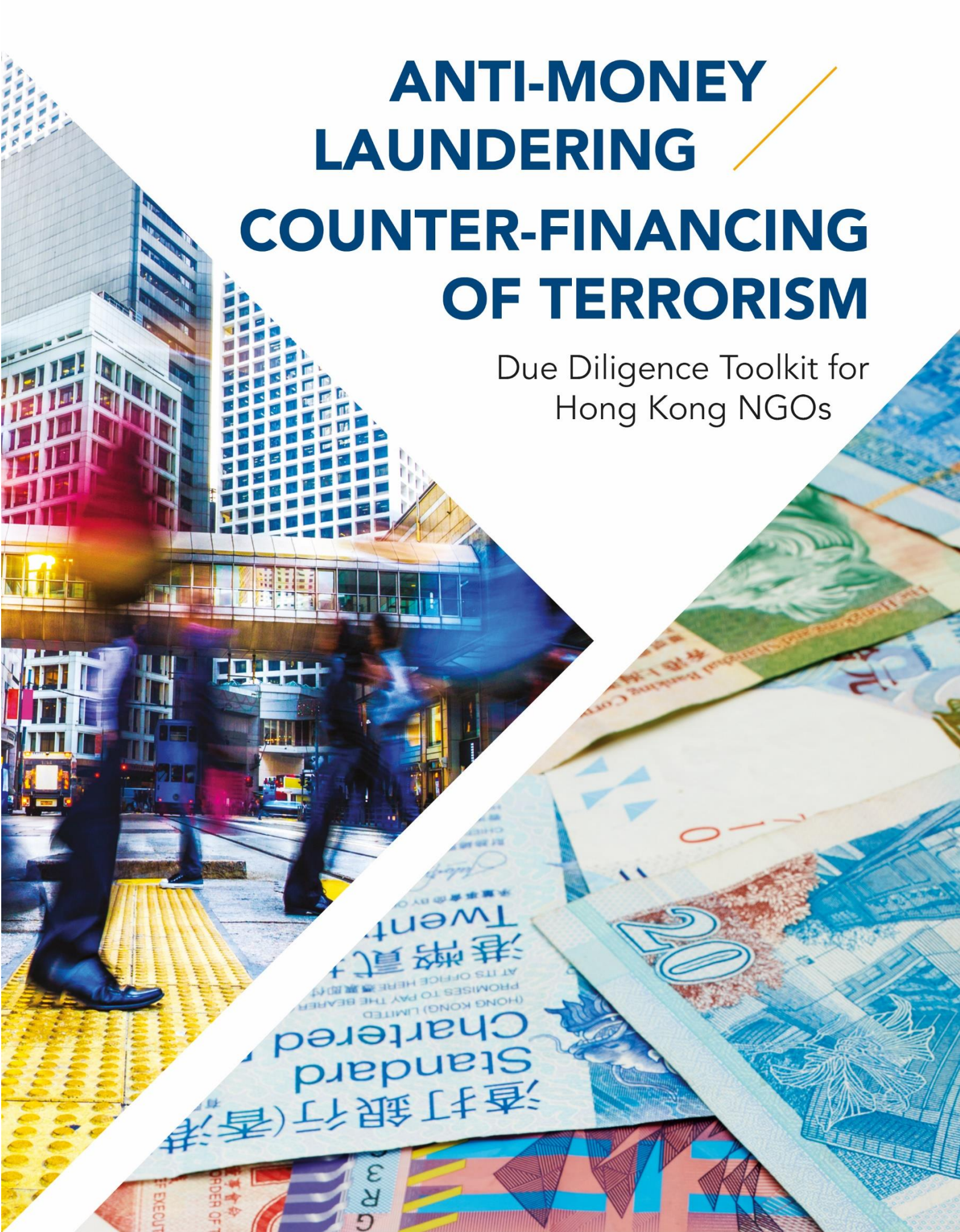


ANTI-MONEY LAUNDERING COUNTER-FINANCING OF TERRORISM

Due Diligence Toolkit for
Hong Kong NGOs



Foreword

30 June 2023

Mayer Brown and BNP Paribas have collaborated with the NGO Governance Platform Project of The Hong Kong Council of Social Service (“**HKCSS**”) to develop this Guide. The contents of this publication are intended to provide a general guide to the subject matter only and are not intended to provide legal advice or be a substitute for specific advice concerning individual situations. Readers should seek legal advice before taking any action with respect to the matters discussed herein.

Table of Contents

| | |
|---|-----------|
| CHAPTER 1 – EXECUTIVE SUMMARY | 1 |
| CHAPTER 2 – INTRODUCTION | 2 |
| CHAPTER 3 – ML/TF RISKS IN THE NGO SECTOR..... | 3 |
| CHAPTER 4 – ORGANISATIONAL INTEGRITY | 7 |
| CHAPTER 5 – RISK ASSESSMENT AND MITIGATION | 11 |
| CHAPTER 6 – REPORTING AND RECORD-KEEPING | 16 |
| CHAPTER 7 – STAFF ADMINISTRATION AND ACCOUNTABILITY | 20 |
| APPENDIX A – LIST OF AML/CFT RELATED LEGISLATIONS..... | 22 |
| APPENDIX B – GUIDELINES ON DUE DILIGENCE ACCORDING TO DIFFERENT TYPES OF DONATIONS | 28 |
| APPENDIX C – NON-EXHAUSTIVE CHECKLIST FOR IDENTIFYING AND DETECTING ML/TF RISKS | 31 |
| APPENDIX D – DUE DILIGENCE CHECKLIST ON DONORS, PARTNERS AND BENEFICIARIES..... | 34 |
| APPENDIX E – SEGREGATION OF DUTIES CHECKLIST..... | 40 |

Chapter 1 – Executive Summary

As an international financial centre, Hong Kong is at the forefront of safeguarding the integrity of the financial system by implementing international standards on Anti-Money Laundering and Counter-Financing of Terrorism ("**AML/CFT**"). A rigorous AML/CFT risk assessment framework assists organisations, including the Non-Governmental Organisations ("**NGOs**"), in complying with AML/CFT laws and guidelines.

This Guide is designed to provide a holistic overview of the latest¹ AML/CFT legal and regulatory requirements, as well as related risks and potential vulnerabilities posed to NGOs when conducting and managing charitable fundraising activities and operations in Hong Kong. The appendices include checklists and practical tips to guide NGOs on how to proactively identify and address potential money laundering ("**ML**")/terrorist financing ("**TF**") risks.

It is recommended that NGOs implement an AML/CFT risk management framework that is commensurate to the scale and scope of the NGO's practice. This means that each NGO should consider each of the best practices suggested in this Guide and decide whether it is applicable or suitable for the actual needs of that NGO. AML/CFT risk assessment is also an ongoing process, which means NGOs should carry out continuous reviews to ensure that they can live up to challenges posed by the fast-changing financial market and security landscapes in Hong Kong.

There is no one-size-fits-all AML/CFT risk assessment framework or model. While this Guide sets out general principles and recommended practices that should be considered, it is not intended to compel, or advise changes to existing practices of an NGO and should not be treated in any way as a definitive guide. There are different ways to meet the guiding principles and the recommended practices as well as the requirements of the relevant laws and regulations. Accordingly, NGOs are recommended to apply these guidelines in a way that can best serve them in the most effective and efficient manner.

In addition to this Guide, NGOs may refer to the [AML Policy Template for NGOs](#) published by PILnet Hong Kong Limited ("**PILnet**"), an NGO in Hong Kong. This AML Policy Template is specially tailored to NGOs in Hong Kong and provides a comprehensive set of policies and rules with reference to the prevailing AML/CFT requirements in Hong Kong.

¹ As at the date stated in the Foreword of this Guide.

Chapter 2 – Introduction

2.1 Background

The effectiveness of Hong Kong's AML/CFT regime enables the city to reinforce the resilience of its economy and the financial system, and enhance Hong Kong's competitiveness as a globally trusted business centre for financial institutions. Hong Kong is an active member of international AML/CFT organisations, having been a member of the Financial Action Task Force ("FATF") since 1991 and a founding member of the Asia-Pacific Group on Money Laundering since 1997². On 4 September 2019, FATF published the Mutual Evaluation Report of Hong Kong³ concluding that Hong Kong's AML/CFT regime has a robust legal foundation, effective law enforcement and an effective system for combating ML/TF. However, many NGOs, especially small-to-medium-sized NGOs, may have compliance challenges, including having limited resources to keep up with the latest legal and regulatory requirements.

2.2 Scope and objectives

Given the various challenges faced, this Guide aims to provide NGOs in Hong Kong, in particular small-to-medium-sized NGOs, with a risk assessment framework that addresses the latest AML/CFT and related requirements.

The objectives of this Guide are as follows:-

- To assist NGOs to conduct and manage their charitable fundraising activities and operations in Hong Kong, through enhancing their knowledge and understanding of ML/TF risks and potential vulnerabilities posed to NGOs in their activities.
- To enhance NGOs' understanding on the practical implications of the AML/CFT regime against the broader legal and regulatory environment in Hong Kong, and provide a practical guide for NGOs to adopt a risk-based approach that is necessary and appropriate for the scale and scope of their practices.
- To assist NGOs in keeping up with the latest legal and regulatory requirements.

In light of the above objectives, the scope of this Guide will cover the current ML/TF risks that are present in the NGO sector in Hong Kong, as well as the recommended practices and measures appropriate for NGOs to ensure any proposed measures can be effectively implemented in practice. However, even though this Guide is focused on Hong Kong, NGOs should also bear these principles in mind when there are overseas elements to their operations, especially since Hong Kong is a member of international AML/CFT organisations.

² See information available at FATF's official website: <https://www.fatf-gafi.org/content/fatf-gafi/en/countries/detail/Hong-Kong-China.html>

³ See also the Follow-up Report & Technical Compliance Re-Rating published on 17 February 2023

Chapter 3 – ML/TF Risks in the NGO Sector

3.1 Legal and regulatory environment in Hong Kong

Hong Kong is exposed to a range of ML/TF threats. Hong Kong's competitive advantages – orderly flows of capital, people, goods and information; well-established legal system; sophisticated market infrastructure; and advanced professional services also make it attractive for criminals seeking to launder and conceal criminal proceeds⁴. ML/TF risks are sometimes more difficult to detect because, for example, financial activities have become more sophisticated in the digital era. Hong Kong attaches great importance to safeguarding its financial systems and has put in place a number of legislations to underpin the implementation of a robust AML/CFT regime⁵. These include:-

- (1) Anti-Money Laundering and Counter-Terrorist Financing Ordinance ("**AMLO**") Cap. 615
- (2) Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Ordinance 2022 ("**Amended AMLO**")
- (3) Drug Trafficking (Recovery of Proceeds) Ordinance ("**DTROP**") Cap. 405
- (4) Organized and Serious Crimes Ordinance ("**OSCO**") Cap. 455
- (5) United Nations (Anti-Terrorism Measures) Ordinance ("**UNATMO**") Cap. 575
- (6) United Nations Sanctions Ordinance ("**UNSO**") Cap. 537
- (7) Weapons of Mass Destruction (Control of Provision of Services) Ordinance ("**WMDO**") Cap. 526

(collectively, the "**AML/CFT Related Legislations**")

The key provisions relating to the AML/CFT Related Legislations are summarised in **Appendix A**. AMLO and Amended AMLO differ from the other AML/CFT Related Legislations in that they apply only to financial institutions and designated non-financial businesses and professions. While these legislations are not directly applicable to NGOs, they provide a useful guide regarding due diligence and related record-keeping requirements.

It is important to note that as between AMLO and Amended AMLO, existing provisions under AMLO which have not been amended by Amended AMLO will remain in effect. The key changes made under Amended AMLO are summarised in **Appendix A**. Both ML and TF are criminal offences under the laws of Hong Kong. A person commits the offence of ML if he or she deals with any property, including money, which he or she knows or has reasonable grounds to believe it to be proceeds of drug trafficking or an indictable offence. A person commits the offence of TF if he or she provides or collects any property knowing or with the intention that the property will be used for terrorist acts.

⁴ See the [Hong Kong Money Laundering and Terrorist Financing Risk Assessment Report](#) last updated by the Financial Services and the Treasury Bureau in July 2022.

⁵ The AML/CFT Related Legislations are viewable from the [Companies Registry's website](#).

DTROP, OSCO and UNATMO also impose obligations on **all persons and entities** to report suspicious transactions if they have knowledge or suspicion that ML acts and/or criminal proceeds are involved. It is an offence (tipping off) to reveal to any person any information which might prejudice an investigation by law enforcement authorities.

Fundraising and payments made in the course of an NGO's operations may expose the organisation to risk. The Tax Guide for Charitable Institutions and Trusts of a Public Character last updated in June 2023 states that "*any institution, organisation or individual in the Hong Kong Special Administrative Region*" shall abide by the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region ("**HKNSL**"), and the laws of the Hong Kong "*in relation to the safeguarding of national security, and shall not engage in any act or activity which endangers national security.*"⁶ An NGO that is a charity may lose its tax exemption status under section 88 of the Inland Revenue Ordinance (Cap. 112) ("**IRO**") if the Inland Revenue Department ("**IRD**") considers that it supports acts or activities "*...which are unlawful or contrary to the interests of national security.*"⁷ Further, contravention of the HKNSL is a criminal offence: see **Section 4.2.2 (National security)** of this Guide and **Appendix A**.

A robust AML/CFT compliance programme will help NGOs apply appropriate due diligence, monitoring and supervision to comply with the AML/CFT Related Legislations.

3.2 The NGO sector

3.2.1 NGOs' operations and vulnerabilities to ML/TF

An understanding of the NGO sector and the associated ML/TF risks it faces are critical to the effective implementation of the AML/CFT regime within an NGO. **Section 3.2.3 (Categories of ML/TF risks)** of this Guide sets out 5 general categories of ML/TF risks for NGOs, as identified by FATF.

NGOs may be particularly susceptible to ML/TF abuse for a number of reasons. Firstly, NGOs tend to operate on a smaller scale with limited resources and/or funds for AML/CFT governance and compliance. Secondly, the nature of donation collecting and NGOs being relatively cash intensive are also risk factors. Moreover, the movement of money through an NGO may add to the complexity of a transaction or money flows, making it more difficult to spot illicit activities.

In addition, the Hong Kong Government recently identified crowdfunding as a potentially new and emerging ML/TF risk, as it could facilitate raising funds to support terrorist activities or launder proceeds of crime. Please see the Thoughts on Regulating Crowd-funding published by the Financial Services and the Treasury Bureau.

3.2.2 Nature of ML/TF threats

ML threats

⁶ Paragraph 13 of the Tax Guide for Charitable Institutions and Trusts of a Public Character, referring to Article 6 of the HKNSL.

⁷ Paragraphs 3 and 67 of the Tax Guide for Charitable Institutions and Trusts of a Public Character.

As set out in section 1 of Part 1 of Schedule 1 of AMLO, ML generally means an act that is intended to have the effect of making any property (which includes money and goods), which are proceeds obtained from the commission of (or what would have constituted) an indictable offence in Hong Kong, appear not to represent such proceeds. Simply put, it is to "wash" illegal proceeds and make them appear 'clean' and 'legitimate'.

Generally speaking, the process of ML occurs in 3 stages:-

- (1) **Placement** of money that has been obtained or derived from illegal activity;
- (2) **Layering** of the money, through different transactions and change of hands, in order to hide or disguise the real source of the money; and
- (3) **Integration**, which is where the money is re-introduced to the general financial system, now with the appearance of being derived from legitimate sources.

TF threats

TF occurs when property (usually money) is provided or collected with the intention or knowledge that the property will be used to commit terrorist acts or for the benefit of a person knowing that (or being reckless as to whether) the person is a terrorist or terrorist associate. TF can occur even if the NGO does not intend for property to be used for TF.

3.2.3 Categories of ML/TF risks

FATF identified 5 general categories of abuse of NGOs in its FATF REPORT: Risk of Terrorist Abuse in Non-Profit Organisations published in 2014:-

- (1) Diversion of funds;
- (2) Affiliation with a terrorist entity;
- (3) Support for recruitment efforts of terrorist organisations;
- (4) Abuse of programming; and
- (5) False representation.

Below is a brief description of each category:-

- (1) **Diversion of funds**

This is the most common method of abuse of NGOs, where legitimately raised funds may be diverted to terrorist entities, either by those acting within the NGO, or by external parties such as foreign partners or third-party fundraisers. This can occur at different stages of an NGO's fundraising process.

Diversion of funds by internal actors is the most common, mainly due to the position such actors have during the collection, retention and transfer stages involving NGO money. Depending on the seniority of the internal actor, or the access they may have

to the NGO's bank accounts or cash, it is relatively easier for that internal actor to have access to the legitimate funds of the NGO, and to divert or funnel those funds out.

(2) **Affiliation with a terrorist entity**

This can happen both knowingly and unknowingly, where an NGO maintains, in the course of its operations, an affiliation with a terrorist entity. The NGO may be used for purposes such as providing general logistical support to a terrorist entity, for example, (1) where internal actors in the NGO have an affiliation with terrorists, and act from the inside to influence the NGO's operations for the benefit of those terrorists; or (2) where there is a more formalised relationship between the NGO and a terrorist entity.

(3) **Support for recruitment efforts of terrorist organisations**

This is linked to category 2, and can similarly happen in an NGO both knowingly and unknowingly.

(4) **Abuse of programming**

A legitimate flow of resources, funds or information may be misused or abused at the point of delivery. An NGO may set up a legitimate project or programme, but at the point of delivery, the programme may be changed to support terrorism or other illegal activities.

(5) **False representation**

Under this category, terrorist entities will essentially trick donors into giving money, under the illusion that they are giving money to a real NGO. This may be done through the creation of "sham" NGOs, or by individuals or groups making false representations that they are agents of a legitimate NGO. This risk is even greater today, given the ease and speed with which society is now able to transfer money electronically. Furthermore, this risk is relatively harder to protect against, since this kind of activity happens outside of the NGO.

Chapter 4 – Organisational Integrity

4.1 Know your responsibilities as an NGO

NGOs are founded for the public good and entrusted with funds earmarked for the purposes of accomplishing their missions. With considerable sources of funds, whether from donors, volunteers and other sources, many NGOs' operations could be an attractive target for criminals seeking to launder proceeds of crime or finance terrorist activities. While it is difficult to weed out every bad actor within an organisation, organisational integrity can help NGOs mitigate the risks of financial crimes and in turn safeguard the public trust and confidence in the NGO sector.

4.2 Governance

Sound governance structure and robust internal systems and controls are crucial measures for NGOs to manage the risks of ML and TF.

4.2.1 Organisational structure

An NGO is led by its board, whose collective responsibility is to ensure that the NGO complies with its governing document(s) and all applicable laws and regulations. Generally, the board maintains oversight over the NGO by setting strategic plans and objectives, overseeing senior management, reviewing financial statements and performance reports, approving budgetary matters and other significant matters reserved to the board, as further described in the Guide to Corporate Governance For Subvented Organisations published by the Efficiency Office under the Innovation, Technology and Industry Bureau in June 2015.

While each NGO should take into account its size and the nature of its activities in developing its own governance structure, the overarching objective is to enhance accountability and transparency to make it difficult to misuse the NGO for ML, TF or other illegal purposes. Below are hallmarks of good corporate governance for NGOs:-

- Board structure and composition
 - The board comprises directors with diverse backgrounds who can provide stewardship and oversight.
 - The roles of chairperson and chief executive are separate and are performed by different people.
 - Directors' attendance rates for board meetings are taken into account when considering re-appointments.
- Board operation
 - There are clear guidelines/manuals on meeting proceedings (including procedures for directors to declare their interests, if any, before each meeting).

- There are procedures in place to prevent directors from approving any matters in which they have an interest.
- Minutes are properly taken at board/committee meetings and circulated to the board/committee members soon thereafter.
- Board members are provided with the agenda and other papers (e.g., financial and other periodic reports) for review in a timely manner ahead of each meeting.
- Transparency and disclosure
 - Performance measures of the organisation are periodically reviewed and disclosed to the public.
 - The organisation's finances (and the changes thereto in comparison to the previous reporting period), including reasonable details on the amount of funds raised, the donors, the amount of funds distributed, the beneficiaries and administrative and other expenses, are accurately and clearly disclosed in annual reports available to the public.
 - The organisation's directors and their biographies are disclosed to the public (e.g., on the organisation's website or in print available for public inspection).

The management team of an NGO reports, and is accountable, to the board. In order to assist the board in discharging its duty to oversee the NGO, the management team should keep the board informed of the NGO's activities, developments and other material incidents. These should include the circulation of periodic reports summarising the material events that have taken place during the reporting period and recent changes in the NGO's finances, as well as ad hoc discussions with the board or a designated board committee on pressing matters from time to time.

4.2.2 Policies, controls and procedures

Due diligence

At its core, due diligence for NGOs means knowing your stakeholders including donors, beneficiaries and partners, and adopting a risk-based approach to identify potential red flags. Each NGO should develop its own due diligence procedures/framework based on their operational needs.

A risk-based approach to conducting due diligence is necessary to ensure that the need to mitigate risks of financial crimes is balanced against different levels of risks and the resources required to carry out due diligence. For more detailed discussion on risk-based approach and due diligence, please see **Section 5.1 (Risk assessment)** and **Section 5.2 (Due diligence)** of this Guide.

National security

As noted in **Chapter 3 (ML/TF Risks in the NGO Sector)** of this Guide, an NGO that is a charity may lose its tax exemption status under section 88 of the IRO if the IRD considers that it supports acts or activities "*...which are unlawful or contrary to the interests of national security.*"⁸ Conducting appropriate

⁸ Paragraphs 3 and 67 of the [Tax Guide for Charitable Institutions and Trusts of a Public Character](#).

due diligence on, and understanding the background of, a charity's stakeholders including donors, beneficiaries and partners can help an NGO mitigate the risk of supporting activities that are contrary to the interests of national security.

Further, Article 26 of the HKNSL prohibits the provision of support, assistance or facility (which includes the provision of funds) to a terrorist organisation or a terrorist, or for the commission of a terrorist activity. Article 29 of the HKNSL prohibits receipts of funds or support from a foreign country or organisation to, among other things, provoke by unlawful means, hatred among Hong Kong residents towards the Central People's Government or the Hong Kong Government: see **Appendix A**.

Hong Kong sanctions

Certain individuals, organisations, countries and territories are subject to sanctions imposed by the United Nations. Sanctions are implemented in Hong Kong through the United Nations Sanctions Ordinance (Cap. 537) ("**UNSO**") and its subsidiary legislation. The lists of persons and entities subject to financial sanctions are available on the website of the Commerce, Industry and Tourism Branch of the Commerce and Economic Development Bureau, and the Hong Kong regulations implementing the sanctions are found at the Gazettal and Commencement of UN Sanctions Regulations ("**Sanctions Regulations**"). These lists should be checked as part of the due diligence process when dealing with external parties (e.g., to ascertain whether an NGO's significant donors, beneficiaries and partners are on the lists of sanctioned persons and entities). Pursuant to section 3(3) of UNSO, the Sanctions Regulations may prescribe the following punishments for contravention or breach: (a) on summary conviction by a fine not exceeding HKD500,000 and imprisonment for a term not exceeding 2 years; (b) on conviction on indictment by an unlimited fine and imprisonment for a term not exceeding 7 years.

Procurement

An NGO should adopt a policy for the procurement of goods and services as well as the selection of suppliers and service providers. The policy should set out the selection criteria and process, which should include obtaining quotes from a number of suppliers for internal review (and in the case of a substantial procurement or project, a competitive tender to invite bids from the public should be considered). Conflict of interest between suppliers on the one hand and any directors and employees (and their family members and affiliates) of the NGO on the other hand should be avoided. There should also be a process to evaluate current suppliers on an ongoing basis and a mechanism to change suppliers, as necessary, in the interest of the NGO.

4.2.3 Supervision and monitoring

Effective supervision and monitoring form an integral part of a robust risk management framework and ensure that internal policies, controls and procedures are adhered to and properly implemented at different levels within an NGO.

For detailed guidance on how to implement effective supervision and monitoring including segregation of duties amongst staff in an NGO, please see **Chapter 7 (Staff Administration and Accountability)** of this Guide.

4.3 Financial accountability and transparency

A sound and transparent framework for financial operations is key to enhancing accountability and transparency within an NGO, and facilitating the detection of red flags and related risks associated with the NGO's fundraising activities.

4.3.1 Collecting donations

An accurate paper trail of donations can facilitate the conduct of any investigations or audit procedures should there be any anomalies in the underlying financial and accounting records. When collecting donations, the measures recommended by the Social Welfare Department ("**SWD**") in its Guidance Note on Internal Financial Controls for Charitable Fund-raising Activities should be adopted as appropriate to enhance the integrity of the fundraising process.

The SWD's Guidance Note on Internal Financial Controls for Charitable Fund-raising Activities also contains guidelines for conducting different types of fundraising activities such as flag day, collection boxes placed in stationed counters, charity sales of commodities, solicitation of signed authorisation forms, charity walks, charity balls, concerts, variety shows and film premieres.

4.3.2 Managing payments and transactions

Banking mandate

NGOs should adopt a tiered authority for approving different amounts of payments, to reduce the risk of misappropriation of funds while minimising operational inconveniences.

NGOs may refer to Governance and Internal Control in Non-Governmental Organisations, a best practice checklist published by the Independent Commission Against Corruption ("**ICAC**").

4.3.3 Financing operations overseas

Moving funds overseas entails the risk of the money being unknowingly diverted to illegal purposes (e.g., supporting terrorist organisations). That risk is heightened when funds are funnelled outside the formal banking system, making it difficult to trace their whereabouts. It is important to make inquiries about the banking system of the countries or territories in which an NGO operates to determine whether funds can be reliably transferred to the intended recipients. Particular attention should be paid to the following circumstances:-

- Transferring funds to or through high risk countries or territories, which could lead to money being diverted before reaching the intended recipients; and
- Moving funds outside the formal banking system of the countries or territories.

Chapter 5 – Risk Assessment and Mitigation

5.1 Risk assessment

5.1.1 Risk-based approach

A risk-based approach means that an NGO should first look at its operations and activities, identify the potential risks those operations and activities may pose, and then determine what measures can be taken to address those potential risks. A risk-based approach ensures that each NGO adopts measures that match the risks that actually apply to them, rather than taking a standard approach which may not be applicable to their operations.

FATF sets out the purpose, benefits and challenges to a risk-based approach in its [Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing – High Level Principles and Procedures](#) and also its [Guidance for a Risk-Based Approach: the Banking Sector](#). According to FATF, by adopting a risk-based approach, NGOs are able to ensure that measures to prevent or mitigate ML/TF risks are commensurate to the risks identified. This will allow resources to be allocated in the most efficient way. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention. Where NGOs identify higher risks, they should ensure that their AML/CFT regime adequately addresses such risks. Where NGOs identify lower risks, they may decide to follow simplified measures.

5.1.2 Assessing risks

In the context of a risk-based approach, the assessment of risks is crucial. NGOs should first identify the relevant situation or circumstance (for example, receiving a donation), and then assess the level of due diligence (if any at all) required. NGOs should refer to **Appendix B** for the **Guidelines on Due Diligence According to Different Types of Donations**, and **Appendix C** for the **Non-exhaustive Checklist for Identifying and Detecting ML/TF Risks** in charitable fundraising and operations.

[An Advisory Guideline on Preventing the Misuse of Charities for Terrorist Financing](#) produced by the Narcotics Division of the Security Bureau also sets out the following factors to be considered in the risk assessment:-

- Nature of the activities of the donors/beneficiaries/partners;
- Target group(s) of the donors/beneficiaries/partners;
- Location of operation of the donors/beneficiaries/partners;
- Known reputation of the donors/beneficiaries/partners and their staff;
- Years of the acquaintanceship with them; and
- Publicly available information including the terrorist lists published in the government Gazette from time to time.

As noted above, NGOs need to set thresholds for conducting due diligence that is commensurate to the scale and scope of the NGO's practice, and having regard to their risk profile and risk appetite. NGOs may find it helpful to use the [AML Policy Template for NGOs](#) published by PILnet, and to update the contents to cater for their actual operations.

After the level of risk has been identified, the corresponding type of due diligence should be carried out. NGOs should refer to **Appendix D** for the **Due Diligence Checklist on Donors, Partners and Beneficiaries** as to how such due diligence may be conducted.

5.2 Due diligence

5.2.1 Overview of the “know your” principles

Due diligence is the main action NGOs can take in order to guard against ML/TF. In the financial sector, banks and other institutions have to take reasonable steps to ensure that they know who they are doing business with. For NGOs, these requirements can be summed up in the following 3 “know your” principles:

- Know your donors
- Know your beneficiaries
- Know your partners

These principles can help NGOs be assured of the provenance of their funds and that they know the people and organisations they work with, and on behalf of. NGOs should follow these principles to help ensure the charitable funds and services are not misused. To satisfy the core elements of due diligence, NGOs are encouraged to take reasonable steps, including:-

- Identify – know who you are dealing with;
- Verify – verify identities, where reasonable, and when the risks are high;
- Perform name screening against open source media or lists published by local government;
- Know what the organisation's or individual's business is and be assured it is appropriate for the NGO to be involved with;
- Know what their specific business is with your NGO and have confidence they will deliver what you want them to; and
- Watch out for unusual or suspicious activities, conduct or requests.

NGO's should first identify and assess the risk (see **Appendix B** for the **Guidelines on Due Diligence According to Different Types of Donations**, and **Appendix C** for the **Non-exhaustive Checklist for Identifying and Detecting ML/TF Risks**), and then carry out the appropriate level of due diligence (set out in the **Due Diligence Checklist on Donors, Partners and Beneficiaries** in **Appendix D**).

5.2.2 Know your donors

Most NGOs should know, at least in broad terms, where the donated money comes from. NGOs should take reasonable and appropriate steps to know who the donors are, particularly when significant sums are being donated or the circumstances of the donation give rise to notable risk or suspicion.

NGOs will benefit from effective processes that provide adequate assurances about the identity of donors and verify the identity against open source media or against lists from reliable sources. They should also have assurance on the provenance of funds and know what the donor's specific business is. This does not mean NGOs have to question every donation, nor must they know vast quantities of personal details about every donor. The process should be risk-based, meaning that the higher the risk of ML/TF is presented by the donor, the more extensive the due diligence process should be.

Please see **Appendix B** for the **Guidelines on Due Diligence According to Different Types of Donations**. NGOs should follow the guidelines and are encouraged to tailor one with proper assessment of risks involved in their own operations, such as the amount of donation, type of donation, and geographical risk. After assessing the type of due diligence to be carried out, NGOs should then refer to **Appendix D** for the **Due Diligence Checklist on Donors, Partners and Beneficiaries** as to how due diligence may be conducted.

As for anonymous donations, NGOs should have proper safeguards in place to mitigate the risk of receiving funds from illegitimate sources. **Appendix B** for the **Guidelines on Due Diligence According to Different Types of Donations** notes that small anonymous donations may be received. Larger anonymous donations may require approval by the directors or senior management. In deciding whether to accept a large anonymous donation, an NGO should take reasonable measures to attempt to ascertain the identity of the donor and/or the source of funds and take into account red flags arising from the donation (if any) to determine the level of due diligence required.

5.2.3 Know your beneficiaries

NGOs assist beneficiaries through for example: charitable activities, providing funding for others, and co-ordinating efforts to provide assistance. It is important that NGOs take reasonable steps to ensure that the funds they provide are used in accordance with the objective of the programme and not for any illicit purposes.

NGOs should conduct risk-based due diligence on the beneficiaries (see **Appendix D** for the **Due Diligence Checklist on Donors, Partners and Beneficiaries**). In addition to reasonable checks on the end-use of the donations, if financial support is provided by NGOs through a third party/partner organisation, reasonable due diligence should be carried out on that organisation as well.

If the NGOs' activities are fully accessible to members of the public and the NGOs do not choose the beneficiaries, then there is no need to check and verify their identity.

This "know your beneficiary" principle is more likely to directly affect NGOs that restrict access to services or activities to a certain number of beneficiaries. The due diligence measures as set out in the **Due Diligence Checklist on Donors, Partners and Beneficiaries** in **Appendix D** and the **Non-exhaustive**

Checklist for Identifying and Detecting ML/TF Risks in **Appendix C** should be conducted during selection of particular individuals receiving services or support from NGOs to ensure that:

- they know who those individuals are;
- the beneficiary does not present ML/TF risk or reputational or other risk to the NGOs; and
- where the risks are high, appropriate checks are carried out to ensure it is appropriate for the NGOs to provide assistance.

5.2.4 Know your partners

The “know your partner” principle applies to all close partnership, collaboration, and coordination work with other organisations, including other NGOs. Due diligence of partners is important as the duties of NGOs are not just concerned with whether charitable money actually reaches the place, people and purpose intended; their duties also involve consideration of whether a partner is appropriate and suitable for their organisation to work with.

Every partner should be subject to at least simplified due diligence measures as set out in the **Due Diligence Checklist on Donors, Partners and Beneficiaries** in **Appendix D**. In case of a partner that is also a charity or NGO, the verification process should also include cross-checking the charitable status of the organisation, such as checking the tax-exempt status under section 88 of the IRO for Hong Kong entities on the [IRD's website](#). If the partner is in a jurisdiction which regulates charities/NGOs, the relevant register should also be reviewed to check the entity's status.

The higher the risks or the more significant or substantial the work or partnership, the more steps for due diligence NGOs will need to take. NGOs should undertake enhanced due diligence if higher risk factors are identified per the **Non-exhaustive Checklist for Identifying and Detecting ML/TF Risks** in **Appendix C**. In addition, NGOs may also need to consider undertaking other forms of financial due diligence on the partner. Due diligence is also an opportunity for the NGOs to check that the partner has adequate operational capacity and capability, and that the partner fully understands the aims and parameters of the projects.

5.2.5 Due diligence guidelines

As mentioned in above sections, due diligence should be undertaken in a risk-based approach according to the risk identified on the donor/beneficiary/partner. There are 3 levels of due diligence: standard, simplified, and enhanced. The due diligence should be conducted prior to or as soon as possible when confirming the relationship with donor/beneficiary/partner. As previously mentioned, NGOs should first identify what level of due diligence should be conducted (with reference to the **Guidelines on Due Diligence According to Different Types of Donations** in **Appendix B**), and then use the **Due Diligence Checklist on Donors, Partners and Beneficiaries** in **Appendix D** in order to carry out such diligence.

NGOs should ensure that the due diligence is regularly reviewed and kept up to date. With a risk-based approach, due diligence at different risk levels could be reviewed according to different timelines. Higher risks should be reviewed more frequently (e.g., on an annual basis) than lower risks. Since the

checklists are not exhaustive, NGOs should make the appropriate adjustments to make sure that they reflect the needs of the organisations according to their actual operations.

5.3 Risk mitigation

To mitigate ML/TF risks, NGOs should have appropriate controls in place for their fundraising activities and operations. There is no “one-size-fits-all” approach to the controls, and the risk-based approach mentioned in **Section 5.1.1 (Risk-based approach)** of this Guide should be applied. Practical steps to consider include:-

Please see **Section 5.2 (Due diligence)** of this Guide and the **Due Diligence Checklist on Donors, Partners and Beneficiaries** in **Appendix D** regarding due diligence on individuals and organisations for donors, beneficiaries and partners.

- **Proper record of transactions**

Records of domestic and international payments should have enough details (particularly for large donations or disbursements; details of the donor or beneficiary should be recorded) to show that funds have been received, transferred and spent as intended. NGOs should have systems and controls in place that enable them to identify international transactions separately from domestic transactions. This will assist them to become aware of any suspicious transactions involving payments overseas, which normally have greater risks associated with ML/TF.

- **Reporting**

NGOs should have policies and procedures for making reports of suspicious transactions internally to their compliance team/officer, as well as to the authority (the Joint Financial Intelligence Unit (“**JFIU**”). Further information on internal reporting and external reporting is given in **Section 6.1 (Internal reporting)** and **6.2 (External reporting)** of this Guide, respectively.

- **Training**

NGOs should also ensure that their staff and volunteers are aware of ways in which their organisation could be used for ML/TF so they can be alert for any suspicious transactions. Training should cover the specific procedures for reporting any suspicions.

- **Record-Keeping**

NGOs should keep an audit trail of decisions made for risk assessment. NGOs should also ensure records of income and expenditure are kept, together with receipts, invoices and supporting documents. Further information on record-keeping is given in the **Section 6.4 (Record-Keeping)** of this Guide.

Chapter 6 – Reporting and Record-Keeping

6.1 Internal reporting

NGOs should establish internal reporting policies and procedures that require staff to report any information that causes them to believe or suspect that someone is engaging in ML/TF activities, to the NGOs’ compliance officer. If an NGO does not already have a compliance officer, one should be designated. Please see the [AML Policy Template for NGOs](#) published by PILnet regarding sample provisions on reporting obligations within an NGO.

Section 12 of UNATMO requires any person, including NGOs to report knowledge or suspicion of terrorist property. According to section 2 of UNATMO, “terrorist property” is defined as *“the property of a terrorist or terrorist associate; or any other property that is intended to be used to finance or otherwise assist the commission of a terrorist act; or was used to finance or otherwise assist the commission of a terrorist act”*.

An effective systematic approach to identify suspicious financial activity may safeguard NGOs from the risk of being involved with TF and ML. NGOs should consider adopting the “SAFE” approach recommended by the JFIU in identifying a suspicion as set out in [How to identify a Suspicion?](#)

| | |
|---------------------|---|
| Screen (S) | “Screen” the account for suspicious indicators |
| Ask (A) | “Ask” appropriate questions |
| Find (F) | “Find” out the customer’s records and review information already known when deciding if the apparently suspicious activity is to be expected |
| Evaluate (E) | “Evaluate” all the above information and determine if the alleged transaction is suspicious |

The compliance officer is responsible for assessing any information disclosed to determine whether it might indicate that ML or TF is being engaged in, or whether the information disclosed might give rise to a suspicion of such activities. The internal reporting policies and procedures must authorise the compliance officer to request any information required to assist in assessing the information disclosed.

6.2 External reporting

If the compliance officer determines that the information disclosed does indicate that ML/TF activities have taken place, or causes a suspicion, the procedures must specify that a suspicious transaction report (“STR”) is to be filed with the JFIU and to keep a written record of such reports. Under DTROP, OSCO and UNATMO, **failure to file an STR is a criminal offence** that is subject to a Level 5 fine (HKD50,000) and imprisonment for 3 months for the person who fails to make the disclosure of his or her knowledge or suspicion of ML/TF activities. Note a disclosure by a staff member to the appropriate person (usually

the compliance officer) in accordance with the procedure established by an NGO will satisfy his/her personal obligation to report a suspicion.

6.3 Tipping off and confidentiality

Tipping off is an offence under the laws of Hong Kong. Parties named in the STR should not be notified or otherwise be informed of any investigation or internal examination of their transactions.

A person commits an offence if, knowing or suspecting that an STR has been made, the person discloses to any other person any matter which is likely to prejudice any investigation⁹. NGO staff should be reminded that there is a risk that other parties could be unintentionally tipped off when the NGO seeks to inquire about a suspicious transaction. The maximum penalty for tipping off is imprisonment for 3 years and a fine up to HKD500,000. Please see the [Guideline on Anti-Money Laundering and Counter-Financing of Terrorism \(For Authorized Institutions\)](#) last revised in May 2023 by the Hong Kong Monetary Authority ("HKMA").

Furthermore, NGOs should provide training to their staff and volunteers on the offence of tipping off, to provide guidance on how to avoid tipping off and to explain, for example, that making enquiries, when conducted properly and in good faith, will not constitute tipping off.

6.4 Record-Keeping

Record-keeping is an essential part of the audit trail for the detection, investigation and confiscation of criminal or terrorist property or funds. An NGO should maintain due diligence information, transaction records and other records that are necessary and sufficient to meet the record-keeping requirements under this Guide, the AML/CFT Related Legislations (see **Appendix A**) and other regulatory requirements that are appropriate to the nature, size and complexity of its operation.

An NGO should ensure that:-

- the audit trail for funds moving through the NGO that relate to a donor/beneficiary/partner is clear and complete;
- all due diligence information and transaction records are recorded and/or retained; and
- adequate staff training is provided to ensure compliance with due diligence and record-keeping requirements.

Retention of records relating to due diligence and transactions

An NGO should retain the following documents in its records:-

- the original or a copy of the documents, and a record of the data and information, obtained in the course of identifying and verifying the identity of a donor/beneficiary/partner and/or persons who purport to act on behalf of the donor;

⁹ Section 12(5) of UNATMO, section 25A(5) of DTROP and OSCO respectively.

- other documents and records obtained throughout the due diligence and ongoing monitoring process, including enhanced due diligence;
- where applicable, the original or a copy of the documents, and a record of the data and information, as to the purpose and intended nature of the transaction;
- the original or a copy of the records and documents relating to the donor/beneficiary/partner's account and related correspondence; and
- the results of any analysis undertaken (e.g., inquiries to establish the background and purposes of transactions that are complex, unusually large in amount or of unusual pattern, and have no apparent economic or lawful purpose).

All documents and records mentioned above should be kept throughout the continuance of the relationship with the relevant donor/beneficiary/partner, and for a period of at least 5 years beginning on the date on which the business relationship ends¹⁰. Similarly, for occasional transactions equal to or exceeding the due diligence threshold (i.e., HKD8,000 for wire transfers and HKD120,000 for other types of transactions), an NGO should keep all documents and records for a period of at least 5 years after the date of the occasional transaction.

All documents and records mentioned should be kept for a period of at least 5 years beginning on the date on which the transaction is completed, regardless of whether the business relationship ends during that period¹¹.

If the record consists of a document, either the original or copy of the document should be retained.

Staff training

It is an NGO's responsibility to provide adequate training for its staff to implement the relevant due diligence and record-keeping requirements. The scope and frequency of training should be tailored to the specific risks faced by the NGO and pitched according to the job functions, responsibilities and experience of the staff. New staff should be required to attend initial training as soon as possible after being hired or appointed. Apart from the initial training, an NGO should also provide refresher training regularly to ensure that its staff are reminded of their responsibilities and are kept informed of new developments related to ML/TF.

An NGO should implement a clear and well-articulated policy for ensuring that relevant staff receive adequate AML/CFT training.

Staff should be made aware of:-

- the NGO's and their own personal statutory obligations and the possible consequences for failure to comply with due diligence and record-keeping requirements;

¹⁰ Section 20(3), Schedule 2 (Requirements Relating to Customer Due Diligence and Record-Keeping) of AMLO.

¹¹ Section 20(2), Schedule 2 (Requirements Relating to Customer Due Diligence and Record-Keeping) of AMLO.

- the NGO's and their own personal statutory obligations and the possible consequences for failure to report suspicious transactions;
- the NGO's policies and procedures relating to AML/CFT, including suspicious transaction identification and reporting.

The NGO should monitor and maintain records of who has been trained, when the staff has received training, and the type of the training provided.

Chapter 7 – Staff Administration and Accountability

7.1 Staff administration

Effective staff management contributes positively to the use of an NGO's resources, ensures that staff of the required qualification and experience are employed, improves staff performance and morale, and minimises opportunities for abuse.

The ICAC has published a user-friendly guide entitled Best Practice Checklist: Staff Administration which provides procedures and safeguards in relation to staff administration, including recruitment, supervision and promotion of staff, performance appraisal, and handling of staff complaints. It is highly recommended that NGOs review and implement the proposed measures and adopt any forms and templates which are appropriate to their practices.

7.2 Segregation of duties

Segregation of duties is an essential internal control in any organisation designed to reduce the risk of fraud and error. No employee or group of employees should assume conflicting duties and responsibilities within an organisation. However, segregation of duties may not be easily achieved by NGOs, where the same person may be responsible for multiple roles across different functions within the organisation. Please see the Internal Control Toolkit for Small Non-Governmental Organizations jointly issued by HKCSS and Ernst & Young.

Recognising the challenges faced by NGOs, the **Segregation of Duties Checklist** in **Appendix E** is designed to assist NGOs to evaluate the extent to which their internal control procedures for segregation of duties have been set up and complied with. For any recommended process or procedure with which the NGOs are not able to comply, it would be proper for the organisations to review their existing internal control procedures and to determine if any follow-up action is needed.

7.3 Supervisory accountability

An NGO's board needs to be open, transparent, responsive and accountable to all stakeholders, including the staff. In practical terms, the board should consider adopting the following measures in achieving supervisory accountability within the organisation:-

- Identify who the key staff are and establish procedures that foster effective communication.
- Clearly delineate the scope of duties and responsibilities of the key staff, bearing in mind the guidelines regarding segregation of duties above.

- Require the staff to properly execute their supervisory role in performing checks and reviews on the operation of the NGO in the conduct of fundraising activities, particularly in relation to major activities that are more prone to ML/TF risks (see **Chapter 3 (ML/TF Risks in the NGO Sector)** of this Guide for details).
- Require the staff to report major activities to facilitate monitoring, including statistical analyses, deliverables and any matters of concern. For detailed guidelines with respect to internal reporting, please see **Chapter 6 (Reporting and Record-Keeping)** above.

7.4 Feedback channel

A strong feedback culture facilitates staff engagement and improves staff morale within an organisation. Even if an NGO is operating on a small scale with limited resources, establishing a simple process for giving and receiving feedback amongst staff is still essential to the administration of staff and the operation of the NGO.

Appendix A – List of AML/CFT Related Legislations¹²

Legend:

- (1) Anti-Money Laundering and Counter-Terrorist Financing Ordinance ("**AMLO**") Cap. 615
- (2) Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Ordinance 2022 ("**Amended AMLO**")
- (3) Drug Trafficking (Recovery of Proceeds) Ordinance ("**DTROP**") Cap. 405
- (4) Organized and Serious Crimes Ordinance ("**OSCO**") Cap. 455
- (5) United Nations (Anti-Terrorism Measures) Ordinance ("**UNATMO**") Cap. 575
- (6) United Nations Sanctions Ordinance ("**UNSO**") Cap. 537
- (7) Weapons of Mass Destruction (Control of Provision of Services) Ordinance ("**WMDO**") Cap. 526
- (8) Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region ("**HKNSL**") and its Implementation Rules

| No. | Ordinance / Provision | Details |
|--|---|--|
| Anti-Money Laundering and Counter-Terrorist Financing Ordinance | | |
| 1. | s.1, Part 1, Sch. 1, AMLO ¹³ | The term "money laundering" (ML) is defined in section 1 of Part 1 of Schedule 1 to AMLO and means an act intended to have the effect of making any property: <ol style="list-style-type: none"> (a) that is the proceeds obtained from the commission of an indictable offence under the laws of Hong Kong, or of any conduct which if it had occurred in Hong Kong would constitute an indictable offence under the laws of Hong Kong; or (b) that in whole or in part, directly or indirectly, represents such proceeds, not to appear to be or so represent such proceeds. |
| 2. | s.1, Part 1, Sch. 1, AMLO ¹⁴ | The term "terrorist financing" (TF) is defined in section 1 of Part 1 of Schedule 1 to AMLO and means: |

¹² See the [Guideline on Anti-Money Laundering and Counter-Financing of Terrorism \(For Authorized Institutions\)](#) (Revised May 2023) by the HKMA and the [Guideline on Compliance of Anti-Money Laundering and Counter-Terrorist Financing Requirements for Licensed Money Lenders](#) (Revised June 2023) by the Companies Registry, the relevant AML/CFT provisions of which have been extracted and set out in this Appendix A.

¹³ The term "money laundering" remains unchanged under Amended AMLO.

¹⁴ The term "terrorist financing" remains unchanged under Amended AMLO.

| No. | Ordinance / Provision | Details |
|---|-------------------------------------|---|
| | | <p>(a) the provision or collection, by any means, directly or indirectly, of any property –</p> <ul style="list-style-type: none"> (i) with the intention that the property be used; or (ii) knowing that the property will be used, <p>in whole or in part, to commit one or more terrorist acts (whether or not the property is actually so used);</p> <p>(b) the making available of any property or financial (or related) services, by any means, directly or indirectly, to or for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate; or</p> <p>(c) the collection of property or solicitation of financial (or related) services, by any means, directly or indirectly, for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate.</p> |
| Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Ordinance 2022 | | |
| 3. | Key changes made under Amended AMLO | <p>Amended AMLO has introduced two new regimes:</p> <ul style="list-style-type: none"> (a) a licensing regime for virtual asset service providers; and (b) a two-tier registration regime for dealers in precious metals and stones. (c) amending the definition of “politically exposed person” (“PEP”); (d) providing a new definition of “former politically exposed person” (“Former PEP”); (e) amending the definition of “beneficial owner” in relation to a trust to include (1) a beneficiary or a class of beneficiaries of the trust entitled to a vested interest in the trust; (2) the settlor of the trust; (3) the trustee of the trust; (4) a protector or enforcer of the trust; and (5) an individual who has ultimate control over the trust. |
| Drug Trafficking (Recovery of Proceeds) Ordinance | | |
| 4. | s.25, DTROP | Under DTROP and OSCO, a person commits an offence if he deals with any property knowing or having reasonable grounds to believe it to represent any person's proceeds of drug trafficking or of an indictable offence respectively. |

| No. | Ordinance / Provision | Details |
|---|--------------------------------|--|
| | | The highest penalty for the offence upon conviction is imprisonment for 14 years and a fine of HKD5 million. |
| 5. | s.25A, DTROP | DTROP, OSCO and UNATMO also make it an offence if a person fails to disclose, as soon as it is reasonable for him to do so, his knowledge or suspicion of any property that directly or indirectly, represents a person's proceeds of, was used in connection with, or is intended to be used in connection with, drug trafficking, an indictable offence or is terrorist property respectively. This offence carries a maximum term of imprisonment of 3 months and a fine of HKD50,000 upon conviction. |
| 6. | s.25A, DTROP | "Tipping off" is another offence under DTROP, OSCO and UNATMO. A person commits an offence if, knowing or suspecting that a disclosure has been made, he discloses to any other person any matter which is likely to prejudice any investigation which might be conducted following that first-mentioned disclosure. The maximum penalty for the offence upon conviction is imprisonment for 3 years and a fine. |
| Organized and Serious Crimes Ordinance | | |
| 7. | s.25, OSCO | Please see item 4 above. |
| 8. | s.25A, OSCO | Please see items 5 and 6 above. |
| United Nations (Anti-Terrorism Measures) Ordinance | | |
| 9. | s.6, 7, 8, 8A, 13 & 14, UNATMO | UNATMO, among other things, criminalises the provision or collection of property and making any property or financial (or related) services available to terrorists or terrorist associates. The highest penalty for the offence upon conviction is imprisonment for 14 years and a fine. UNATMO also permits terrorist property to be frozen and subsequently forfeited. |
| 10. | s.11L, UNATMO | Section 11L of UNATMO prohibits any person from providing or collecting property with the intention or knowing that the property will be used, in whole or in part, to finance the travel of a person between states for the purpose of the perpetration, planning or preparation of, or participation in, terrorist acts, or the provision or receiving of terrorist training (whether or not the property is actually so used). Contraventions are subject to a maximum penalty of 7 years' imprisonment and a fine. |

| No. | Ordinance / Provision | Details |
|--|-----------------------|--|
| 11. | s.12 & 14, UNATMO | Please see items 5 and 6 above. |
| United Nations Sanctions Ordinance | | |
| 12. | s.3, UNSO | <p>The Chief Executive makes regulations under the United Nations Sanctions Ordinance, Cap. 537 (“UNSO”) to implement sanctions, including targeted financial sanctions against certain persons and entities designated by the Security Council of the United Nations (“the Security Council”).</p> <p>The Chief Executive or the Secretary for Commerce and Economic Development may, by notice published in the Gazette or on the website of the Commerce and Economic Development Bureau (https://www.cedb.gov.hk/en/policies/united-nations-security-council-sanctions.html), specify persons or entities designated by the Security Council or its Sanctions Committees for the purpose of financial sanctions, as “relevant persons” or “relevant entities”. It is an offence for any person to make available any funds or other financial assets or economic resources to or for the benefit of relevant persons or relevant entities; or to deal with any funds, other financial assets or economic resources belonging to, owned or controlled by, such persons or entities, except under the authority of a licence granted by the Chief Executive. A licensee seeking such a licence should write to the Commerce and Economic Development Bureau to apply for such a licence. Offenders will be subject to a maximum sentence of 7 years’ imprisonment and a fine.</p> |
| Weapons of Mass Destruction (Control of Provision of Services) Ordinance | | |
| 13. | s.4, WMDO | WMDO controls the provision of services that will or may assist the development, production, acquisition or stockpiling of weapons capable of causing mass destruction or that will or may assist the means of delivery of such weapons. Section 4 of WMDO prohibits a person from providing any services where he believes or suspects, on reasonable grounds, that those services may be connected to financing of proliferation of weapons of mass destruction. The provision of services is widely defined and includes the lending of money or other provision of financial assistance. |
| Law of the People’s Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region and its Implementation Rules | | |
| 14. | Article 6, HKNSL | It is the common responsibility of all the people of China, including the people of Hong Kong, to safeguard the sovereignty, unification and territorial integrity of the People’s Republic of China. |

| No. | Ordinance / Provision | Details |
|-----|-----------------------|---|
| | | <p>Any institution, organisation or individual in the Hong Kong Special Administrative Region shall abide by the HKNSL and the laws of the Region in relation to the safeguarding of national security, and shall not engage in any act or activity which endangers national security.</p> <p>A resident of the Region who stands for election or assumes public office shall confirm in writing or take an oath to uphold the Basic Law of the Hong Kong Special Administrative Region of the People’s Republic of China and swear allegiance to the Hong Kong Special Administrative Region of the People’s Republic of China in accordance with the law.</p> |
| 15. | Article 26, HKNSL | <p>A person who provides support, assistance or facility such as training, weapons, information, funds, supplies, labour, transport, technologies or venues to a terrorist organisation or a terrorist, or for the commission of a terrorist activity; or manufactures or illegally possesses substances such as explosive, poisonous or radioactive substances and pathogens of infectious diseases or uses other means to prepare for the commission of a terrorist activity, shall be guilty of an offence. If the circumstances of the offence committed by a person are of a serious nature, the person shall be sentenced to fixed-term imprisonment of not less than 5 years but not more than ten years, and shall be imposed with a criminal fine or subject to confiscation of property; in other circumstances, a person shall be sentenced to fixed-term imprisonment of not more than 5 years, short-term detention or restriction, and shall be imposed with a criminal fine.</p> <p>If the act referred to in the preceding paragraph also constitutes other offences, the person who commits the act shall be convicted and sentenced for the offence that carries a more severe penalty.</p> |
| 16. | Article 29, HKNSL | <p>A person who steals, spies, obtains with payment, or unlawfully provides State secrets or intelligence concerning national security for a foreign country or an institution, organisation or individual outside the mainland, Hong Kong, and Macao of the People’s Republic of China shall be guilty of an offence; a person who requests a foreign country or an institution, organisation or individual outside the mainland, Hong Kong, and Macao of the People’s Republic of China, or conspires with a foreign country or an institution, organisation or individual outside the mainland, Hong Kong, and Macao of the People’s Republic of China, or directly or indirectly receives instructions, control, funding or other kinds of support from a foreign country or an institution, organisation or individual outside the mainland, Hong Kong, and Macao of the People’s</p> |

| No. | Ordinance / Provision | Details |
|-----|--|--|
| | | <p>Republic of China, to commit any of the following acts shall be guilty of an offence:</p> <ol style="list-style-type: none"> (1) waging a war against the People’s Republic of China, or using or threatening to use force to seriously undermine the sovereignty, unification and territorial integrity of the People’s Republic of China; (2) seriously disrupting the formulation and implementation of laws or policies by the Government of the Hong Kong Special Administrative Region or by the Central People’s Government, which is likely to cause serious consequences; (3) rigging or undermining an election in the Hong Kong Special Administrative Region, which is likely to cause serious consequences; (4) imposing sanctions or blockade, or engaging in other hostile activities against the Hong Kong Special Administrative Region or the People’s Republic of China; or (5) provoking by unlawful means hatred among Hong Kong residents towards the Central People’s Government or the Government of the Region, which is likely to cause serious consequences. <p>A person who commits the offence shall be sentenced to fixed-term imprisonment of not less than 3 years but not more than ten years; a person who commits an offence of a grave nature shall be sentenced to life imprisonment or fixed-term imprisonment of not less than ten years.</p> <p>The institution, organisation and individual outside the mainland, Hong Kong, and Macao of the People’s Republic of China referred to in the first paragraph of this Article shall be convicted and punished for the same offence.</p> |
| 17. | s.5, Sch.3, Implementation Rules for Article 43 of the HKNSL | <p>Disclosure of knowledge or suspicion that property is offence related property etc.</p> <ol style="list-style-type: none"> (1) Where a person knows or suspects that any property is offence related property, then the person must disclose to a police officer the information or other matter— <ol style="list-style-type: none"> (a) on which the knowledge or suspicion is based; and (b) as soon as is reasonably practicable after that information or other matter comes to the person’s attention. [...] |

Appendix B – Guidelines on Due Diligence According to Different Types of Donations

The following are examples of factors that NGOs may take into account when determining the thresholds for due diligence undertaken:-

1. Small and regular donation – No due diligence

- Some donors give relatively small amounts of money as a one-off donation, by cheque, bank transfer or cash, as opposed to significant funds, from fundraising events in public cash collections, such as charity runs, and through charity boxes or flag selling. NGOs are not expected to know the identity, or take steps to find out the identity of each small cash donor in these sorts of circumstances. This would not be reasonable or necessary.
- Some individuals and organisations will donate regularly to the NGO and set up regular payments through direct debits. NGOs will already have the name, address and details of those donors and their bank details to collect the money. Therefore, it is unlikely that NGO will need to take any further steps in such cases.
- NGOs may also receive small anonymous donations without knowing the identity of the donor or the source of funds¹⁵.

2. Donation from lower risk entity – Simplified due diligence

- Simplified due diligence may be applied to certain entities which have lower risk or are already under authority monitoring, without the need to conduct due diligence on its beneficial owners¹⁶ or senior management officials. Please see **Appendix D** for the **Due Diligence Checklist on Donors, Partners and Beneficiaries** setting out the simplified due diligence process.
- The following entities may be considered for simplified due diligence in the absence of any other high risk indicators:-
 - a financial institution as defined in AMLO¹⁷;
 - an institution that:-
 - is incorporated or established in a non-high risk jurisdiction¹⁸;

¹⁵ See also **Section 5.2.2 (Know your donors)** of this Guide.

¹⁶ See the amended definition of "beneficial owner" in relation to a trust set out in item 3 of Appendix A of this Guide.

¹⁷ Pursuant to AMLO, a "financial institution" includes: (1) an authorised institution (as defined in the Banking Ordinance); (2) a licensed corporation (which is granted a licence by the SFC); and (3) an authorised insurer.

¹⁸ See FATF's [Jurisdictions under Increased Monitoring - 23 June 2023](#) and [High-Risk Jurisdictions subject to a Call for Action - June 2023](#) for those jurisdictions which have been identified as lacking appropriate AML/CFT laws and regulations, and the lists of persons, entities and countries that are subject to financial sanctions to help identify high risk jurisdictions, which are available on the website of the [Commerce, Industry and Tourism Branch of the Commerce and Economic Development Bureau](#).

- has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2 of AMLO; and
- is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the regulatory authorities;
 - the Government or any public body in Hong Kong;
 - the government of a non-high risk jurisdiction or a body in a non-high risk jurisdiction that performs functions similar to those of a public body;
 - a charitable institution as defined in the laws of and subject to governmental regulation in any jurisdiction which is not a high risk jurisdiction¹⁹; and
 - well-established companies which are listed on the Hong Kong or other equivalent stock exchange with clear company structure and audited financial report.

(Note: This is subject to risk-based approach and the assessment for simplified due diligence should be documented properly.)

3. Large donation and corporate donor – Standard due diligence

- Some donors give significant grants to NGOs, with whom they may have a close working relationship. It is important to carry out further due diligence and take steps to verify the identity of the donor to assess any risks.
- If the significant donor is an organisation, NGOs should know what its business is and be assured that the organisation is appropriate for the NGOs to be involved or linked with. NGOs should perform standard due diligence (see **Appendix D** for the **Due Diligence Checklist on Donors, Partners and Beneficiaries**) to understand the source of wealth, identify the ultimate beneficial owner and undertake company search, open source media search and screening.
- If the individual donor is or is closely connected to a Former PEP (see item 4 of Appendix C for the meaning of a Former PEP), such donor should be treated as posing relatively low ML/TF risks and standard due diligence should usually be sufficient.
- If the individual donor is carrying on the business of dealing in precious metals and stones in Hong Kong and engaging in transactions at or above HK\$120,000 (cash or non-cash), NGOs are reminded to check and ensure that such person is registered with the Commissioner of Customs and Excise.
- In addition, NGOs are reminded to assess how reliable the information is during an open source search. For example, has the information been proven? How old is the information?
- Standard due diligence for individual donors should be also performed. The due diligence process would be similar to the corporate one, with focus on the true identity of the donor.

¹⁹ See footnote 18 above for identifying high risk countries.

- Standard due diligence should also be performed on an individual donor who is engaging in the virtual asset exchange business. NGOs should check and ensure that such person is licensed by the Securities and Futures Commission.
- NGOs are encouraged to set the monetary threshold for standard due diligence according to the situation of the organisation.

4. Higher risk factors/situations – Enhanced due diligence

- When NGOs identify a higher risk factor, enhanced due diligence should be undertaken to assess the risks. Examples of higher risk indicators are set out in the **Non-exhaustive Checklist for Identifying and Detecting ML/TF Risks** in **Appendix C**.
- If any higher risk factor is identified, the case should be escalated to the compliance officer or other relevant official or management for further assessment. Please see **Appendix D** for the **Due Diligence Checklist on Donors, Partners and Beneficiaries** setting out the enhanced due diligence process.
- If the individual donor is or is closely connected to a PEP (see item 4 of **Appendix C** for the meaning of a PEP), such donor should be treated as posing high ML/TF risks and enhanced due diligence should generally be required.

Appendix C – Non-exhaustive Checklist for Identifying and Detecting ML/TF Risks

The non-exhaustive list below indicates examples of situations where NGOs may face higher ML/TF risks²⁰:-

| Situation | ML/TF Risk |
|---|--|
| 1. Donations | <ul style="list-style-type: none"> • Donations above certain threshold²¹. • Unusual or substantial one-off donations or a series of smaller donations or interest-free loans from sources that cannot be identified or checked by the NGOs. • Donation from a known donor but which comes through an unknown party or unusual payment mechanism (e.g., a donation made using a large number of fund transfers in small amounts, perhaps to avoid triggering reporting requirements). |
| 2. Conditions that come with donations | <ul style="list-style-type: none"> • Conditions are attached to a donation such that an NGO would merely be a vehicle for transferring funds from one individual or organisation to another, without serving any other role. • A donation is provided to the NGO to keep for a certain period of time, perhaps with the attraction of being able to keep any interest earned whilst holding the money, but the principal sum is requested to be returned at the end of the period. • A donation is provided in a foreign currency, and with unusual conditions attached on the usage, including a requirement that the original sum is to be returned to the donor in a different currency. • A donation is conditional on particular individuals or organisations being used to do work for the NGO where the NGO has concerns about those individuals or organisations. • A donation is conditional on being applied to benefit particular individuals either directly or indirectly. • NGO is asked to act as a conduit for the passing of a donation to a second body which may or may not be another NGO. |

²⁰ See also Appendix A of the [AML Policy Template for NGOs](#) published by PILnet.

²¹ NGOs should assess the threshold that is appropriate according to its size, risk appetite, scale of operations etc. by adopting a risk-based approach as outlined in **Section 5.1.1 (Risk-based approach)** of this Guide. NGOs may also refer to the [AML Policy Template for NGOs](#) published by PILnet.

| Situation | ML/TF Risk |
|--|---|
| | <ul style="list-style-type: none"> • NGO is asked to provide services or benefits on favourable terms to the donor or a person nominated by the donor. • NGO is asked by a donor to engage in specific work and/or deliver work product for the exclusive use of the donor, particularly in cases where that work is outside NGO's area of focus. |
| <p>3. Suspicious or missing details</p> | <ul style="list-style-type: none"> • Beneficiaries with identical characteristics and addresses or multiple identical or similar names and signatures. • Fake or suspicious identity documents of beneficiary. • Evidence that third parties have demanded payment for recommending or nominating beneficiaries. • The project proposal is vague or lacks adequate financial or technical details. • The structure or nature of the proposed project makes it difficult to identify the partner and verify their identity and details. • It is difficult to contact the partner at their main address, or their telephone numbers are not working, or the partner always insists upon contacting the NGO and not the other way round. • The project involves unusual payment mechanisms, or requests for cash, or for money to be paid into an account not held in the name of the partner, or in a country in which the partner is not based and not where the project is being carried out. • Donors/beneficiary/partners request unnecessary or unusual levels of privacy and secrecy. |
| <p>4. Other High Risk Indicators</p> | <ul style="list-style-type: none"> • Any nexus to a high risk country, including the location or residential address of donor/beneficiary/partner, or the source of donation, or the application of charitable fund in a high risk country²². • The source of wealth is unclear, and/or not commensurate with the background or profile of donor. • The source of wealth of donor or his or her close connection (i.e., family members) is derived from higher ML risk industry (e.g., money service provider, casino, cryptocurrency, etc.) |

²² See footnote 18 above for identifying high risk countries.

| Situation | ML/TF Risk |
|-----------|--|
| | <ul style="list-style-type: none"> • The donor or partner is or is closely connected to a PEP²³; this would be particularly high risk if the underlying PEP position is connected with a high risk country for corruption²⁴ but in view of the new definition of a Former PEP²⁵ under Amended AMLO, a donor or partner that is or is closely connected to a Former PEP should be treated as posing lower ML/TF risks as compared to a PEP and standard due diligence should usually be sufficient (see item 3 of Appendix B). • The donor, partner or beneficiary is or is closely connected with an individual or entity on a sanctions list. • The donor, partner or beneficiary is subject to any material adverse news: see Appendix D for suggested search terms to identify adverse news from open sources. • The donor, partner or beneficiary is associated with activities which could be considered to fall under the HKNSL. • The donor, partner or beneficiary is associated with any political group (local or overseas). • The donor or partner has an unusual complex ownership structure or unknown ultimate beneficiary owner. |

²³ “Politically Exposed Person” (PEP) has a fairly complicated definition set out in s.1(1), Part 1, Sch. 2 of Amended AMLO. In short, it generally refers to an individual who is or has been entrusted with a prominent public function in a place outside Hong Kong. Examples include a head of state, a head of government, a senior government, judicial or military official or an important political party official.

²⁴ See footnote 18 above for identifying high risk countries.

²⁵ “Former Politically Exposed Person” (Former PEP) also has its definition set out in s.1(1), Part 1, Sch. 2 of Amended AMLO. In short, it generally refers to an individual who has been but is *not* currently entrusted with a prominent public function in a place outside Hong Kong and is therefore no longer a PEP.

Appendix D – Due Diligence Checklist on Donors, Partners and Beneficiaries²⁶

| | Identification | Verification |
|---|---|---|
| A. Standard Due Diligence | | |
| 1. Identification and verification | | |
| Individuals | | |
| i) Hong Kong residents ii) Non-Hong Kong residents | i) Full name; ii) Date of birth; iii) Identity document number/travel document number; and iv) Residential address. | Address proof by letter issued from an official institutions (e.g., utility bill, bank statement, letters from government or financial institutions) dated within the last 3 months; and Hong Kong identity card; or i) a valid passport/travel document ; ii) a national (i.e., Government or State-issued) identity card bearing the photograph of the natural person; or iii) a valid national (i.e., Government or State-issued) driving licence incorporating photographic evidence of the identity of the natural person. |
| Corporations and institutions | | |
| i) Hong Kong incorporated companies ii) Overseas companies | i) Full legal name and trading name; ii) Place and date of incorporation, establishment or registration; iii) Unique identification number; | Searches on Hong Kong Companies Registry. Documents from a reliable and independent source (e.g., certificate of incumbency) |

²⁶ These due diligence guidelines are based on the [Guideline on Anti-Money Laundering and Counter-Financing of Terrorism \(For Authorized Institutions\)](#) last revised in May 2023 by HKMA, and the [Frequently Asked Questions in relation to Anti-Money Laundering and Counter-Financing of Terrorism](#) from the Hong Kong Association of Banks last updated on 5 October 2022.

| | Identification | Verification |
|---|--|---|
| | iv) Registration address; v) Business address in Hong Kong; vi) Nature/type of business; vii) Full name of ultimate beneficial owner ²⁷ and its intermediary shareholders. (with ownership chart if organisation structure is complicated); and viii) If there is no natural person who is a beneficial owner, NGOs should identify at least 2 senior management officials such as chief executive officer, managing or executive director, president, or natural person(s) who has significant authority over the entity's operations. | <ul style="list-style-type: none"> The related individuals (e.g., beneficial owner and senior management official) should be verified according to procedure set out above for "individuals". Financial institutions, government bodies, charitable institutions and well-established listed companies upon assessment are subject to simplified due diligence without the need to conduct due diligence on its beneficial owners or senior management officials. |
| iii) Charitable institutions | i) Generally follow the process set out for corporations and institutions above; and ii) Cross-check the identity e.g., unique identification number as charitable institution. | List of charitable institutions with tax-exempt status under section 88 of the IRO for Hong Kong entities. <ul style="list-style-type: none"> If the partner is in a jurisdiction that regulates charities/NGOs, the relevant register should be reviewed to check the entity's status. |
| 2. Name/country screening | | |
| Name screening - <u>Lists issued by governments</u> | i) Security Council of the United Nations; and ii) (Recommended) the People's Republic of China ²⁸ and other major nations or regions, such as the <u>United States</u> , <u>European Union</u> and the <u>United Kingdom</u> . | |

²⁷ Frequently Asked Questions in relation to Anti-Money Laundering and Counter-Financing of Terrorism issued by the Hong Kong Association of Banks and last updated on 5 October 2022.

²⁸ The government of the People's Republic of China has not published any accumulative list or search platform in relation to entities/individuals whose names are identified under the restrictive measures regime in the People's Republic of China. The

| | Identification | Verification |
|--|---|--------------|
| | <ul style="list-style-type: none"> Any true match against the lists at sub-section i) and ii) above should be escalated to the compliance officer or other relevant official or management. If an NGO decides to continue its relationship or activities with the hit individual/entity, enhanced due diligence should be undertaken with proper assessment and documentation. Any (potential) true hit of United Nations Security Council list at sub-section i) should be reported to the JFIU by filing an STR. Please see Chapter 6 (Reporting and Record-Keeping) of this Guide for the details on filing an STR. Connected parties, including beneficial owners, intermediary shareholders, should be also subject to screening. For individual donors whose source of wealth is from family or inheritance, name screening should be conducted on his/her family members, i.e., parents, grandparents. | |
| Name screening - adverse news/public information | <p>Search at open source media with search strings, for example:-</p> <p>i) "(Name of individual)" AND "BRIBERY" OR "BRIBE" OR "CORRUPT" OR "FACILITATION PAYMENT" OR "GREASE PAYMENT" OR "QUID PRO QUO" OR "CORRUPTION" OR "KICKBACK" OR "GRATIFICATION" OR "INDUCEMENT" OR "COURT CASE" OR "MONEY LAUNDERING" OR "DIRTY MONEY" OR "SANCTIONS" OR "CRIME" OR "CRIMINAL" OR "ARREST" OR "DRUG" OR "TERRORIST" OR "FRAUD" OR "EMBEZZLE" OR "ALLEGATION" OR "PEP" OR "POLITICAL" OR "PUBLIC OFFICIAL";</p> <p>ii) "(Name of entity)" AND "BRIBERY" OR "BRIBE" OR "CORRUPT" OR "FACILITATION PAYMENT" OR "GREASE PAYMENT" OR "QUID PRO QUO" OR "CORRUPTION" OR "KICKBACK" OR "GRATIFICATION" OR "INDUCEMENT" OR "COURT CASE" OR "MONEY LAUNDERING" OR "DIRTY MONEY" OR "SANCTIONS" OR "CRIME" OR "CRIMINAL" OR "ARREST" OR "DRUG" OR "TERRORIST" OR "FRAUD" OR "EMBEZZLE" OR "ALLEGATION".</p> <ul style="list-style-type: none"> Any true hit of adverse news which is considered material should be escalated to the compliance officer or other relevant official or | |

Ministry of Foreign Affairs and its spokespersons release announcements and/or remarks from time to time containing measures against certain entities/individuals. Reference can be made to the column entitled "Spokesperson's Remarks" (發言人表態) at the official website of the Ministry of Foreign Affairs: https://www.fmprc.gov.cn/web/fyrbt_673021/ which sets out the Chinese text of the regular press conferences and spokespersons' remarks in chronological order. For a quick reference as a starting point, an NGO may consider searching possible names within the Wikipedia article entitled 「[中華人民共和國的制裁](http://www.pbc.gov.cn/fanxiqianju/135153/135267/index.html)」. <http://www.pbc.gov.cn/fanxiqianju/135153/135267/index.html>

| | Identification | Verification |
|---|--|--|
| | | <p>management. If an NGO decides to continue its relationship or activities with the hit individual/entity, enhanced due diligence should be undertaken with proper assessment and documentation.</p> <ul style="list-style-type: none"> The above search strings are just for reference; NGOs should customise their own search strings for the relevant individual or entity. |
| Name screening - Politically Exposed Person ("PEP") | <p>Search at open source media with keyword "PEP", "Political" or "Public official", or include the keyword in the adverse news search strings set out above.</p> <ul style="list-style-type: none"> Any true hit of a PEP should be escalated to the compliance officer or other relevant official or management. If the NGO decides to continue its relationship or activities with the hit individual/entity, enhanced due diligence should be undertaken with proper assessment and documentation. | |
| Country screening | <p>Required under Hong Kong law:</p> <p>i) Check for any sanctions and embargo restrictions imposed by Security Council of the United Nations, as implemented through Hong Kong regulations under UNSO, found at the Gazettal and Commencement of UN Sanctions Regulations. Breach of such regulations may constitute a criminal offence.</p> <p>Recommended – check the following:</p> <p>i) the People's Republic of China (see the section entitled Risk Warning and Financial Sanction (風險提示與金融制裁) at the official website of the Anti-Money Laundering Bureau of People's Bank of China), and other major nations or regions, such as United States (see the Sanctions Programs and Country Information by Department of the Treasury), European Union (see the EU Sanctions Map offering easily accessible information on all EU restrictive measures regimes currently in place) and United Kingdom (see the financial sanctions targets by regime from Office of Financial Sanctions Implementation);</p> <p>ii) FATF list of High-risk and other monitored jurisdictions;</p> <p>iii) Basel AML Index by The Basel Institute on Governance; and</p> <p>iv) Transparency International's 2022 Corruption Perceptions Index.</p> <p>If NGOs are participating in humanitarian projects involving a sanctioned country and region, they are advised to check if there is any general</p> | |

| | Identification | Verification |
|------------------------------------|---|--------------|
| | licence or exclusion term in the sanctions regulation for such humanitarian projects, which will be helpful to facilitate any related transactions with financial institutions. | |
| 3. Others | | |
| Other information | Understand and identify the business nature of the entity, the source of wealth of the individual or any particular purpose of donation. This information is helpful for NGOs to decide if it is appropriate to be involved with that business/industry section from a reputational perspective. | |
| B. Simplified Due Diligence | | |
| Requirements | The simplified due diligence process is basically similar to the standard due diligence process, without the need to conduct due diligence (including the identification and verification) on the beneficial owners or senior management officials of the entity. | |
| C. Enhanced Due Diligence | | |
| Requirements | <p>Under the risk-based approach, different additional measure should be applied under different situation, which may include:-</p> <ul style="list-style-type: none"> • Obtaining additional company documents, e.g., registration documents, documents showing the ultimate beneficial owner, in order to understand the company structure and thoroughly identify ultimate beneficial owner; • Certification of documents by a notary, lawyer or accountant; • Obtaining additional documents on an individual's source of wealth²⁹, e.g., bank statements, audited financial accounts. If the source of wealth is from family member or inheritance, NGOs should thoroughly understand the background and affiliations, such as identify parents or grandparents and conduct proper searches and screening. Where appropriate, NGOs may seek evidence from a reliable, independent source that can corroborate the gist of the source of wealth information (e.g., publicly available property registers, land registers, asset disclosure registers or company registers); and • Meeting the donor/beneficiary/partner in person. | |

²⁹ NGOs may refer to point 52 and Appendix 1 of the [Frequently Asked Questions in relation to Anti-Money Laundering and Counter-Financing of Terrorism](#) issued by the Hong Kong Association of Banks last updated on 5 October 2022.

| | Identification | Verification |
|--|---|--------------|
| | <p>NGOs should come up with a feasible mitigation control before deciding to commence or continue any relationship which may present material risk. Proper level of approval, e.g., from the compliance officer or senior management, should be obtained with proper documentation.</p> | |

Appendix E – Segregation of Duties Checklist

| Key Areas | Action Checklists | Is your NGO complying? | |
|--|---|------------------------|--|
| | | Yes/ No | If no, what are the follow-up actions? |
| 1. Segregation of duties³⁰ | | | |
| 1.1 | Duties are segregated among different people to maintain check and balance. Responsibilities for authorising transactions, accounting and recording transactions and handling the related asset (custody) are divided. To the extent possible, one person should not undertake roles that overlap across these functions within an NGO. | | |
| 1.2 | Perform periodic reviews or internal audits, as appropriate, on important processes, particularly those performed by a single staff member. Conduct internal audits on major operations if resources permit. | | |
| 1.3 | Perform reconciliation between similar records maintained by different staff to ensure consistency and accuracy. | | |
| 1.4 | Establish policies, procedures, and manuals that provide guidance to ensure consistent performance at a required level of quality. Such documentation should be available at all levels of the organisation. | | |
| 1.5 | Provide periodic training to staff to ensure there is proper understanding of the relevant processes and policies in place relating to segregation of duties. | | |
| 2. Purchasing and payments | | | |
| 2.1 | Staff handling purchasing and receiving of goods/services should be separate, where possible to prevent staff from gaining access to goods improperly ordered. | | |
| 2.2 | Staff handling payments are to be separated to the extent possible with regard to:- | | |

³⁰ See the [Internal Control Toolkit for Small Non-Governmental Organizations](#) jointly issued by HKCSS and Ernst & Young in 2020.

| Key Areas | Action Checklists | Is your NGO complying? | |
|--|---|------------------------|--|
| | | Yes/ No | If no, what are the follow-up actions? |
| | a. initiation of purchase requisition; b. approval of vouchers and invoices; c. preparation of cheques and recording of payments; and d. signing of cheques | | |
| 3. Bank accounts handling | | | |
| 3.1 | There should be segregation of duties involving the mailing of cheques to reduce the risk of theft or alterations. | | |
| 3.2 | Cheques should be mailed by someone other than the person preparing them. | | |
| 4. Payroll and remuneration | | | |
| 4.1 | Duties should be segregated as to the payroll function for preparation and payments. | | |
| 4.2 | Staff preparing the payroll should not be the same staff paying out the salaries. | | |
| 4.3 | Cash payment for salaries should be avoided. | | |
| 5. Revenue and receipt transactions | | | |
| 5.1 | Duties should be segregated for staff in charge of receiving purchases and those making requisitions. If this is not possible, the supervisor or board member must be more involved in checking the staff work. | | |