Hong Kong Institute of
Certified Public Accountants
香港會計師公會

July 2017

CONSULTATION DRAFT

Guidelines on

Anti-Money Laundering

and

Counter-Terrorist Financing for Professional Accountants

CONTENTS

Page

CONTENTS

Page

SUMMARY OF MAIN REQUIREMENTS

The matters set out in this summary reproduce the paragraphs in bold typeface from the more detailed sections below. These are essential principles which need be taken on board for compliance with the legal requirements in Hong Kong, and the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, issued by the Financial Action Task Force, more commonly referred to as the FATF Recommendations. They are brought together here for the convenience of members of the Institute and to aid clarity. While there is some degree of flexibility in applying the detailed sections of these Guidelines, the Guidelines should be read in conjunction with, and understood in the context of, relevant provisions of the law. Subsection 1.2 of these Guidelines deals with their scope and application and members should view the following principles with that in mind. Members should, however, take the time to read and understand the Guidelines in their entirety.

Section 2: <u>AML/CFT POLICIES, PROCEDURES AND CONTROLS</u>

Practices should develop and implement anti-money laundering/combating the financing of terrorism (AML/CTF) internal policies, procedures and other controls to address ML/TF concerns and compliance with the existing legal requirements on AML/CFT; and, more generally, to safeguard themselves against the legal and reputational risks of being found to be involved in facilitating ML/TF or not reporting known or suspected ML/TF activities. Practices should communicate these policies and procedures clearly to employees.

Internal controls should cover:

(a) Risk assessment and management
(b) Customer due diligence
(c) Record keeping
(d) Suspicious transaction reports
(e) Ongoing employee training programme
(f) Compliance management arrangements, including the appointment of a compliance officer at the management level
(g) Hiring, e.g., an adequate screening procedures to ensure high standards when hiring employees
(h) An independent audit function, to test the system
(i) Group policy, where appropriate.

Section 3: <u>CUSTOMER DUE DILIGENCE</u>

Where applicable, practices should carry out the following customer due diligence measures:

(a) identify the client and verify the client's identity using documents, data or information provided by a government body or other reliable, independent source;

(b) where there is a beneficial owner in relation to the client (subject to certain limited exceptions), identify and take reasonable measures to verify the beneficial owner's identity, so that the practice is satisfied that it knows who the beneficial owner is, including in the case of a legal person or trust, measures to enable the practice to understand the ownership and control structure of the legal person or trust;

(c) understand and as appropriate, obtain information on the purpose and intended nature of the business relationship (if any) to be established with the practice;

(d) if a person purports to act on behalf of the client:
- **(i) identify the person and take reasonable measures to verify the person's identity using documents, data or information provided by a government body or other reliable and independent source; and**
- **(ii) verify the person's authority to act on behalf of the client;**

(e) practices should adopt enhanced due diligence measures in relation to high-risk clients (including foreign "politically exposed persons"); and

(f) may adopt simplified due diligence measures in certain specified circumstances.

Section 4: <u>ONGOING MONITORING</u>

Effective ongoing monitoring is vital for understanding clients' business and an integral part of effective AML/CFT controls. It helps practices to know their clients and to detect unusual or suspicious activities.

Where applicable, practices should monitor their business relationships with clients by:

(a) reviewing from time to time documents, data and information relating to the client to ensure that they are up to date and relevant;

(b) paying attention to the business activities of clients to ensure that they are consistent with what the practice understands to be the nature of business, the risk profile and source of funds. An unusual activity may be in the form of one that is inconsistent with the expected pattern for that client, or with the normal business activities for the type of product or service that is being delivered; and

(c) identifying activities that are complex, involve large sums or unusual or patterns of activities that have no apparent economic or lawful purpose and which may indicate ML/TF.

Section 5: MAKING SUSPICIOUS TRANSACTION REPORTS

The Organised and Serious Crimes and Drug Trafficking (Recovery of Proceeds) Ordinances contain a requirement (section 25A) require a person to report if he/she knows or suspects any property to be the proceeds of an indictable offence or drug trafficking, respectively. The United Nations (Anti-Terrorism Measures) Ordinance (section 12(1)) requires a person to report if he/she knows or suspects that any property is terrorist property.

Once knowledge or suspicion of an ML/TF transaction or activity has been established, the following general principles should be applied:

(a) Practices should make a report to an authorised officer or the Money Laundering Reporting Officer designated by his/her employer, even where no service has been provided by the practice;

(b) the report should be made as soon as is reasonably practical after the suspicion or knowledge is first established; and

(c) practices should ensure that they have in place internal controls to prevent any partner, director, or employee committing the offence of "tipping off" the client, or any other person who is the subject of the report. Practices should also take care that their line of enquiry with clients is such that tipping off cannot be construed to have taken place.

Section 6: FINANCIAL SANCTIONS AND TERRORIST FINANCING

In relation to financial sanctions and the financing of terrorism/ proliferation of weapons of mass destruction, practices should be aware of and comply with their legal obligations under Hong Kong's financial sanctions regime, which may include considering the need to make STRs.

Section 7: RECORD-KEEPING

Where applicable, practices should prepare, maintain and retain documentation and records on their business relations with, and transactions for, clients that are necessary and sufficient to achieve the record-keeping objectives indicated below and fulfil any related legal or regulatory requirements, and which are appropriate to the scale, nature and complexity of their businesses. The information maintained should be sufficient is to ensure that:

(a) any client and, where appropriate, the beneficial owner of the client, can be properly identified and verified;

(b) the audit trail for particular transactions and properties dealt with by a practice that relates to any client and, where appropriate, the beneficial owner of the client, is clear and complete;

(c) the original or suitable copies of all relevant client and transaction records and information are available on a timely basis to the Institute or other relevant authority, upon appropriate authority; and

(d) practices are able to show evidence of compliance with any relevant requirements specified in other sections of these Guidelines (e.g., relating to client identification, verification and risk assessments, internal reports and suspicious transaction reports, and training).

(e) records in relation to particular transactions and clients should be retained for six years after the transaction has been completed or the business relationship has ended, respectively.

Section 8: STAFF HIRING AND TRAINING

Practices' AML/CTF policies, procedures and controls should extend to employee hiring and training.

Preamble

The Hong Kong SAR Government ("the Government) intends to extend the scope of the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap. 615)("AMLO") beyond financial institutions ("FIs"). A bill to amend the AMLO in order to implement the "International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation", issued by the Financial Action Task Force ("FATF Recommendations" or "Rs") as these relate to customer due diligence ("CDD") and record keeping ("RK") for "designated non-financial businesses and professions ('DNFBPs')", is currently being considered by the Legislative Council. As a member of FATF, Hong Kong is required to implement the Rs, key parts of which apply not only to FIs but also to DNFBPs, including accountants. The Guidelines below are based on AMLO as it is expected to be amended.

Section 1: OVERVIEW AND APPLICATION

1.1 Introduction and Purpose of Guidelines

1.1.1 These Guidelines are published under section 7 of Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap. 615)("AMLO"). They apply primarily to member practices and members working in practices. In the Guidelines, reference to "practices" includes practice units under the Professional Accountants Ordinance (Cap. 50) and also trust or company service providers ("TCSP"), where the proprietors, partners or directors are members. Reference to "practices" should also be taken to include references to members working in practices, where the context may be so construed. The Guidelines should also provide useful information for members generally.[1]

1.1.2 The Guidelines make reference to AMLO, as well as to other existing legislation containing requirements relating to anti-money laundering/combating the financing of terrorism ("AML/CFT"), principally, the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405) ("DTROP"), the Organised and Serious Crimes Ordinance (Cap. 455) ("OSCO") and the United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575) ("UNATMO"). AMLO, and also relevant sections of the other ordinances, seek to give effect to the "International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation", issued by the Financial Action Task Force[2] ("FATF Recommendations" or "Rs"). As a member of FATF, Hong Kong is required to implement the Rs, key parts of which apply not only to financial institutions ("FIs"), to which the Rs were originally applied, but also to FATF "designated non-financial businesses and professions ('DNFBPs')", including accountants.[3]

1.1.3 It is recognised that, in contrast to FIs, professional standards limit the circumstances in which a practice may initiate, authorise, or execute cash transactions on behalf of clients and practices are not licensed to hold client monies or process cash transactions, so the money

[1] Members working in the financial services or other sectors specified in the Anti-Money Laundering and Counter-Terrorist Financing(Financial Institutions) Ordinance (Cap. 615) are advised to familiarise themselves with any guidelines issued by the appropriate relevant authority or regulatory body under that ordinance to facilitate compliance with the requirements of the ordinance.

[2] For more information about the FATF, see Appendix A.

[3] For the AMLO definition of DNFBPs, see Appendix E.

laundering/terrorist financing ("ML/TF") risks may be reduced for members.

1.1.4 At the same time, as members are bound by the Code of Ethics for Professional Accountants to conduct themselves with integrity and professionalism and to act in the public interest, not only the interests of their clients, even without legislation in place, practices may be expected to have in place adequate CDD or "know your client" procedures and arrangements for maintaining documentation, to minimise any risk of involvement in ML/TF. In order to mitigate and address the risks, whether legal, regulatory and reputational, of being found to be involved in facilitating, or turning a blind eye to, ML/TF, it is in the interests of practices to take on board the relevant Rs within their risk management programmes, including those Rs already incorporated in legislation, such as the requirement to report suspicious transactions.

1.1.5 Against the above background, these Guidelines are intended to:

- Provide general guidance on AML/CFT requirements under AMLO and other relevant legislation.
- Provide guidance on applying other relevant FATF Rs.
- Summarise relevant legislative provisions on AML/CFT.
- Require compliance by members with prescribed requirements to prevent ML/TF activities.
- Offer some general guidance to practices and their senior management in designing and implementing their own policies, procedures and controls for AML/CFT, appropriate to the nature of their businesses.

1.1.6 It should be noted that, while these Guidelines require compliance by practices with certain provisions, they do not constitute legal advice and, in case of doubt, members should consider seeking their own legal advice.

1.1.7 A failure by a practice to comply with a provision in these Guidelines does not by itself render the practices liable to any judicial or other proceedings but, in any court proceedings under the AMLO, the guideline is admissible in evidence; and if any provision set out in the guideline appears to the court to be relevant to any question arising in the proceedings, the provision will be taken into account in determining that question. In considering whether a practice has contravened a requirement under Schedule 2 of AMLO, or relevant section of other AML/CFT-related legislation, the Institute will have regard to any provision in the guideline published under this section that is relevant to the requirement.

1.1.8 In addition to the above, practices that pay insufficient attention to the AML/ CFT issues covered in these Guidelines could be at greater risk of becoming unwittingly associated with ML/ TF activities, with potentially serious consequences, such as criminal prosecution and loss of reputation.

1.1.9 For terms, abbreviations and definitions used in these Guidelines members should also refer to Appendix E.

1.2 Application of the guidelines

The Guidelines apply as follows:	AML/CTF policies, procedures and controls (section 2)	CDD, RK and ongoing monitoring (sections 3,4,7)	Suspicious transaction reporting and financial sanctions (sections 5,6)	Staff hiring and training (section 8)
Practices:				
When providing any service specified in paragraphs 1.2.1 or 1.2.2	**Mandatory**	**Mandatory**	**Mandatory**	**Mandatory**
When providing services other than those specified in paragraphs 1.2.1 or 1.2.2	**Mandatory**	**Good practice**	**Mandatory**	**Good practice**

1.2.1 When practices prepare for or carry out for a client a transaction concerning one or more of the following services, there are specific CDD, ongoing monitoring and RK measures that they must adopt, as set out in Sections 3, 4 and 7:

(a) buying and selling of real estate;
(b) managing of client money, securities or other assets;
(c) management of bank, savings or securities accounts;
(d) organisation of contributions for the creation, operation or management of companies;
(e) creation, operation or management of legal persons or arrangements;
(f) buying and selling of business entities.

1.2.2 In addition, practices that provide trust or company services should adopt the same CDD, ongoing monitoring and RK procedures, when they prepare for or carry out for a client a transaction concerning any of the following services:

(a) forming corporations or other legal persons;
(b) acting as, or arranging for another person to act as, a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
(c) providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
(d) acting as, or arranging for another person to act as, a trustee of an express trust or similar legal arrangement; or
(e) acting, or arranging for another person to act, as a nominee shareholder for a person other than a corporation whose securities are listed on a recognised stock market.

1.2.3 The provisions of these Guidelines should be read in the context of this subsection (i.e., subsection 1.2) and in conjunction with the relevant provisions of Hong Kong laws, and applied accordingly.

1.3 The nature of ML and TF

1.3.1 "Money laundering" is defined[4] to mean an act intended to have the effect of making any property:

(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.

1.3.2 "Terrorist financing" is defined[5] to mean:

(a) the provision or collection, by any means, directly or indirectly, of any property –
    (i) with the intention that the property will be used; or
    (ii) knowing that the property will be used,

    in whole or in part, to commit one or more terrorist acts (whether or not the property is actually so used); or

(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

(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.

1.3.3 Terrorists or terrorist organisations require financial support in order to achieve their aims. There is often a need for them to obscure or disguise links between them and their funding sources. It follows that terrorist groups must find ways to obscure fund movements, in the same way as ML, regardless of whether the funds are from a legitimate or illegitimate source, in order to be able to use them without attracting the attention of the authorities.

1.4 FATF and legislation concerned with money laundering and terrorist financing

1.4.1 The FATF has issued the Rs as a framework to detect and prevent ML/TF activities. The Rs have become a widely-accepted international benchmark and are used as the basis of, or as a reference for, legislation and regulation in many jurisdictions around the world.

1.4.2 Among the key Rs are those covering CDD and RK and the making of suspicious transaction reports ("STRs"), as well as AML/ CFT controls and monitoring. FATF members are expected to incorporate the basic requirements of CDD, RK and making STRs in law. They apply not only to FIs, but also to DNFPBs, including accountants, in relation to specified service offerings (see paragraphs 1.2.1 and 1.2.2, above). Meanwhile, requirements for AML/ CFT policies, procedures and controls (see section 2) apply to services generally.

[4] See AMLO, Schedule 1, section 1 of Part 1

[5] Ibid.

1.4.3 Legislation prescribing criminal offences for involvement in ML/TF, and including requirements on making STRs, has been in place for a number of years in Hong Kong. The legislation applies to everyone in Hong Kong. It should be noted that the requirement to make STRs is not limited to the FATF-specified services and includes a general obligation to report where there is knowledge or suspicion of ML/ TF.

1.4.4 Apart from AMLO, the three main pieces of legislation enacted in Hong Kong that are relevant to ML/TF are DTROP, OSCO and UNATMO. It is important that practices and their staff fully understand their responsibilities under the respective pieces of legislation.

1.4.5 DTROP and OSCO create an offence of ML in relation to dealing with property known or believed to represent proceeds of drug trafficking or of an indictable offence, respectively[6]. This is a serious offence carrying a maximum penalty of 14 years imprisonment and a fine of 5 million dollars.

1.4.6 DTROP, OSCO and UNATMO also contain provisions on making STRs and create an offence of not reporting where a person has the requisite suspicion or knowledge[7]. They also create an offence of "tipping off" in relation to making STRs (see Section 5). Additional information on the above legislation is provided in Appendix A.

[6] Section 25 of DTROP and OSCO

[7] Section 25A of DTROP and OSCO and sections 12(1) and 14 of UNATMO

Section 2: AML/CFT POLICIES, PROCEDURES AND CONTROLS

General requirements

2.1 Practices should develop and implement AML/CTF internal policies, procedures and other controls to address ML/TF concerns and compliance with the existing legal requirements on AML/CFT; and, more generally, to safeguard themselves against the legal and reputational risks of being found to be involved in facilitating ML/TF or not reporting known or suspected ML/TF activities. Practices should communicate these policies and procedures clearly to employees.

2.1.1 **Controls should cover:**

- **(a) Risk assessment and management**
- **(b) CDD**
- **(c) RK**
- **(d) Making STRs**
- **(e) A regular employee training programme**
- **(f) Compliance management arrangements, including the appointment of a compliance officer ("CO") at the management level**
- **(g) Hiring, e.g., adequate screening procedures to ensure high standards when hiring employees**
- **(h) An independent audit function, to test the system**
- **(i) Group policy, where appropriate**.

2.2 Adopting a risk-based approach ("RBA")

2.2.1 The type and extent of measures to be taken in relation to the items in paragraph 2.1.1 above should be appropriate and reasonable having regard to the risk of ML/TF and the size and nature of the business; that is, practices should adopt a risk-based approach ("RBA").

2.3 Ensuring effective controls

2.3.1 To ensure proper implementation of appropriate policies and procedures in relation to the items in paragraph 2.1.1 above, practices should have effective controls covering:

- (a) senior management oversight;
- (b) appointment of a CO and, depending on the size and complexity of the business, a separate Money Laundering Reporting Officer ("MLRO");
- (c) compliance and audit function; and
- (d) staff screening and training.

Senior management oversight

2.3.2 The senior management of a practice are responsible for managing the business effectively and within relevant legal and regulatory requirements, which should include adequate oversight in relation to AML/CFT. They should:

- (a) be satisfied that the AML/CFT controls are capable of addressing the practice's ML/TF identified risks;
- (b) appoint a partner, director or equivalent as a CO, who has overall responsibility for the establishment and maintenance of the practice's AML/CFT controls; and
- (c) appoint a senior member of the practice's staff as the MLRO, who is the central reference point for making STRs and who may, in some practices, be the same person as the CO).

2.3.3 To enable the CO and MLRO to discharge their responsibilities effectively, senior management should, as far as practicable, ensure that the CO and MLRO are:

(a) subject to any constraints, having regard to the size of the practice, independent of all operational and business functions;
(b) based in Hong Kong;
(c) of a sufficient level of seniority and authority;
(d) afforded regular contact with, and when required, direct access to senior management to ensure that senior management are able to satisfy themselves that their statutory obligations are being met and that the business is taking sufficiently robust measures to protect itself against the risks of ML/TF;
(e) fully conversant with the practice's statutory and regulatory requirements and the ML/TF risks arising from the business;
(f) capable of accessing, on a timely basis, all available information (both from internal sources, such as CDD records, and external sources, such as notices and circulars from the Institute); and
(g) equipped with sufficient resources, including staff and appropriate cover for the absence of the CO and the MLRO.

Roles of CO and MLRO

2.3.4 The principal function of the CO is to act as the focal point within a practice for the oversight of all activities relating to the prevention and detection of ML/TF and providing support and guidance to the senior management to ensure that ML/TF risks are adequately managed. Typically the CO would have responsibility for:

(a) reviewing the practice's AML/CFT systems to ensure they are up to date and meet current statutory and regulatory requirements; and
(b) oversight of the practice's AML/CFT controls, including monitoring their effectiveness and enhancing the controls and procedures where necessary.

2.3.5 In order to discharge these responsibilities, areas which may need to be considered by the CO, include:

(a) how the AML/CFT controls are to be managed and tested;
(b) identifying and addressing significant deficiencies in the controls;
(c) mitigating ML/TF risks arising from business relationships and transactions with persons from countries that do not apply, or insufficiently apply, the FATF Rs;
(d) communicating key AML/CFT issues to the senior management, including, where appropriate, significant compliance deficiencies;
(e) considering changes that may need to be made or proposed as a result of new legislation, regulatory requirements or guidance relevant to AML/CFT;
(f) training of staff for AML/CFT purposes.

2.3.6 The MLRO should play an active role in the identification and reporting of suspicious transactions. Principal functions performed would normally include:

(a) reviewing internal disclosures and exception reports and, in light of available relevant information, determining whether or not it is necessary to make an STR to the Joint Financial Intelligence Unit ("JFIU")[8];

[8] JFIU was established in 1989 and is run jointly by the Hong Kong Police Force and Customs & Excise Department. Its role is to receive, analyse and store suspicious transactions reports, and disseminate them to the appropriate investigative units.

(b) maintaining records related to such internal reviews;
(c) providing guidance on how to avoid "tipping off", where disclosures are made; and
(d) acting as the main point of contact with the JFIU, law enforcement, and any other competent authorities in relation to ML/TF prevention and detection, investigation or compliance.

Compliance and audit function

2.3.7 The compliance and audit function of a practice should review the implementation of the AML/CFT controls, e.g., by sample testing (in particular, the controls for recognising and reporting suspicious transactions), to ensure effectiveness. The frequency and extent of the review should be commensurate with the risks of ML/TF and the size of the practice's business. Where appropriate, practices may engage an external party to conduct the review.

2.3.8 Where practicable, practices should establish an independent compliance and audit function which should have a direct line of communication to the senior management.

Staff screening

2.3.9 Practices should establish, maintain and operate appropriate procedures in order to be satisfied of the integrity of any new employees.

2.4 Risk factors

2.4.1 While no system can be expected to detect and prevent all ML/TF activities, practices should establish and implement adequate and appropriate AML/CFT controls (including client acceptance policies and procedures), taking into account factors such as:

- types of client involved and their geographical locations
- services/ products offered
- mode of delivery of the service/ product; and
- size of the practice.

Appendix B provides some examples of steps practices should consider taking. See also the FATF Guidance on RBA for Accountants.

2.5 Adopting a risk-based approach in relation to clients

2.5.1 An RBA is recognised as an effective way to combat ML/TF. It helps to ensure that measures to prevent or mitigate ML/TF are proportionate to the risks identified and to facilitate decisions on how to allocate resources in the most effective way. The general principle of an RBA in relation to clients is that where clients are assessed to be of higher ML/TF risks, practices should take enhanced measures to manage and mitigate those risks, and that, where the risks are lower, simplified measures may be applied.

2.5.2 While there are no universally accepted methodologies that prescribe the nature and extent of an RBA, an effective RBA involves identifying and categorising ML/TF overall risks at the client level and establishing reasonable measures based on risks identified. An effective RBA will allow practices to exercise reasonable business judgment with respect to their clients.

2.5.3 An effective RBA will enable practices to subject clients to proportionate controls and oversight by determining:

(a) the extent of the CDD to be performed on the direct client; the extent of the measures to be undertaken to verify the identity of any beneficial owner and any person purporting

to act on behalf of the client (see Section 3);
(b) the level of ongoing monitoring to be applied to the relationship (see section 4); and
(c) measures to mitigate any risks identified.

2.5.4 For example, an RBA may require extensive CDD for high-risk clients, such as an individual (or corporate entity) whose source of wealth and funds is unclear or who requires the setting up of complex structures.

2.5.5 A reasonably designed RBA should assist practices to effectively manage potential ML/TF risks, rather than prohibit practices from engaging in transactions with clients or establishing business relationships with potential clients. It should also not be designed to prevent practices from finding innovative ways to diversify their businesses.

Documenting risk assessment (see also Section 7)

2.5.6 Practices should document their risk assessment, so that, if called upon to do so, they can demonstrate to the Institute:
(a) how they assess a client's ML/TF risk; and
(b) that the extent of their CDD and ongoing monitoring is appropriate based on that client's ML/TF risk.

2.6 Ongoing review of risks and controls

2.6.1 The identification of risks associated with clients, services (including delivery channels), and geographical locations, is not a static assessment and may change over time, depending on how circumstances develop, and how threats evolve. In addition, while a risk assessment should always be performed at the inception of a client relationship, for some clients, a comprehensive risk profile may only become evident once the service has begun, making monitoring of client activity and ongoing review a fundamental component of a reasonably designed RBA. Practices may therefore have to adjust their risk assessment of a particular client from time to time, or based upon information received, and review the extent and frequency of the CDD and ongoing monitoring to be applied to the client. Further advice on ongoing monitoring is contained in Section 4.

2.6.2 More broadly, practices should keep their policies and procedures under review and assess that their risk mitigation procedures and controls are working effectively.

2.7 Business conducted outside Hong Kong

2.7.1 Practices with overseas branches/ offices, or subsidiary undertakings, should adopt a group AML/CFT policy to ensure that branches/ offices and subsidiary undertakings that carry on the same business as the practice in a place outside of Hong Kong have procedures in place to comply with CDD and RK requirements, similar to those imposed under Schedule 2 of AMLO, to the extent permitted by the law of that location.

2.7.2 If the law of the place at which a branch/ office, or subsidiary undertaking carries on business does not permit the application of any procedures relating to any of the requirements referred to in 2.7.1, the practice should (a) inform the Institute and (b) take additional measures to effectively mitigate the risk of ML/TF faced by the branch/ office, or subsidiary undertaking as a result of its inability to comply with the requirement.

Section 3: CUSTOMER DUE DILIGENCE

General requirements[9]

3.1 Where applicable, practices should carry out the following CDD measures:

(a) identify the client and verify the client's identity using documents, data or information provided by a government body or other reliable, independent source;

(b) where there is a beneficial owner[10] in relation to the client (subject to certain limited exceptions indicated below) identify and take reasonable measures to verify the beneficial owner's identity, so that the practice is satisfied that it knows who the beneficial owner is, including in the case of a legal person or trust[11], measures to enable the practice to understand the ownership and control structure of the legal person or trust;

(c) obtain information on the purpose and intended nature of the business relationship (if any) to be established with the practice, unless the purpose and intended nature are obvious; and

(d) if a person purports to act on behalf of the client:
- **(i) identify the person and take reasonable measures to verify the person's identity using documents, data or information provided by a government body or other reliable and independent source;**
- **(ii) verify the person's authority to act on behalf of the client;**

(e) practices should adopt enhanced due diligence measures in relation to high-risk clients (including foreign "politically exposed persons"); and

(f) may adopt simplified due diligence measures in certain specified circumstances.

3.2 Introduction to CDD

3.2.1 CDD information is an important element in recognising whether there are grounds for knowledge or suspicion of ML/TF. It is intended to enable practices to form a reasonable belief that they know the true identity of each client and, with an appropriate degree of confidence, know the type of business and transactions that the client is likely to undertake and the source and intended use of funds.

3.2.2 Practices should, therefore, identify, and verify the identity of their clients, to the extent

---

[9] See Appendix C for further details on the application of CDD requirements

[10] For definitions, see Appendix E

[11] For the purpose of these Guidelines, a trust means an express trust or any similar arrangement for which a legal-binding document (i.e. a trust deed or in any other forms) is in place.

necessary to provide them with reasonable assurance that the information they have is an appropriate and sufficient indication of the client's true identity. A standard level of due diligence should be applied to all clients, with the possibility to carry out simplified CDD ("SDD") in lower-risk scenarios. In contrast, enhanced CDD ("EDD") should be applied in respect of clients or circumstances determined to be of higher ML/TF risk.

3.2.3 Practices may have other client acceptance and continuance procedures, for example, to ensure compliance with independence requirements and to avoid conflicts of interest. The CDD may either be integrated with those procedures or addressed separately. Initial CDD information assists in client acceptance decisions and also enables practices to form expectations of their client's behaviour, which provides some assistance on detecting potentially suspicious behaviour during the business relationship.

3.2.4 In determining what constitutes "reasonable measures" to verify the identity of a beneficial owner and understand the ownership and control structure of a legal person or trust, and/or to verify the identity of a person who purports to act on behalf of a client, practices should consider and give due regard to the ML/TF risks posed by a particular client and a particular business relationship. Examples of possible risk factors are set out in Appendix B.

3.3 Circumstances where CDD should be applied

3.3.1 CDD requirements should generally be applied:

(a) before establishing a business relationship with a client;

(b) before carrying out for the client an occasional transaction involving an amount equal to or above $120,000 or an equivalent amount in any other currency, whether the transaction is carried out in a single operation or in several operations that appear to be linked;

(c) where there may be a suspicion of ML/TF; o**r**

(d) when there is doubt about the veracity or adequacy of any information previously obtained for the purpose of identifying the client or verifying the client's identity.

Pre-existing clients

(a) Practices should perform the CDD measures set out in these Guidelines in respect of pre-existing clients (with whom the business relationship was established before the Guidelines came into effect), in addition to the situations in paragraph 3.3.1 (c) and (d), when a transaction takes place with regard to the client, which is:

(i) by virtue of the amount or nature of the transaction, unusual or suspicious; or

(ii) not consistent with the practice's knowledge of the client or the client's business or risk profile, or with its knowledge of the source of the client's funds; or

(b) a material change occurs in the way in which the client's business in conducted.

3.3.2 Practices should, in any case, over time, review the information known about pre-existing clients, assess the ML/TF risks of such clients and seek more information if necessary. Requirements for ongoing monitoring also apply to pre-existing clients (see Section 4).

3.4 Client acceptance/risk assessment and risk categories

3.4.1 Practices should assess the ML/TF risks of individual clients and may consider assigning different ML/TF risk levels to the clients.

3.4.2 While there is no agreed upon definitive set of risk factors and no one methodology to apply

these risk factors in determining the ML/TF risk rating of clients, as indicated in Appendix B, relevant factors can, generally speaking, be organised into three broad categories, which, in practice, are often inter-related: client risk, country or geographic risk and service, including delivery channel, risk.

3.4.3 For example, some key generic factors that may indicate a higher level of client risk are:

(a) Factors indicating that the client is attempting to obscure understanding of its business, ownership or the nature of its transactions.

(b) Factors indicating certain transactions, structures, geographical locations, international activities, or other factors, that are not in keeping with the practice's understanding of the client's business or economic situation.

(c) Client industries, sectors or categories where opportunities for ML/TF are particularly prevalent.

3.4.4 However, not all clients falling into such risk categories are necessarily high-risk clients. After adequate review, it may be determined that a particular client is pursuing a legitimate purpose. Provided the economic rationale for the structure and/or activities or transactions of a client can be made clear, if called upon to do so, a practice may be able to demonstrate that the client is carrying out legitimate operations for which there is a satisfactory explanation and non-criminal purpose.

3.4.5 As regards country or geographic risk, this, in conjunction with other risk factors, may provide useful information as to potential ML/TF risks, though it should be borne in mind that lower-risk and legitimate commercial enterprises may be located or operate in high-risk countries. Nevertheless, clients may be judged to pose a higher than normal risk where they, or their source or destination of funds, are located in a country that is, e.g., subject to sanctions, identified by the FATF, or other credible sources, as lacking an appropriate AML/CFT regime, or identified by credible sources as having significant level of corruption or providing support to terrorists or terrorist activities.

3.4.6 A balanced and common sense approach should be adopted with regard to clients connected with jurisdictions which do not, or which insufficiently, apply the FATF recommendations (see paragraphs 3.13.27- 3.13.29). While extra care may well be justified in such cases, it is not a requirement to refuse to do any business with such clients or automatically classify them as high risk and subject them to EDD process. Rather, practices should weigh all the circumstances of the particular situation and assess whether there is a higher than normal risk of ML/TF.

3.5 Identification and verification of the client's identity

Practices should identify the customer and verify the client's identity by reference to documents, data or information provided by a reliable and independent source, such as a governmental body, public register, or other source generally recognised as being reliable and independent. Copies of all reference source documents, data or information used to verify the identity of the client should be retained. Where the client is unable to produce original documents, practices may consider accepting documents that are certified to be true copies by an independent, qualified person (see paragraph 3.13.4).

Appendix C contains further information on documents generally recognised as appropriate, independent and reliable sources for identity verification purposes for natural persons, legal persons and trusts.

3.6 Identification and verification of a beneficial owner

3.6.1 A beneficial owner is normally an individual, or individuals, who ultimately own or control the client, or on whose behalf a service is being provided. In respect of a client who is an individual, not acting in an official capacity on behalf of a legal person or trust, the client himself is normally the beneficial owner. There is no requirement to make proactive searches for beneficial owners in such a case, but practices should make appropriate enquiries where there are indications that the client is not acting on his own behalf.

3.6.2 Where an individual is identified as a beneficial owner, practices should endeavour to obtain identification information of the kind set out in Part I of Appendix C.

3.6.3 Generally, however, the verification requirements are different for a client and a beneficial owner. The obligation to verify the identity of a beneficial owner is to take reasonable measures, based on an assessment of the ML/TF risks, so that the practice is satisfied that it knows who the beneficial owner is.

3.6.4 Practices should identify all beneficial owners of a client. In relation to verification of beneficial owners' identities, in normal situations, the AMLO refers to reasonable measures being taken to verify the identity of any beneficial owners. A beneficial owner in relation to a corporation is an individual who owns or controls, directly or indirectly, more than 25% of the issued share capital or voting rights, or who exercises ultimate control over the management, of the corporation. If the corporation is acting on behalf of another person, reference to "beneficial owner" means that other person. There are equivalent definitions for the beneficial owner of a partnership or trust (see Appendix E).

3.7 Identification and verification of a person purporting to act on behalf of the client

3.7.1 If a person purports to act on behalf of the client, practices should:

a) identify the person and take reasonable measures to verify the person's identity on the basis of documents, data or information provided by-
   (i) a governmental body;
   (ii) any other source generally recognised as being reliable and independent
b) verify the person's authority to act on behalf of the client.

3.7.2 In taking reasonable measures to verify the identity of persons purporting to act on behalf of clients (e.g., authorised account signatories and attorneys), practices should endeavour to obtain the same kind of identification information as that set out in Part I of Appendix C.

3.7.3 Practices should also obtain written authority[12] verifying that the individual purporting to represent the client is authorised to do so.

3.8 Characteristics and evidence of identity

3.8.1 Some types of documents are more easily forged than others. If suspicions are raised in relation to any document offered, practices should take whatever practical and proportionate steps are available to establish whether the document offered is genuine, or has been reported as lost or stolen. This may include searching publicly-available information, approaching relevant authorities (such as the Immigration Department through its hotline) or requesting corroboratory evidence from the client. Where suspicion cannot be eliminated, the document should not be accepted and consideration should be given to making a report to the JFIU.

[12] For a corporation, the board resolution or similar written authority should be obtained.

3.8.2 Where documents are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents provide evidence of the client's identity (e.g., ensuring that staff members assessing such documents are proficient in the language or obtaining a translation from a suitably qualified person).

3.9 Purpose and intended nature of business relationship

3.9.1 Practices should understand the purpose and intended nature of the client relationship. In some instances, this will be self-evident, but in many cases, more information may have to be obtained.

3.9.2 Unless the purpose and intended nature are obvious, satisfactory information should be obtained from all new clients as to the intended purpose and reason for establishing the relationship, and document the information. Depending on the practice's risk assessment of the situation, relevant information may include:

(a) nature and details of the business/occupation/employment;
(b) the anticipated level and nature of the activity that is to be undertaken through the relationship (e.g., what services are likely to be required);
(c) location of client;
(d) the expected source and origin of any funds to be used in the relationship; and
(e) initial and ongoing source(s) of wealth or income.

3.9.3 This requirement also applies in the context of non-residents. While most non-residents seek business relationships in Hong Kong for perfectly legitimate reasons, some may represent a higher risk for ML/TF. Practices should therefore aim to understand the rationale for a non-resident to seek to establish a client relationship with the practice in Hong Kong.

3.10 Timing of identification and verification of identity

General requirement

3.10.1 The CDD process, i.e., obtaining information on the client and beneficial owners, and about the purpose and intended nature of the business relationship, should always be completed before establishing any client relationship and/or before carrying out occasional transactions or assignments, other than in exceptional cases, as set out in 3.10.3.

3.10.2 In normal circumstances, where practices are unable to complete the CDD process as indicated above, they should not establish a client relationship or carry out any occasional transactions or assignments with that client and should assess whether this failure, in itself, provides grounds for knowledge or suspicion of ML/TF and making a report to the JFIU is appropriate.

Delayed client identity verification and failure to complete verification

3.10.3 Exceptionally, practices may verify the identity of the client and, to the extent necessary, any beneficial owner, after establishing the business relationship, provided that:

(a) any risk of ML/TF arising from the delayed verification of the client's or beneficial owner's identity can be effectively managed;
(b) it is necessary not to interrupt the normal course of business with the client;
(c) verification is completed as soon as reasonably practicable afterwards; and
(d) the business relationship will be terminated if verification cannot be completed as soon as reasonably practicable afterwards.

3.10.4 This discretion should not be used to defer CDD procedures unnecessarily, in particular, where:

(a) there may be some indications of ML/TF;
(b) practices become aware of anything that gives rise to doubt the identity or intentions of the client or beneficial owner; or
(c) the relationship is assessed to pose a higher risk.

3.10.5 Verification of identity should be concluded within a reasonable timeframe thereafter[13]. Where this cannot be done, practices should as soon as reasonably practicable suspend or terminate the service or relationship, unless there is a reasonable explanation for the delay[14].

Practices should assess whether a failure to complete the desired verification of itself provides grounds for knowledge or suspicion of ML/TF and for making an STR to the JFIU.

Keeping client information up-to-date

3.10.6 Once the identity of a client has been satisfactorily verified, there is no obligation to re-verify identity (unless doubts arise as to the veracity or adequacy of the evidence previously obtained). However, steps should be taken from time to time to ensure that the client information that has been obtained for the purposes of CDD is up to date and relevant, by undertaking periodic reviews of existing records of clients. An appropriate time to do so is upon certain trigger events such as:

(a) when a significant or unusual activity or transaction[15] is to take place;
(b) when a material change occurs in the client's ownership and/or activities – practices are advised to consider at least annually whether there have been changes suggesting that a full reappraisal would be sensible[16];
(c) when a practice's client documentation standards change substantially; or
(d) when a practice is aware that it lacks sufficient information about the client concerned.

In all cases, the factors determining the period of review or what constitutes a trigger event should be set out in the practice's policies and procedures.

3.10.7 All clients assessed as high risk should be subject to at least an annual review of their profile to ensure the CDD information retained remains up to date and relevant. It would be prudent to review the risk category of other clients also on an annual basis.

[13] The same principle applies to the verification of address for a direct customer; an example of a reasonable timeframe being 90 working days.

[14] For reference only, the Hong Kong Monetary Authority specifies the following timeframes:
(a) completing such verification no later than 30 working days after the establishment of business relations;
(b) suspending business relations with the client and refraining from carrying out further activities or transactions (except, where relevant, to return funds to their sources, to the extent that this is possible) if such verification remains uncompleted 30 working days after the establishment of business relations; and
(c) terminating business relations with the client if such verification remains uncompleted 120 working days after the establishment of business relations.

[15] "Significant" is not necessarily linked to monetary value. It may include activities that are unusual or not in line with the practice's knowledge of the client.

[16] Reference should also be made to section 6 of Schedule 2 "Provisions relating to Pre-Existing Customers".

3.11 Application of SDD

When SDD can be conducted generally

3.11.1 Where the risks of ML/TF are lower, practices may conduct SDD measures, which take into account the nature of the lower risk. The simplified measures should be commensurate with the lower risk factors (e.g., a lower risk for identification and verification purpose at the client acceptance stage does not automatically mean that the same client is lower risk at the ongoing monitoring stage). Examples of possible SDD measures are:

(a) Verifying the identity of the client and the beneficial owner after the establishment of the business relationship.
(b) In some circumstances, not trying to identify the beneficial owner[17] (see 3.12.6).
(c) Reducing the frequency of client identification updates.
(d) Reducing the degree of on-going monitoring and scrutinising of activities.
(e) Not collecting specific information to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

3.11.2 SDD measures should not be adopted whenever there may be a suspicion of ML/TF, when a practice doubts the veracity or adequacy of any client identification/ verification information previously obtained, even though the client or the activity falls within paragraphs 3.12.6, 3.12.10 and 3.12.11 below, or where specific higher-risk scenarios apply, e.g., where the client is from, or based in, a higher-risk country or jurisdiction.

3.11.3 Practices should set out in their internal procedures what is considered to constitute reasonable grounds to conclude that a client can be subject to SDD measures. Where SDD is performed, the grounds for and details of the risk assessment, and the nature of the SDD measures, should be documented. Practices may have to substantiate these grounds to the Institute or other relevant authorities**.**

3.11.4 The following are some examples where SDD measures may be adopted:

(a) Reliable information on the client is publicly available.
(b) The practice is familiar with the client's AML/CFT controls due to previous dealings with the client.
(c) The client is a listed company that is subject to regulatory disclosure requirements, or an FI that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF.

3.11.5 A practice's knowledge about a client will generally grow within the context of an ongoing relationship with that client. Relevant information that the practice obtains may come from, for example:

(a) The reasons for the proposed engagement of the practice and non-reappointment of the previous firm.
(b) Communications with existing or previous providers of professional services to the client, and discussions with other third parties.
(c) Enquiry of other firm personnel or third parties.
(d) Background searches of relevant databases.

---

[17] It includes the individuals who ultimately own or control the customer and the person(s) on whose behalf the client is acting (e.g., underlying client(s) of a client that is an FI).

Specific types of client to which SDD may be applied

3.11.6 The AMLO indicates that it is not necessary to identify and verify the identity of any beneficial owner, in the circumstances set out in paragraph 3.3.1(a) or (b), where the client is:

(a) a Hong Kong SAR Government entity or a public body in Hong Kong;
(b) a government or public body in an equivalent jurisdiction (see subsection 3.16);
(c) a corporation listed on a stock exchange;
(d) a majority-owned subsidiary of a company in (c) or (d);
(e) an FI, as defined in AMLO
(f) an institution that-
    (i) is incorporated or established in an equivalent jurisdiction;
    (ii) carries on a business similar to that carried on by an FI;
    (iii) is subject to compliance with AML/CFT requirements consistent with standards set by the FATF and
    (iv) is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the relevant authorities[18];
(g) an investment vehicle where the person responsible for carrying out measures that are similar to the CDD measures in relation to all the investors of the investment vehicle is-
    (i) an FI;
    (ii) an institution incorporated or established in Hong Kong, or in an equivalent jurisdiction, that-
        i. is subject to compliance with AML/CFT requirements consistent with standards set by the FATF (i.e., has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2 of AMLO); and
        ii. is supervised for compliance with those requirements.

3.11.7 If a client not falling within paragraph 3.12.6 has in its ownership chain an entity falling within the scope of that paragraph, it is not necessary to identify or verify the beneficial owners of that entity in that chain in the circumstances referred to in paragraph 3.3.1(a) or (b). However, practices should still identify and take reasonable measures to verify the identity of beneficial owners in the ownership chain that are not connected with that entity.

Foreign financial institutions

3.11.8 For ascertaining whether an institution meets the criteria set out in paragraph 3.12.6(g), it will generally be sufficient for practices to verify that the institution is on the list of authorised (and supervised) FIs in the jurisdiction concerned.

Listed companies

3.11.9 For relevant listed companies, it will be generally sufficient for practices to obtain proof of listed status on a stock exchange. In other cases, practices should endeavour to obtain the identification information for a legal person of the kind set out in Appendix C.

[18] I.e., the regulators of relevant FIs

Government and public bodies

3.11.10 Public body includes:
(a) any executive, legislative, municipal or urban council;
(b) any government department or undertaking;
(c) any local or public authority or undertaking;
(d) any board, commission, committee or other body, whether paid or unpaid, appointed by the chief executive or the government; and
(e) any board, commission, committee or other body that has power to act in a public capacity under or for the purposes of any enactment.

SDD in relation to specific products

3.11.11 It is not necessary to identify and verify the identity of any beneficial owner of the client, in the circumstances referred to in paragraph 3.3.1(a) or (b), if the practice has reasonable grounds to believe that the product to which the transaction relates is:
(a) a provident, pension, retirement or superannuation scheme (however described) that provides retirement benefits to employees, where contributions to the scheme are made by way of deduction from income from employment and the scheme rules do not permit the assignment of a member's interest under the scheme; or
(b) an insurance policy of the kind stipulated in Schedule 2, section 4(5) of AMLO.

3.11.12 For the purpose of paragraph 3.12.11(a), the employer may generally be treated as the client and SDD applied on the employer. Where the practice has a client relationship with the employees, it should endeavour identify and verify the identities of the employees in by obtaining information of the kind set out in Appendix C.

Solicitor's client accounts

3.11.13 If a client of a practice is a solicitor or a firm of solicitors, the practice is not required to identify any beneficial owner of the customer account opened by the practice's client in the circumstances referred to in paragraph 3.3.1(a) or (b), provided that the following criteria are satisfied:
(a) the customer account is kept in the name of the practice's client ;
(b) moneys or securities of the client's customers in the client account are mingled; and
(c) the client account is managed by the client as agent of those customers.

3.12 Application of EDD

High-risk situations

3.12.1 In situations that, by their nature, present a higher risk of ML/TF, additional measures should be taken to mitigate the risk of ML/TF. (Examples of possible risk factors are indicated in Appendix B.) Additional measures[19] or EDD, for illustrative purposes, may include:
(a) obtaining additional information on the client (e.g., connected parties[20], accounts or relationships) and updating the client profile more regularly, including the identification data;
(b) obtaining additional information on the intended nature of the business relationship (e.g., anticipated account activity), the source of wealth and source of funds;

[19] Additional measures should be documented in the practice's policies and procedures
[20] Consideration might be given to obtaining, and taking reasonable measures to verify, the addresses of directors and account signatories.

(c) obtaining the approval of senior management to commence or continue the relationship; and
(d) conducting enhanced monitoring of the business relationship, by increasing the number and timing of the controls applied and selecting patterns of transactions that need further examination.

Clients not physically present for identification purposes

3.12.2 Practices should apply equally effective client identification procedures and ongoing monitoring standards for clients not physically present for identification purposes as for those where the client is available for interview[21]. Where a client has not been physically present for identification purposes, practices will generally not be able to determine that the documentary evidence of identity actually relates to the client they are dealing with. Consequently, there are increased risks and practices should carry out at least one of the following measures to mitigate the risks posed:
(a) further verifying the client's identity on the basis of documents, data or information referred to in paragraph 3.5 but not previously used for the purposes of verification of the client's identity under that section;
(b) taking supplementary measures to verify the information relating to the client that has been obtained by the practice.

3.12.3 Consideration should be given on the basis of the ML/TF risk to obtaining copies of documents that have been certified by a suitable certifier.

Suitable certifiers and the certification procedure

3.12.4 Use of an independent suitable certifier guards against the risk that documentation provided does not correspond to the client whose identity is being verified. However, for certification to be effective, the certifier will need to have seen the original documentation. Suitable persons to certify verification of identity documents may include:
(a) an intermediary specified in Schedule 2, section 18(3) of AMLO;
(b) a member of the judiciary in an equivalent jurisdiction;
(c) an officer of an embassy, consulate or high commission of the country of issue of documentary verification of identity; and
(d) a Justice of the Peace.

3.12.5 The certifier must sign and date the copy document (printing his/her name clearly underneath) and clearly indicate his position or capacity on it. The certifier must state that it is a true copy of the original (or words to similar effect).

3.12.6 Practices should exercise caution when considering accepting certified copy documents, especially where such documents originate from a country perceived to represent a high risk, or from unregulated entities in any jurisdiction.

3.12.7 In any circumstances where practices are unsure of the authenticity of certified documents, or that the documents relate to the client, they should take additional measures to mitigate the ML/TF risk.

[21] This is not restricted to being physically present in Hong Kong; a face-to-face meeting could take place outside Hong Kong.

Politically exposed persons ("PEPs")

General

3.12.8 Much international attention has been paid in recent years to the risks associated with providing financial and business services to those with a prominent political profile or holding senior public office. However, PEP status itself does not mean that the individuals are corrupt or that they have been incriminated in any corruption.

3.12.9 However, their office and position may render PEPs vulnerable to corruption. The risks increase when the person concerned is from a foreign country with widely-known problems of bribery, corruption and financial irregularity within their governments and society. This risk is even more acute where such countries do not have adequate AML/CFT standards.

3.12.10 While the statutory definition of PEPs in AMLO (see paragraph 3.13.12) includes only individuals entrusted with prominent public function in a place outside the People's Republic of China[22], domestic PEPs may also present, by virtue of the positions they hold, a high risk situation where EDD should be applied. Practices should therefore adopt an RBA to determining whether to also apply the measures in paragraph 3.13.18 to domestic PEPs.

3.12.11 The statutory definition does not automatically exclude sub-national political figures. In determining what constitutes a prominent public function, practices should consider factors such as persons with significant influence in general, significant influence over or control of public procurement, state-owned enterprises, etc.

(Foreign) Politically exposed persons

3.12.12 A PEP is defined in AMLO as:

(a) an individual who is or has been entrusted with a prominent public function in a place outside the People's Republic of China and
  (i) includes a head of state, head of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation and an important political party official;
  (ii) but does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph (i);
(b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or
(c) a close associate of an individual falling within paragraph (a).

3.12.13 AMLO defines a "close associate" as:

(a) an individual who has close business relations with a person falling under paragraph 3.13.12(a) above, including an individual who is a beneficial owner of a legal person or trust of which the person falling under paragraph 3.13.12(a) is also a beneficial owner; or
(b) an individual who is the beneficial owner of a legal person or trust that is set up for the benefit of a person falling under paragraph 3.13.12(a).

[22] Reference should be made to the definition of the People's Republic of China in the Interpretation and General Clauses Ordinance (Cap. 1), which includes Hong Kong and Macau.

3.12.14 Practices should establish and maintain effective procedures for determining whether a client or a beneficial owner of a client is a PEP.

3.12.15 Practices can reduce risk by conducting EDD before establishing the business relationship and ongoing monitoring where they know or suspect that the client relationship is with or involves a PEP.

3.12.16 Practices may use publicly-available information and/or screening against commercially available databases, or refer to relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations to assess which countries are most vulnerable to corruption (e.g., Transparency International's "Corruption Perceptions Index") and should be vigilant where either the country to which the client has business connections, or the business/ industrial sector, is more vulnerable to corruption.

3.12.17 Specific risk factors practices should consider in handling a business relationship (or potential relationship) with a PEP include:

(a) any particular concern over the country where the PEP holds his public office or has been entrusted with his public functions, taking into account his position;
(b) any unexplained sources of wealth or income (i.e., value of assets owned not in line with the PEP's income level);
(c) expected receipts of large sums from governmental bodies or state-owned entities;
(d) source of wealth described as commission earned on government contracts;
(e) request by the PEP to associate any form of secrecy with a transaction; and
(f) use of government accounts as the source of funds in a transaction.

3.12.18 When practices know that a particular client or beneficial owner is a PEP, they should, before
(i) establishing a business relationship; or
(ii) continuing an existing business relationship, where the client or the beneficial owner is subsequently found to be a PEP,
apply the following EDD measures:

(a) obtain approval from senior management;
(b) take reasonable measures to establish the client's or the beneficial owner's source of wealth and the source of the funds involved in the business relationship; and
(c) if a practice proceeds to establish a relationship or to continue an existing relationship, it should apply enhanced monitoring to the relationship in accordance with the assessed risks.

3.12.19 It is for practices to decide the measures they deem reasonable, in accordance with its assessment of the risks, to establish the source of funds and source of wealth. In practical terms, this will often amount to obtaining information from the PEP and trying to verify it against publicly-available information sources, such as asset and income declarations, which some jurisdictions expect certain senior public officials to file and which often include information about an official's source of wealth and current business interests. Practices should, however, note that not all declarations are publicly available and that a PEP client may have legitimate reasons for not providing a copy.

3.12.20 Practices should be aware that some jurisdictions impose restrictions on their PEP's ability to hold foreign bank accounts or to hold other office or paid employment. However, this does not mean that practices are expected to know about the laws or regulations governing the conduct of PEPs in other jurisdictions.

Domestic politically exposed persons

3.12.21 For the purposes of these Guidelines, a domestic PEP is defined as:

(a) an individual who is or has been entrusted with a prominent public function in a place within the People's Republic of China, including Hong Kong; and

(i) includes a head of state, head of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation and an important political party official;

(ii) but does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph (i);

(b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or

(c) a close associate of an individual falling within paragraph (a) (see paragraph 3.13.13).

3.12.22 Practices should take reasonable measures to determine whether an individual is a domestic PEP. If an individual is known to be a domestic PEP, a practice should perform a risk assessment to determine whether the individual poses a higher risk of ML/TF. Domestic PEPs status in itself does not automatically confer higher risk. In any situation that a practice assesses to present a higher risk of ML/TF, it should apply the EDD and monitoring referred to in paragraph 3.13.18.

3.12.23 Practices should retain a copy of the assessment and should review the assessment whenever concerns as to the activities of the individual arise.

Senior management approval

3.12.24 As regards the level of senior management personnel who may approve the establishment or continuation of a relationship where EDD applies, the approval process should take into account the advice of a practice's CO. In general the more potentially sensitive the PEP, the higher the approval process should be escalated.

Periodic reviews

3.12.25 Foreign PEPs and domestic PEPs assessed to present a higher ML/TF risk should be subject to a minimum annual review. CDD information should be reviewed to ensure that it remains up to date and relevant.

Bearer shares

3.12.26 Bearer shares lack the regulation and control of common shares because ownership is not recorded. Therefore, if practices come across companies with capital in the form of bearer shares, they should adopt procedures to establish the identities of the holders and beneficial owners of such shares and ensure that they are notified whenever there is a change of holder or beneficial owner.

Jurisdictions that do not or insufficiently apply the FATF Rs or otherwise posing higher ML/TF risk

3.12.27 Practices should give particular attention to, and exercise extra care in respect of:

(a) client relationships with, and the provision of ad hoc services to, persons (including legal persons and FIs) from or in jurisdictions that do not, or which insufficiently, apply the FATF Rs; and

(b) transactions and businesses connected with jurisdictions assessed as higher ML/TF risk.

3.12.28 In determining which jurisdictions either do not, or insufficiently, apply the FATF Rs, or may otherwise pose a higher risk, practices should consider, among other things:

(a) information that may be issued by the Institute from time to time (see paragraph 3.13.30);
(b) whether the jurisdiction is subject to sanctions, embargoes or similar measures issued by, for example, the United Nations ("UN")(see Section 6);
(c) whether the jurisdiction is identified by credible sources[23] as lacking appropriate AML/CFT laws, regulations and other measures;
(d) whether the jurisdiction is identified by credible sources as providing funding or support for terrorist activities and has designated terrorist organisations operating within it; and
(e) whether the jurisdiction is identified by credible sources as having significant levels of corruption, or other criminal activity.

3.12.29 Practices should be aware of the potential reputational risk of conducting business in jurisdictions that do not, or which insufficiently, apply the FATF Rs, or other jurisdictions known to apply inferior standards for the prevention of ML/TF. If practices established in Hong Kong have operating units in such jurisdictions, practices should ensure that the controls adopted in such overseas units are, as far as possible, similar to those adopted in Hong Kong.

3.12.30 Where the requirement is called for by the FATF, or in other circumstances independent of the FATF, but also considered to be higher risk, the Institute may advise practices to undertake EDD measures, proportionate to the nature of the risks.

3.13 Prohibition on anonymous accounts

3.13.1 Practices should not assist new or existing clients to open or maintain anonymous accounts or accounts in fictitious names.

3.14 Jurisdictional equivalence

General

3.14.1 Jurisdictional equivalence is an important aspect in the application of CDD measures above. "Equivalent jurisdiction" is defined in the AMLO as meaning:

(a) a jurisdiction that is a member of the FATF, other than Hong Kong; or
(b) a jurisdiction that imposes requirements similar to those imposed under Schedule 2 of the AMLO

Determination of jurisdictional equivalence

3.14.2 Practices may, therefore, need to consider which jurisdictions, other than FATF members,

[23] "Credible sources" refers to information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-government organisations. The information provided by these credible sources does not have the effect of law or regulation and should not be viewed as an automatic determination that something is of higher risk.

apply requirements similar to those imposed under Schedule 2 of the AMLO (or these Guidelines) for jurisdictional equivalence purposes. When doing so practices should document their assessment of the jurisdiction in question, which may include consideration of the following factors:

(a) membership of a regional group of jurisdictions that admit jurisdictions that have demonstrated a commitment to combating ML/TF, and which have an appropriate legal and regulatory regime to back up this commitment;

(b) mutual evaluation reports. Particular attention should be paid to assessments that have been undertaken by the FATF, FATF-style regional bodies, the International Monetary Fund and the World Bank. Practices should however bear in mind that mutual evaluation reports are at a "point in time";

(c) lists of jurisdictions published by the FATF with strategic AML/CFT deficiencies through the International Co-operation Review Group processes;

(d) information that may be circulated by the Institute from time to time alerting practices to jurisdictions regarded as having poor AML/CFT controls;

(e) lists of jurisdictions, entities and individuals that are involved, or that are alleged to be involved, in activities that cast doubt on their integrity in the AML/CFT area, published by specialised national, international, non-governmental and commercial organisations (e.g., Transparency International's "Corruption Perceptions Index"; and

(f) guidance provided at paragraph 3.13.28.

3.14.3 The judgment of equivalence is for practices to make in the light of the particular circumstances, and senior management may need to substantiate this judgment. Therefore, it is important that the reasons for concluding that a particular jurisdiction (other than another FATF member) is equivalent are documented at the time and that the decision is made on up-to-date and relevant information. A record of the assessment performed and factors considered should be retained for regulatory scrutiny and periodically reviewed to ensure it remains up to date and valid.

Section 4: ONGOING MONITORING

General requirements

4.1 Effective ongoing monitoring is vital for understanding of clients' business and an integral part of effective AML/CFT controls. It helps practices to know their clients and to detect unusual or suspicious transactions.

4.1.1 **Where applicable, practices should monitor their business relationships with clients by:**

(a) reviewing from time to time documents, data and information relating to the client, obtained by the practice for the purposes of complying with AMLO, to ensure that they are up to date and relevant;

(b) paying attention to transactions carried out for the client to ensure that they are consistent with the practice's knowledge of the client and the client's nature of business, risk profile and source of funds. An unusual activity may be in the form of one that is inconsistent with the expected pattern for that client, or with the normal business activities for the type of product or service that is being delivered; and

(c) identifying transactions that are complex, involve unusually large sums, or unusual patterns of activity, which have no apparent economic or lawful purpose, and examining the background and purposes of those transactions and recording their written findings.

4.1.2 A failure to conduct proper ongoing monitoring could expose practices to potential abuse by criminals, and may call into question the adequacy of controls, or the prudence and integrity of a practice's management.

4.1.3 Possible characteristics practices should consider monitoring include:
(a) the nature and type of activities (e.g., abnormal amounts or frequency);
(b) the nature of a series of transactions;
(c) the amount of any transactions, paying particular attention to particularly substantial transactions;
(d) the geographical origin/destination of a payment or receipt; and
(e) the client's normal activity or turnover.

4.1.4 Practices should be vigilant for significant changes regarding the basis of the business relationship with the client over time. These may include where:
(a) new products or services that pose higher risk are entered into;
(b) new corporate or trust structures are created;
(c) the stated activity or turnover of a client changes or increases; or
(d) the nature of activities changes or their frequency or size increases etc.

4.1.5 Where the basis of the business relationship changes significantly, practices should carry out further CDD procedures to ensure that the ML/TF risk involved and basis of the relationship are fully understood. Ongoing monitoring procedures should take account of the above changes.

4.2 RBA in relation to monitoring

4.2.1 The extent of monitoring should be linked to the risk profile of the client, determined through

the risk assessment. To be most effective, resources should be targeted towards business relationships presenting a higher risk of ML/TF. At the same time practices should also periodically review the risk profile of their clients generally as part of their ongoing monitoring, and may need to re-categorise individual clients, as appropriate.

4.2.2 Practices should take additional measures, such as more frequent and intensive monitoring, when monitoring relationships that are assessed as posing a higher risk, e.g., where (a) a client has not been physically present for identification purposes, or (b) a client, or a beneficial owner of a client is known to the practice, from publicly-known information or information in its possession, to be a PEP.

Methods and procedures

4.2.3 When considering how best to monitor client relationships and transactions, factors that practices may take into account include:

(a) the size and complexity of their business;
(b) their assessment of the ML/TF risks arising from their business; the nature of their systems and controls;
(c) the monitoring procedures that already exist to satisfy other business needs; and
(d) the nature of the services provided to clients (which includes the means of delivery or communication).

4.2.4 Where transactions are complex, unusually large or involve unusual patterns of activity, and have no apparent economic or lawful purpose, practices should examine the background and purpose, including, where appropriate, the circumstances, of the transactions. The findings of these examinations should be properly documented in writing. Proper records of decisions made, by whom, and the rationale for them will help to demonstrate that a practice is handling unusual or suspicious activities appropriately.

4.2.5 Such examinations may include asking the client common sense questions that a reasonable person would ask in the circumstances. Such enquiries, when conducted properly, and in good faith, should not constitute tipping off (see Section 5) and are directly linked to the CDD requirements. Such enquiries and their results should be properly documented. Where there is a suspicion of ML/TF, a report should be made internally to the MLRO, and if he/she comes to the same conclusion, an STR should be made to the JFIU. The documentation referred to in paragraphs 4.2.4 should be available to assist the Institute and other relevant authorities, where necessary.

Pre-existing clients

4.2.6 In relation to pre-existing clients, when practices carry out their responsibilities in relation to ongoing monitoring before they first conduct CDD measures in relation to the client, in accordance with the requirements of the AMLO, practices are required to review only the documents, data and information relating to the client that are held by them at the time that they conducts the review.

Section 5: MAKING SUSPICIOUS TRANSACTION REPORTS

General requirements[24]

5.1 OSCO and DTROP (section 25A) require a person to report if he/she knows or suspects any property to be the proceeds of an indictable offence or drug trafficking, respectively. UNATMO (section 12(1)) requires a person to report if he/she knows or suspects that any property is terrorist property.

5.1.1 **Once knowledge or suspicion of an ML/TF transaction or activity has been established, the following general principles should be applied:**

(a) Practices should make a report even where no service has been provided[25];

(b) the report should be made as soon as is reasonably practical after the suspicion or knowledge is first established; and

(c) practices should ensure that they have in place internal controls to prevent any partner, director, or employee committing the offence of "tipping off" the client, or any other person who is the subject of the report. Practices should also take care that their line of enquiry with clients is such that tipping off cannot be construed to have taken place.

5.2 Legal requirements in relation to making suspicious transaction reports

5.2.1 Under sections 25A(1) of DTROP/ OSCO, a person should make a disclosure to an authorised officer as soon as it is reasonable for him/her to do so, if he/she knows or suspects that any property:
(a) in whole or in part, directly or indirectly, represents the proceeds of [26];
(b) was used in connection with; or
(c) is intended to be used in connection with,
an indictable offence/drug trafficking.

5.2.2 It is an offence under section 25A, carrying a maximum penalty of three months imprisonment and a fine at level 5[27], to fail to disclose to an authorised officer where a person knows or suspects any of the above matters

5.2.3 Under section 12(1) of UNATMO, where a person knows or suspects that any property is terrorist property, the person should disclose to an authorised officer the information or other matter:
(a) on which the knowledge or suspicion is based; and
(b) as soon as is practicable after that information or other matter comes to the person's attention.

---

[24] See also the Institute's frequently-asked questions on suspicious transaction reporting.

[25] The reporting obligations of section 25A(1) DTROP/OSCO and section 12(1) UNATMO apply to "any property" and require a person to report suspicions of ML/TF, irrespective of the amount involved. These provisions establish a reporting obligation whenever a suspicion arises, without reference to transactions *per se*. Thus, the obligation to report applies whether or not a transaction was actually conducted and also covers attempted transactions.

[26] OSCO and DTROP, section 25A(1).

[27] Standard levels of fines under various ordinances are specified in Schedule 8, Criminal Procedure Ordinance.

5.2.4 Failure to disclose knowledge or suspicion of terrorist property is an offence under section 14(5) of UNATMO, carrying a maximum penalty of three months imprisonment and a fine at level 5.

5.2.5 If a person who has made the necessary disclosure contravenes section 25(1) of DTROP/ OSCO, which relates to dealing with property that represents the proceeds of an indictable offence/drug trafficking, sections 7 or 8 of UNATMO (on the provision or collection of property to commit terrorist acts, or making property available to, or collecting for, terrorists or terrorist associates), and the disclosure relates to that act, he/she does not commit an offence, if the disclosure is made:

(a) before he/she acts, and that act is done with the consent of an authorised officer; or

(b) after he/she acts, and the disclosure is made on his/her own initiative, as soon as it is reasonable for him/her to make it.[28]
DTROP

(See Appendix A for further information on DTROP, OSCO and UNATMO)

5.2.6 Filing an STR to the JFIU provides a statutory defence to the offence of ML/TF in respect of the acts disclosed in the report, provided:

(a) the STR is made before a practice undertakes the disclosed acts and the acts are undertaken with the consent of the JFIU; or

(b) the STR is made after a practice has performed the disclosed acts and the report is made on the practice's own initiative and as soon as it is reasonable for the practice to do so.

5.2.7 A disclosure under section 25A of DTROP/OSCO or section 12 of UNATMO will not be a breach of contract, enactment, rule of conduct, or provision restricting disclosure of information. The person making the disclosure will not be liable in damages for loss arising out of the disclosure.[29]

5.2.8 Once an employee has reported his suspicion to an appropriate person (see Section 2 on the appointment and roles of an MLRO) and in accordance with the procedure established by his/her employer for the making of such disclosures, he/she has fully satisfied the statutory obligation.

5.2.9 CDD and ongoing monitoring provide the basis for recognising unusual and suspicious transactions and events. The key is to know enough about the client's business to recognise that an activity or transaction, or a series of transactions, is unusual and, from an examination of the unusual, to be able to conclude whether there is a suspicion of ML/TF.

5.2.10 Practices should ensure members of staff are aware of their statutory responsibilities and that sufficient guidance and training are given to staff to enable them to recognise when ML/TF may be taking place[30]. Staff also need to be sensitive to the risk of tipping off during their client work (see paragraphs 5.2.19 -5.2.26).

5.2.11 Where a practice conducts enquiries and obtains what it considers to be a satisfactory

[28] OSCO/ DTROP, section 25A(2); UNATMO, section 12(2).

[29] OSCO/ DTROP, section 25A(3); UNATMO section 12(3).

[30] See Section 8 of these Guidelines for further information on staff hiring and training.

explanation of the activity or transaction, it may conclude that there are no grounds for suspicion, and therefore take no further action. However, where the enquiries do not provide a satisfactory explanation of the activity or transaction, it may conclude that there are grounds for suspicion and should make a disclosure[31].

5.2.12 For a person to have knowledge or suspicion, he/she does not need to know the nature of the criminal activity underlying the ML, or that the funds themselves definitely arose from the criminal offence.

5.2.13 General suspicious transactions indicators and further examples of situations that could give rise to suspicions are provided in Appendix D. The examples are not intended to be exhaustive and only provide indications of the most basic ways in which money may be laundered. However, identification of any of the circumstances similar to those listed in Appendix D, may prompt further investigations and, at least, be a trigger for making initial enquiries about the source of funds and the nature of the client's activities.

5.2.14 Practices should also be aware of elements of individual transactions that could indicate property involved in TF. The FATF has issued Guidance for FIs in detecting TF, which may also be a useful reference for practices.

Timing and manner of reports

5.2.15 When practices know or suspect that any property represents the proceeds of crime or terrorist property, an STR should be made to the JFIU, as soon as it is reasonable to do so. The use of a standard form or the use of the e-channel "STREAMS"[32] by registered users is encouraged by the JFIU. Further details of reporting methods and advice may be found on the JFIU website. In the event that an STR is urgent, particularly when the matter is part of an ongoing investigation, this should be indicated in the STR. Where exceptional circumstances exist in relation to an urgent STR, an immediate notification to the JFIU by telephone would be desirable.

5.2.16 Depending on when knowledge or suspicion arises, an STR may be made either before a suspicious transaction or activity occurs (whether the intended transaction ultimately takes place or not), or after a transaction or activity has been completed.

5.2.17 The law requires the STR to be made together with any matter on which the knowledge or suspicion is based. The need for prompt disclosures is especially important where a client has instructed a practice to move funds or other property, make cash available for collection, or carry out significant changes to the business relationship. In such circumstances, an urgent notification to the JFIU by telephone would be desirable.

5.2.18 Knowledge or suspicion that any property represents the proceeds of an indictable offence should normally be reported within the jurisdiction where the knowledge or suspicion arises and where the records of the related activities are held. However, in certain cases, e.g., when there is a very clear nexus with Hong Kong, even though the knowledge or suspicion arises outside Hong Kong, reporting to the JFIU[33] may be required, but only if section 25A of

---

[31] See: http://www.jfiu.gov.hk/en/str.html

[32] STREAMS (Suspicion Transaction Report and Management System) is a web-based platform to assist in the receipt, analysis and dissemination of STRs. Use of STREAMS is recommended, especially for practices which make frequent reports. Further details may be obtained from the JFIU.

[33] Section 25(4) of OSCO stipulates that an indictable offence includes conduct outside Hong Kong which would constitute an indictable offence if it had occurred in Hong Kong. Therefore, where a practice in Hong Kong has information regarding

OSCO/DTROP applies.

Tipping off

5.2.19 A person commits an offence of "tipping off", under DTROP/OSCO or UNATMO[34], if, knowing or suspecting that an STR has been made (under section 25A(1) or (4) of OSCO/ DTROP, or section 12(1) or (4) of UNATMO), he/she discloses to any other person any matter that is likely to prejudice an investigation that might be conducted following the original disclosure. An offence of tipping off carries a maximum penalty, upon conviction, of imprisonment for three years and a fine of HK$500,000.

5.2.20 Therefore, persons who know or suspect that an STR has been made should ensure that no information is given to any person who is likely to prejudice the investigation of the disclosure, to avoid triggering tipping-off.

5.2.21 A risk exists that clients could be unintentionally tipped off when practices are seeking to extend their CDD obligations during the establishment or course of the business relationship, or when conducting occasional or ad hoc transactions or services. If further enquiries of a client become necessary, where it is known or suspected that an STR has already been made, the client must not be made aware that relevant agencies have been alerted of his/her name.

5.2.22 A client's awareness of a possible STR or investigation could prejudice future efforts to investigate the suspected ML/TF operation. Therefore, if practices form a suspicion that activities or transactions relate to ML/TF, they should take into account the risk of tipping off when completing the CDD process. Practices should ensure that their employees are aware of and sensitive to these issues when conducting CDD.

5.2.23 A person cannot be held liable for a tipping-off offence unless that person knows or suspects that an STR has been made, either internally or to the JFIU, or alternatively knows or suspects that the law enforcement agencies are conducting or intending to conduct an ML/TF investigation in relation to the persons or entities concerned.

5.2.24 Therefore, unless the enquiring staff member has knowledge or suspicion of a current or impending investigation, where a member practice seeks additional information during preliminary enquiries of a prospective client, this should not give rise to a tipping-off offence. However, if the enquiries lead to a subsequent report being made, then the client must not be informed or alerted.

5.2.25 It is a defence that it was not known or suspected that the disclosure was likely to prejudice an investigation. Therefore, where a practice communicates suspicions of ML/TF activities to a client's senior management, internal auditors, or other person responsible for monitoring, or reporting, ML/TF, the practice should first be satisfied, as far as possible, that:

(a) the persons to whom it is communicating its suspicions are not implicated in the suspected ML/TF; and
(b) the information communicated will not be passed to others who may prejudice the investigation or proposed investigation.

5.3 Internal reporting and recording

ML/TF, irrespective of the location, it should consider seeking clarification with and making a report to the JFIU.

[34] DTROP/OSCO section 25A(5); UNATMO section 12(5)

5.3.1 As indicated in Section 2, practices should appoint an MLRO as a central reference point for reporting suspicious transactions. The MLRO should:

(a) be responsible for making STRs to the JFIU;
(b) keep a register of all reports made to him/her by employees and to the JFIU;
(c) on request by the employee concerned, provide a written acknowledgement of a report made to him/her by an employee; and
(d) it is also advisable to keep a record of discussions regarding internal reporting.

5.3.2 Where staff members working in a practice have knowledge or suspicion of matters referred to in paragraphs 5.2.1 or 5.2.3, they should inform the MLRO, regardless of whether they believe an STR has already been made by another person to the JFIU or other authorities.

5.3.3 The MLRO should consider all internal disclosures he/she receives in the light of full access to all relevant documentation and other parties. However, the role of the MLRO should not simply be that of a passive recipient of ad hoc reports of suspicious transactions. He/she should play an active role in the identification and reporting of suspicious transactions. The MRLO should promptly evaluate, whether in his/her view, there are suspicious circumstances that would require a report to the JFIU. If there are, the MLRO should report all relevant details to the JFIU, without undue delay and should co-operate with any resulting JFIU investigation. If, on the other hand, a decision is made not to make an STR, the MRLO should document the reasons.

5.3.4 To enable the MLRO to fulfil his/her functions, practices should ensure that he/she receives full co-operation from all staff and access to all relevant documentation so that the MLRO is in a position to decide whether ML/TF is suspected or known.

5.3.5 When reporting suspicious transactions to the JFIU, sufficient information should be provided, including, e.g., the following details[35]:

(a) personal particulars of the person or company involved, e.g., name, identity card or passport number, date of birth, address, telephone number, and bank account number;
(b) details of the suspicious transaction;
(c) the reason why the transaction is suspicious, i.e., which suspicious activity indicators are present;
(d) the explanation, if any, given by the person about the transaction.

5.3.6 To assist the disclosure of all relevant information, JFIU has provided a form on its website. An STR to the JFIU can be made through STREAMS, by email, fax, mail or telephone. Details are available on the JFIU website.[36]

5.3.7 Practices should establish and maintain procedures to ensure that:

(a) all staff are made aware of the identity of the MLRO and of the procedures to follow when making an internal disclosure report; and
(b) all disclosure reports reach the MLRO without undue delay.

5.3.8 While practices may wish to set up internal systems that allow staff to consult with supervisors or managers before sending a report to the MLRO, in the normal course of events,

---

[35] http://www.jfiu.gov.hk/en/str.html#what.

[36] http://www.jfiu.gov.hk/en/str.html#how.

reports raised by staff should not be filtered out by supervisors or managers who have no responsibility for the ML reporting/ compliance function. The legal obligation is to report as soon as it is reasonable to do so, so reporting lines should be as short as possible with the minimum number of people between the staff with the suspicion and the MLRO. This ensures speed, confidentiality and accessibility to the MLRO.

5.3.9 All suspicious activities reported to the MLRO should be documented (in urgent cases this may follow an initial discussion by telephone). The report must include the full details of the client and as full a statement as possible of the information giving rise to the suspicion.

5.3.10 The MLRO should acknowledge receipt of the report and at the same time provide a reminder of the obligation regarding tipping off. The tipping-off provision includes circumstances where a suspicion has been raised internally, but has not yet been reported to the JFIU.

5.3.11 The reporting of a suspicion in respect of a transaction or event does not remove the need to report further suspicious transactions or events in respect of the same client. Further suspicious transactions or events, whether of the same nature or different to the previous suspicion, must continue to be reported to the MLRO who should make further reports to the JFIU, if appropriate.

5.3.12 When evaluating an internal report, the MLRO should take reasonable steps to consider all relevant information, including CDD and ongoing monitoring information available within or to the practice concerning the entity or entities to which the report relates. This may include:

(a) reviewing of other transaction patterns and volumes through connected accounts;
(b) reviewing any previous patterns of instructions, the length of the business relationship and reference to CDD and ongoing monitoring information and documentation; and
(c) appropriate questioning of the client per the systematic approach to identifying suspicious transactions recommended by the JFIU[37].

5.3.13 As part of the review, other clients and/or services may need to be examined. The need to search for information concerning, e.g., connected relationships should strike an appropriate balance between the statutory requirement to make a timely STR to the JFIU and any delays that might arise in searching for more relevant information concerning connected accounts or relationships. The evaluation process, along with any conclusions drawn, should be documented.

5.3.14 If, after completing the evaluation, the MLRO decides that there are grounds for knowledge or suspicion, he/she should disclose the information to the JFIU, together with the information on which that knowledge or suspicion is based, as soon as it is reasonable to do so after his/her evaluation is complete. Providing he/she acts in good faith in deciding not to file an STR with the JFIU, it is unlikely that there will be any criminal liability for failing to report if a MLRO concludes that there is no suspicion after taking into account all available information. It is however essential for MLROs to keep proper records of their deliberations and actions taken to demonstrate that they have acted reasonably. The MLRO may wish to obtain legal advice, as necessary.

5.3.15 In relation to section 25A(2) of OSCO/DTROP and section 12(2) of UNATMO, a member who has made a report should, where appropriate, seek permission from the JFIU to continue to perform his/her duties in relation to the client. Where applicable, such consent should be sought through the MLRO.

[37] For details, see: <www.jfiu.gov.hk>.

5.3.16 In certain circumstances, it may not be feasible to curtail a service that is known, or suspected, to be related to ML/TF, before informing the JFIU, or to do so would likely frustrate efforts to pursue the beneficiaries of a suspected ML/TF operation. Where possible, members should, nevertheless, alert the MLRO to the situation.

5.3.17 It is not an offence where a person, prior to making an STR, deals with property which he knows, or has reasonable grounds to believe, represents the proceeds of an indictable offence, provided that a disclosure is made on his/her own initiative, as soon as reasonable after performing the act (see paragraph 5.2.5).

5.3.18 While a practice may consider communicating its suspicions to a client's regulator if this is permitted and appropriate, this is not a substitute for reporting to the JFIU.

5.3.19 A practice may wish to terminate its relationship with a client that is being, or is likely to be, investigated. However, before terminating a relationship, the practice should consider liaising with the JFIU, or the investigation officer, to ensure that the termination does not tip off the client, or prejudice the investigation. In more complex situations, a practice may also wish to take legal advice on the implications of termination under the terms of the contract.

5.3.20 Practices should note that the statutory duty to make STRs, where applicable, overrides the duty of confidentiality owed to clients and, as indicated above (see paragraph 5.2.7), a disclosure made to the JFIU will be not be a breach of contract, enactment, rule of conduct or provision restricting the disclosure of information. The person who made it will not be liable in damages for loss arising out of the disclosure. At the same time it should be noted that this protection extends only to the disclosure of knowledge or suspicion of ML/TF, and any matter on which that knowledge or suspicion is based. STRs should be made in good faith and based on genuine knowledge or suspicion. If in doubt, practices should consider seeking legal advice before making a disclosure.

<u>Recording internal reports and reports to the JFIU</u>

5.3.21 Practices should establish and maintain a record of all ML/TF reports made to the MLRO. The record should include details of the date that the report was made, the staff members subsequently handling the report, the results of the assessment, whether the report resulted in a disclosure to the JFIU, and information to allow the papers relevant to the report to be located.

5.3.22 Practices should also establish and maintain a record of all STRs made to the JFIU. The record should include details of the date of the STR, the person who made the report, and information to allow the papers relevant to the STR to be located. This record may be combined with the record of internal reports, if considered appropriate.

5.4 Post reporting matters

5.4.1 Practices should note the following:

(a) filing an STR to the JFIU provides a statutory defence to ML/TF only in relation to the acts disclosed in that particular report. It does not absolve practices from the legal, reputational or regulatory risks associated with the continuing assignment or client relationship;

(b) a "consent" response from the JFIU to a pre-transaction STR should not be construed as a "clean bill of health" for the continuing assignment or client relationship, or an indication that the assignment or relationship does not pose a risk to the practice;

(c) practices should conduct an appropriate review of a business relationship upon the

filing of an STR to the JFIU, irrespective of any subsequent feedback provided by the JFIU;

(d) once practices have concerns about an assignment or a client relationship, they should take appropriate action to mitigate the risks. Filing an STR with the JFIU and continuing with the assignment relationship, without any further consideration of the risks and the imposition of appropriate controls to mitigate the risks identified, would not be a sufficient response;

(e) relationships reported to the JFIU should be subject to an appropriate review by the MLRO and, if necessary, the issue should be escalated to the practice's senior management to determine how to handle the relationship, in order to mitigate any potential legal or reputational risks, in line with the practice's business objectives, and its capacity to mitigate the risks identified; and

(f) practices are not obliged to continue assignments and/or client relationships if such action would place them at risk. It is recommended to indicate any intention to terminate an assignment or relationship in the initial STR to the JFIU, thereby allowing the JFIU to comment, at an early stage, on such a course of action.

5.4.2 The JFIU should acknowledge receipt of an STR made under section 25A of DTROP/OSCO or section 12 of UNATMO. If there is no need for imminent action, consent will usually be given in writing for the practice to continue with the relevant activity or transaction, under the provisions of section 25A(2) of DTROP/OSCO. For STRs submitted via "STREAMS", an e-receipt will be issued via the same channel. The JFIU may, on occasion, seek additional information or clarification of any matter on which the knowledge or suspicion is based.

5.4.3 Whilst there is no statutory requirement to provide feedback arising from investigations, the JFIU provides feedback both in its quarterly report[38] and upon request, to a disclosing practice in relation to the current status of an investigation.

5.4.4 After initial analysis by the JFIU, STRs that are to be pursued are allocated to financial investigation officers for further investigation. Practices should respond to production orders within the required time limit and provide the information or material that falls within the scope of such orders. Where a practice encounters difficulty in complying with the timeframes stipulated, the MLRO should at the earliest opportunity contact the officer-in-charge of the investigation for further guidance.

5.4.5 Upon the conviction of a defendant, a court may order the confiscation of relevant criminal proceeds and a practice may be served with a Confiscation Order, in the event that it holds property belonging to that defendant that is deemed by the courts to represent a benefit from the crime. A court may also order the forfeiture of property where it is satisfied that the property is a terrorist property.

5.5 Organisations other than member practices

5.5.1 Members working in organisations other than practices should ascertain whether their employers have procedures for making STRs through a CO/ MLRO. Employees that make reports in accordance with procedures laid down by their employers are regarded as complying with the relevant laws.[39] In the absence of any employer's procedures, STRs would need to be made direct to the JFIU.

---

[38] The purpose of the quarterly report, which is relevant to all financial sectors, is to raise AML/CFT awareness. It consists of two parts, (i) analysis of STRs and (ii) matters of interest and feedback. The report is available through the JFIU's website at www.jfiu.gov.hk. A password is required, details may be found under the typologies and feedback section of the website or by contacting the JFIU directly.

[39] DTROP and OSCO, s.25A(4) and UNATMO, s.12(4).

5.5.2 Members working in the banking, insurance and securities industries are advised to familiarise themselves with AMLO and guidelines on AML/CFT issued by the relevant financial services regulators. It should be noted that, under the AMLO, it is a criminal offence if a person who is an employee of an FI or is employed to work for an FI, or is concerned in the management of an FI, (i) knowingly, or (ii) with intent to defraud the FI or any relevant authority, causes or permits the FI to contravene a specified provision of the AMLO. The maximum penalty in the upon conviction on indictment, in the case of (i), is imprisonment for two years and fine of $1 million and, in the case of (ii), imprisonment for seven years and fine of $1 million[40].

[40] AMLO, s.5

Section 6: FINANCIAL SANCTIONS AND TERRORIST FINANCING

General requirements

6.1 In relation to financial sanctions and the financing of terrorism/ proliferation of weapons of mass destruction, practices should be aware of and comply with their legal obligations under Hong Kong's financial sanctions regime, which may include considering the need to make STRs.

6.1.1 TF generally refers to the carrying out of transactions involving property owned by terrorists, or that has been, or is intended to be, used to assist the commission of terrorist acts. Originally, this was not covered under the AML regime, where the focus is on the handling of criminal proceeds, i.e., the source of property is what matters. With terrorist financing, however, the focus is on the destination or use of property, which may have derived from legitimate sources.

6.1.2 The UN Security Council passed UN Security Council Resolution (UNSCR) 1373 (2001), which calls on all member states to act to prevent and suppress the financing of terrorist acts. Guidance issued by the UN Counter Terrorism Committee in relation to the implementation of UNSCRs regarding terrorism can be found at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/557/43/PDF/N0155743.pdf?OpenElement

6.1.3 The United Nations Sanctions Ordinance (Cap. 537) ("UNSO") requires the Hong Kong chief executive to make regulations to implement sanctions decided by the Security Council of the United Nations against places outside the People's Republic of China, including targeted sanctions against designated individuals or entities.

6.1.4 These sanctions include financial sanctions which prohibit making funds available or dealing with any funds, or economic resources, for the benefit of or belonging to a designated individual or entity. In addition to FIs, these are also relevant to DNFBPs, including accountants, and practices should take steps to keep themselves informed of the latest list of designated individuals and entities, proscribed parties, etc.

6.1.5 The Institute may inform members from time to time of designations published in the Government Gazette pursuant to regulations made under the UNSO.

6.1.6 While practices will not normally have any obligation under Hong Kong law to have regard to lists issued by other organisations or authorities in other jurisdictions, practices with overseas offices may need to be aware of the scope and focus of relevant financial/trade sanctions regimes in those jurisdictions.

6.1.7 The chief executive of the Hong Kong SAR can grant licences for making funds and economic resources available to a designated individual or entity, if specific requirements stipulated in the regulations made under the UNSO are met. For enquiries on this subject, practices should approach the Commerce and Economic Development Bureau.

Terrorist financing and proliferation of weapons of mass destruction

6.1.8 The UN has also published the names of individuals and organisations subject to UN financial sanctions in relation to involvement with Usama bin Laden, Al-Qa'ida, and the Taliban under relevant UNSCRs (e.g., UNSCR 1267 (1999), 1390 (2002) and 1617 (2005)). All UN member states are required under international law to freeze the funds and economic resources of any

legal person(s) named in this list and to report any suspected name matches to the relevant authorities.

6.1.9 UNATMO was enacted in 2002 to give effect to the mandatory elements of UNSCR 1373 and the FATF's special Rs on terrorist financing.

6.1.10 The secretary for security ("S for S") has the power to freeze suspected terrorist property and may direct that a person shall not deal with the frozen property except under the authority of a licence. Contraventions are subject to a maximum penalty of 7 years imprisonment and an unspecified fine.

6.1.11 Section 8 of UNATMO does not affect a freeze per se; it prohibits a person from (i) making available any property or financial services to, or for the benefit of, a person he/she knows, or has reasonable grounds to suspect, is a terrorist or terrorist associate, in the absence of a licence granted by S for S; and (ii) collecting property or soliciting financial (or related) services for the benefit of a person he/she knows, or has reasonable grounds to suspect, is a terrorist or terrorist associate. Contraventions are subject to a maximum sentence of 14 years imprisonment and an unspecified fine.

6.1.12 S for S can license exceptions to the prohibitions to enable frozen property and economic resources to be unfrozen and to allow payments to be made to, or for the benefit of, a designated party under UNATMO.

6.1.13 Where a person is designated by a Committee of the UNSC as a terrorist, generally, that person's details will subsequently published in a notice under section 4 of UNATMO in the Government Gazette.

6.1.14 The Weapons of Mass Destruction (Control of Provision of Services) Ordinance (Cap. 526), section 4, makes it an offence for a person to provide any services where that person believes or suspects, on reasonable grounds, that those services may be connected to weapons of mass destruction proliferation. The provision of services is widely defined and includes the lending of money or other provision of financial assistance.

6.1.15 For lists of designated persons, reference may be made to various sources, including relevant designations by overseas authorities, such as the designations made by the US Government under relevant Executive Orders. The Institute may draw practices' attention to such designations from time to time.

6.1.16 Practices should have controls in place to conduct checks against relevant lists of terrorists, etc., for screening purposes and to ensure that their sources of information are up to date.

6.2 Database maintenance and screening (clients and payments)

6.2.1 Practices should establish CFT policies and procedures. They should take measures to ensure compliance with the relevant regulations and legislation on TF. Staff should be made aware of their legal obligations and suitable guidance and training should be provided to them. The controls for identification of suspicious transactions should cover TF as well as ML.

6.2.2 It is important that practices should be able to identify and report transactions with terrorist suspects and designated parties. They should, therefore, consider maintaining a list or database of names and particulars of terrorist suspects and designated parties, which consolidates the various lists that have been made known to them, or making arrangements to access lists or databases maintained by third party service providers.

6.2.3 Practices should ensure that the relevant designations are included on any list or in any database that they maintain. It should, in particular, include the lists published in the Government Gazette and those designated under the US Executive Order 13224. It should also be subject to timely update when there are changes, and made easily accessible by staff for the purpose of identifying suspicious transactions.

6.2.4 Ongoing screening of practices complete client base is an important part of the internal controls to prevent TF and sanction violations, and may be achieved by:

(a) screening clients against current terrorist and sanction designations at the establishment of the relationship; and

(b) as soon as practicable after new terrorist and sanction designations are made known, or come to the attention of a practice, ensuring that these new designations are screened against a practice's client base.

6.2.5 Where relevant, the screening procedures should extend to the connected parties of the client using an RBA.

6.2.6 Enhanced checks should be conducted before establishing a business relationship or processing a transaction, where possible, if there are circumstances giving rise to suspicion.

6.2.7 In order to be able demonstrate compliance with the provisions of this section, the screening and any results should be documented or recorded electronically.

6.2.8 If practices suspect that an activity or transaction is terrorist related, they should make an STR to the JFIU. Even if there is no evidence of a direct terrorist connection, the activity or transaction should still be reported to the JFIU if it looks suspicious, as it may emerge subsequently that there is a terrorist link.

6.2.9 The legislation in Hong Kong provides exemptions from civil and criminal liability which would apply to practices when sharing third-party information obtained from their clients for the purpose of preventing and suppressing the financing of terrorist acts. The sharing of information potentially relating to TF is not restricted by the Personal Data Privacy Ordinance (Cap. 486).

6.2.10 Where an STR is made pursuant to paragraph 6.2.8, practices must not disclose to another person any information or matters, which are likely to prejudice the investigation, as tipping-off is an offence under UNATMO.

Section 7: RECORD-KEEPING

General requirements

7.1 Practices should prepare, maintain and retain documentation and records on their business relations with, and any transactions for, clients as are necessary and sufficient to achieve the RK objectives indicated below and fulfil any related legal or regulatory requirements, and which are appropriate to the scale, nature and complexity of their businesses. The records maintained must be sufficient to ensure that:

(a) any client and, where appropriate, the beneficial owner of the client, can be properly identified and verified;

(b) the audit trail for particular transactions and, where applicable, property dealt with by a practice that relates to any client and, where relevant, the beneficial owner of the client, is clear and complete;

(c) the original or suitable copies of all relevant client and transaction records and information can be made available on a timely basis to the Institute or other relevant authority, upon appropriate authority;

(d) practices are able to show evidence of compliance with any relevant requirements specified in other sections of these Guidelines (e.g., relating to client identification and verification, risk assessments, STRs and internal reports, staff training);

(e) records in relation to particular transactions and clients should be retained for six years after the transaction has been completed or the business relationship has ended, respectively.

7.1.1 RK is an essential part of the AML/CFT regime and can facilitate the detection, investigation and confiscation of criminal or terrorist property or funds. RK can help investigating authorities to establish a profile of a suspect and trace criminal or terrorist property or funds, and can assist the court to examine all relevant past businesses activities to assess whether the property or funds are the proceeds of, or relate to, criminal or terrorist offences.

7.1.2 Records should be kept of clients' identity, the supporting evidence of verification of identity (including the original and any updated records), the practice's business relationships with them (including any non-engagement related documents relating to the client relationship) and details of any occasional transactions and monitoring of the relationship. Historic as well as current records should be retained.

7.1.3 Practices should also store securely information relating to both internal reports received by the MLRO and disclosures to the JFIU. It is also advisable that evidence of assessment of the training needs of staff and steps taken to meet those needs be retained.

7.2 Retention of records relating to client identity and business relationships

7.2.1 Practices should keep:

(a) 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 clients, beneficial owners of the client, beneficiaries and persons who purport to act on behalf of the

client and other connected parties of the client;

(b) any additional information on a client and/or beneficial owner of the client that may be obtained for the purposes of EDD or ongoing monitoring;

(c) where applicable, the original or a copy of the documents, and a record of the data and information, on the purpose and intended nature of the business relationship;

(d) the original or a copy of business correspondence[41] with the client and any beneficial owner of the client (which, at a minimum, should include business correspondence material to CDD measures or significant changes to the business relationship or activities)

(e) the original or a copy of the documents, and a record of the data and information, obtained in connection with occasional transactions, which should be sufficient to permit reconstruction of individual transactions or business engagements.

All relevant documents and records should be kept throughout the business relationship with or transaction for the client and, under the AMLO, retained for a period of six years after the end of the business relationship or transaction. Information relating to both internal reports and STRs should be retained for at least the same period (i.e., at least six years after receipt by the MLRO). Staff training records should be retained for a similar period. Either the original document or information, or an electronic copy, should be retained.

7.2.2 As practices need to maintain records for a wide range of purposes that comply with legal and professional requirements for the retention of documentation, the general documentation retention systems employed within the practice may be sufficient, provided that they are of an adequate scope and standard.

7.2.3 Records of internal reports are not considered to form part of client assignment working papers, and so it is advisable that such records are kept in a secure form, separately from the practice's normal methods for retaining client work documents. This is to guard against inadvertent disclosure to any party who may have or seek access to the client working paper files, where AML/CFT matters are not relevant to the purpose for which they are examining the file.

7.3 Manner in which records are to be kept

7.3.1 The AMLO states that records required to be kept under section 20 of this Schedule 2 must be kept in the following way:

(a) if the record consists of a document, either (i) the original of the document must be kept; or (ii) a copy of the document must be kept either on microfilm or in the database of a computer;

(b) if the record consists of data or information, a record of the data or information must be kept either on microfilm or in the database of a computer.

7.3.2 Irrespective of where identification and transaction records are held, practices are required to comply with all legal and regulatory requirements in Hong Kong.

[41] Practices are not expected to keep each and every piece of correspondence, such as a series of emails with the client; the expectation is that sufficient correspondence is kept to demonstrate compliance with the Guidelines and to enable STRs to be substantiated and effectively followed up.

Section 8: STAFF HIRING AND TRAINING

8.1 **Practices' AML/CTF policies, procedures and controls should extend to employee hiring and training.**

8.1.1 As indicated in Section 2, the development of internal policies, procedures and controls should include screening procedures to ensure adequate standards when hiring employees. It is in the practices own interest to hire people who are capable of complying with the fundamental principles.

8.1.2 Staff training is an important element of an effective system to prevent and detect ML/TF activities. The effective implementation of even a well-designed internal control system can be compromised if staff members using the system are not adequately trained.

8.1.3 Practices should provide appropriate AML/CFT training to their staff and should have a clear and well-articulated policy for ensuring that relevant members of staff receive adequate AML/CFT training.

8.1.4 The timing and content of training for different groups of staff may be adapted by practices for their own needs, with due consideration given to the size and complexity of their business and the type and level of ML/TF risk. The frequency of training should be sufficient to ensure that members of staff maintain up-to-date AML/CFT knowledge and competence. Staff should be trained in what they need to do to carry out their particular role with respect to AML/CFT. This is especially important before new staff commence work.

8.1.5 Staff members should be made aware of:

(a) The practice's statutory obligations and their own role in relation to AMLO, particularly Schedule 2 of AMLO;
(b) the practice's and their own statutory obligations to report suspicious transactions under DTROP, OSCO and UNATMO, and the possible consequences of breaches of these obligations;
(c) other statutory and regulatory obligations in respect of AML/CFT under DTROP, OSCO, UNATMO, and UNSO that may concern the practice and themselves, and the possible consequences of breaches of these obligations;
(d) the practice's controls (policies and procedures) relating to AML/CFT, including suspicious transaction identification and reporting; and
(e) new and emerging techniques, methods, trends, etc. in ML/TF, to the extent that such information is needed by the staff to carry out their particular roles in the practice with respect to AML/CFT.

8.1.6 Depending on the seniority and nature of work of different groups of staff, training may include:

(a) an introduction to the background to ML/TF and the importance placed on ML/TF by the practice;
(b) the need to identify and report suspicious transactions to the MLRO, and information on the offence of "tipping-off";
(c) training in circumstances that may give rise to suspicion, and relevant policies and procedures, including, for example, lines of reporting and when extra vigilance might be required (e.g., circumstances requiring EDD);
(d) appropriate training on client verification and relevant processing procedures.

COs and other managerial staff, including internal audit may require additional, higher-level

training covering:

(a) all aspects of the practice's AML/CFT regime;

(b) the practice's controls (policies and procedures) in relation to CDD and RK requirements that are relevant to their job responsibilities;

(c) specific training in relation to their responsibilities for supervising or managing staff, auditing the system and performing random checks, as well as making STRs to the JFIU.

MLROs[42] may require more specific training:

(a) on their responsibilities for assessing STRs submitted to them and making STRs to the JFIU; and

(b) to keep abreast of AML/CFT requirements/developments generally.

8.1.7 Practices may consider including available FATF papers and typologies as part of the training materials. All materials should be up to date and in line with current requirements and standards.

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

8.1.9 Practices should monitor the effectiveness of the training. This may be achieved by:

(a) checking staff's understanding of the practice's policies and procedures to combat ML/TF, the understanding of their statutory and regulatory obligations, and also their ability to recognise suspicious transactions and the risks of tipping off; and

(b) monitoring the compliance of staff with the practice's AML/CFT controls, as well as monitoring the quality and quantity of internal reports, so that further training needs may be identified and appropriate action can be taken.

[42] As noted in Section 2, in some practices, the CO and the MLRO may be the same person

APPENDIX A: Further information on the FATF, ML/TF and relevant legislation

Background on FATF

1. FATF is an inter-governmental body formed in 1989 that sets the international AML standards. Its mandate was expanded in October 2001 to CFT. In order to ensure full and effective implementation of its standards at the global level, the FATF monitors compliance by conducting evaluations on jurisdictions and undertakes stringent follow-up after the evaluations, including identifying high-risk and uncooperative jurisdictions which could be subject to enhanced scrutiny by the FATF or counter-measures by the FATF members and the international community at large. Many major economies have joined the FATF which has developed into a global network for international cooperation that facilitates exchanges between member jurisdictions.

2. As a member of the FATF, Hong Kong is obliged to implement the AML/CFT requirements as promulgated by the FATF, which include the 40 Recommendations and the Nine Special Recommendations and it is essential that Hong Kong complies with the international AML/CFT standards in order to safeguard its reputation and standing as an international financial centre.

Processes commonly involved in ML

3. There are three common stages in ML, and they frequently involve numerous transactions. Practices should be alert to any such signs for potential criminal activities. These stages are:
   (a) Placement - the physical disposal of cash proceeds derived from illegal activities;
   (b) Layering - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of the money, subvert the audit trail and provide anonymity; and
   (c) Integration - creating the impression of apparent legitimacy to criminally derived wealth. In situations where the layering process succeeds, integration schemes effectively return the laundered proceeds back into the general financial system and the proceeds appear to be the result of, or connected to, legitimate business activities.

DTROP and OSCO

4. DTROP, which was introduced in 1989, provides for the tracing, confiscation and recovery of the proceeds of drug trafficking and creates a criminal offence of laundering such proceeds. OSCO was introduced in 1994 and key provisions of it were modelled on DTROP. OSCO extends the scope of the money laundering offences to cover the proceeds of indictable offences generally.

5. Some of the relevant provisions of DTROP and OSCO are summarised below.

Dealing in the proceeds of crime

6. Under section 25 of both DTROP and OSCO, it is a serious offence, carrying a maximum penalty, upon conviction, of 14 years' imprisonment and a fine of five million dollars, to deal with any property, knowing or having reasonable grounds to believe that it, in whole or in part, directly or indirectly, represents the proceeds of an indictable offence. "Dealing" has quite a wide definition, including receiving or acquiring, disguising and disposing of property.

7. As regards the interpretation of "having reasonable grounds to believe", in the recent case of *HKSAR v Pang Hung Fai*[43], the Court of Final Appeal ("CFA"), referencing the judgment of the

[43] Paragraphs 52 and 70 of *HKSAR v Pang Hung Fai* [2014] HKCFA 96; *Seng Yuet Fong v HKSAR* [1999] 2 HKC 833 at 836E-F.

Appeal Committee of the CFA, in *Seng Yuet Fong v HKSAR*, stated: "To convict, the jury had to find that the accused had grounds for believing; and there was the additional requirement that the grounds must be reasonable: That is, that anyone looking at those grounds objectively *would* so believe." (Emphasis added).

8. The CFA also considered that the terminology of "subjective" and "objective" tests, which had appeared in decisions following the line of authority from the case of *HKSAR v Shing Siu Ming & Others*, was unnecessarily complicated and liable to confuse.

9. "Proceeds of an offence" has a broad definition that include payments or rewards, property derived from such payments or rewards, or any financial advantage (which could include, e.g., a cost saving).

10. "Indictable offence" is defined in the Crimes Ordinance (Cap. 200), as "any offence other than an offence which is triable only summarily". This means that an offence that may be tried either summarily or on indictment is regarded as an indictable offence for the purposes of DTROP/ OSCO, and consequently the range of relevant offences is broad. The offences listed in Schedules 1 and 2 of OSCO are examples of indictable offences.

11. Various court decisions have interpreted the offence under section 25 quite widely. For example, it is unnecessary for the prosecution to prove that a specific indictable offence has been committed[44] or to specify an indictable offence in the charge[45].

12. It is a defence to a charge of dealing for a person to prove that, as required under section 25A(1):
    (a) he/she had intended to disclose knowledge or suspicion that property represented the proceeds of, was used or was intended to be used in connection with, an indictable offence, together with any matter on which that knowledge or suspicion was based, to an authorised officer, as soon as it was reasonable for him/her to do so; and
    (b) he/she has a reasonable excuse for his/her failure to make a disclosure.

13. It should be noted that, references to an indictable offence in sections 25 and 25A of OSCO/ DTROP include conduct outside of Hong Kong that would have constituted an indictable offence had it taken place here. Therefore, it may be an offence for a person to deal with criminal proceeds, under section 25(1), or fail to disclose, under section 25A(1), even if the relevant action or crime took place outside Hong Kong. This provision should not be interpreted too narrowly. For example, the evasion of taxes in another jurisdiction may be an indictable offence in this context, even though the specific type of tax in question, e.g., capital gains tax, may not exist in Hong Kong. On the other hand, this does not imply that, ordinarily, a person is expected to know the law of other jurisdictions, or that a person could be in breach of the law in Hong Kong if he acted in a particular way without having such knowledge.

Reporting suspicious transactions

14. As explained in section 5 of these Guidelines, both OSCO and DTROP have requirements, under section 25A, to report suspicious transactions, which apply to everybody in Hong Kong. A person should make a disclosure to an authorised officer as soon as it is reasonable for him/her to do so, if he/she knows or suspects that any property:

---

[44] *HKSAR v Li Ching* CACC 436/1997; [1997] 4 HKC 108; *HKSAR v Wong Ping Shui & Others* [2000] 1 HKC 600, which was affirmed by the Appeal Committee of the Court of Final Appeal in FAMC 1/2001.

[45] *HKSAR v Lam Hei Kit* FAMC 27/2004.

(a) in whole or in part, directly or indirectly, represents the proceeds of an indictable offence;
(b) was used in connection with an indictable offence; or
(c) is intended to be used in connection with an indictable offence.

15. "Authorised officer" means:
(a) any police officer;
(b) any member of the Customs and Excise Service established by section 3 of the Customs and Excise Service Ordinance (Cap. 342); and
(c) any other person authorised in writing by the Secretary for Justice for the purposes of this Ordinance.

16. An offence of failing to make a disclosure, in accordance with section 25A, carries a maximum penalty, upon conviction, of imprisonment for three months and a fine at level 5.

17. There are other provisions in OSCO/DTROP, regarding investigation and access to information, of which members may wish to take note.

UNATMO

18. UNATMO is directed primarily towards implementing Resolution 1373 of the United Nations Security Council, dated 28 September 2001, to prevent the financing of terrorist acts. Among other things, it criminalises the supply of funds and making funds, or financial services, available to terrorists or terrorist associates. It permits terrorist property to be frozen and subsequently forfeited.

Reporting under UNATMO

19. UNATMO, which was introduced in 2002, requires a person to report to an authorised officer if he knows or suspects that any property is terrorist property.[46]

20. Relevant definitions under UNATMO include the following:

"Authorised officer" means:
(a) a police officer;
(b) a member of the Customs and Excise Service established by section 3 of the Customs and Excise Service Ordinance (Cap. 342);
(c) a member of the Immigration Service established by section 3 of the Immigration Service Ordinance (Cap. 311); or
(d) an officer of the Independent Commission Against Corruption established by section of the Independent Commission Against Corruption Ordinance (Cap. 204).

"Terrorist property" means:
(a) the property of a terrorist or terrorist associate; or
(b) any other property consisting of funds that:
(i) is intended to be used to finance or otherwise assist the commission of a terrorist act; or
(ii) was used to finance or otherwise assist the commission of a terrorist act.

"Terrorist" means a person who commits, or attempts to commit, a terrorist act, or participates in,

[46] UNATMO, section 12(1)

or facilitates the commission of, a terrorist act.

"Terrorist act" refers to the use, or threat, of action, where this is intended to:

(a) cause serious violence against a person;
(b) cause serious damage to property;
(c) endanger a person's life, other than that of the person committing the action;
(d) create serious risk to the health or safety of the public or a section of the public;
(e) seriously interfere with or seriously disrupt an electronic system; or
(f) seriously interfere with or seriously disrupt an essential service, facility or system,whether public or private; and
(g) and the use or threat is:
    (i) intended to compel the government, or to intimidate the public, or a section of the public; and
    (ii) made for the purpose of advancing a political, religious or ideological cause.

(Paragraphs (d), (e) and (f) do not include the use or threat of action in the course of any advocacy, protest, dissent or industrial action.)

"Terrorist associate" means an entity owned or controlled, directly or indirectly, by a Terrorist.

21. Notices of the names of persons designated as terrorists or terrorist associates are published in the Government Gazette, under section 4 of UNATMO, from time to time. The notices reflect designations made by the United Nations Committee pursuant to UNSC Resolution 1267. UNATMO provides that it should be presumed, in the absence of contrary evidence, that a person specified in such notices is a terrorist or a terrorist associate.

Knowledge vs. suspicion

22. There is a statutory obligation to report where there is knowledge or suspicion of ML/TF. Generally speaking, knowledge is likely to include:
    (a) actual knowledge;
    (b) knowledge of circumstances which would indicate facts to a reasonable person; and
    (c) knowledge of circumstances which would put a reasonable person on inquiry.

23. Suspicion, on the other hand, is more subjective. For example, according to the guidance issued by the Consultative Committee of Accountancy Bodies in the United Kingdom[47], in relation to the United Kingdom legislation, having knowledge means actually knowing that something is the case, whereas, suspicion, according to case law, is a state of mind more definite than speculation. While suspicion is personal and falls short of proof based on firm evidence[48], it must be based on some evidence, even if that evidence is tentative.[49]

24. In the case of Queensland Bacon PTY Ltd v Rees[50] [51], it was stated: "…A suspicion that

[47] The Consultative Committee of Accounting Bodies, 2008, *Anti-money laundering guidance for the accountancy sector*, (http://www.ccab.org.uk/PDFs/CCAB%20guidance%202008-8-26.pdf, para. 2.25).

[48] Ibid.

[49] Ibid., paragraph 2.26).

[50] [1966] 115 CLR 266 at 303, per Kitto J

[51] See footnote 45., paragraph 2.27.

something exists is more than a mere idle wondering whether it exists or not; it is a positive feeling of actual apprehension or mistrust, amounting to a slight opinion, but without sufficient evidence".

25. In the more recent case of Da Silva[52], the court stated: "It seems to us that the essential element in the word "suspect" and its affiliates, in this context, is that the defendant must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice."[53]

Investigations and access to information

26. OSCO, DTROP and UNATMO also contain provisions on investigations and access to information, which include protection for legal privilege.

AMLO

27. AMLO sets out CDD and RK requirements for FIs and the powers of relevant authorities to supervise compliance. It also covers regulation of money services and licensing of money service operators.

28. Part 2 and Schedule 2 cover the specifics of the CDD and RK requirements.

29. Section 7 of AMLO authorises a relevant authority (i.e., primarily the financial service regulators) or regulatory body, which includes the Institute in relation to members of the Institute and member practices, to publish any guideline that it considers appropriate to provide guidance on the operation of Schedule 2. Under section 7(4), a failure by a person to comply with a guideline in published under section 7 does not, by itself, render the person liable to judicial or other proceedings, but the guideline is admissible in evidence in court proceedings under AMLO, and if any provision of the guideline appears to the court to be relevant to any question arising in the proceedings, the provision must be taken into account in determining that question.

30. Under AMLO, FIs may rely on CDD conducted by certain types of intermediary, including certified public accountants practising in Hong Kong, subject to specific conditions. This may be relevant where, for example, an intermediary is introducing or acting on behalf of its client.

[52] Da Silva [2006] EWCA Crim 1654.

[53] Ibid.

APPENDIX B: Examples of possible risk factors when adopting a risk-based approach

Part I

Client risk

1. It is important to consider who clients are, what they do, and any other information that may suggest the client is of higher risk. Vigilance is required, for example, where the client has a legal form that enables individuals to divest themselves of ownership of property whilst retaining an element of control over it, or to retain anonymity, such as:
   (a) companies that can be incorporated without the identity of the ultimate underlying principals being disclosed;
   (b) certain forms of trusts or foundations, where knowledge of the identity of the true underlying principals or controllers cannot be guaranteed;
   (c) provision for nominee shareholders; and
   (d) companies issuing bearer shares.

2. Risks may be inherent in the nature of the activities of the client and the possibility that the activity, transaction and/or related transaction may itself be criminal, or where the business/industrial sector to which a client has business connections is more vulnerable to corruption For example, the arms trade and the financing of it is a type of activity that poses multiple ML/TF and other risks, e.g.:
   (a) corruption risks arising from procurement contracts;
   (b) risks in relation to PEPs; and
   (c) terrorism and TF risks as shipments may be diverted.

3. Some clients, by their nature or behaviour might present a higher risk of ML/TF. Factors might include:
   - the public profile of the clients indicating involvement with, or connection to, PEPs;
   - complexity of the relationship, including use of corporate structures, trusts and the use of nominee and bearer shares, where there is no clear legitimate commercial rationale;
   - a request to remain anonymous or use undue levels of secrecy with a transaction;
   - involvement in cash-intensive businesses;
   - nature, scope and location of business activities generating the funds/assets, having regard to sensitive or high-risk activities; and
   - where the origin of wealth (for high risk clients and PEPs) or ownership cannot be easily verified.

4. Other general factors that may indicate a higher than normal ML/TF risk in relation to clients include:

   i) Reduced transparency

   - lack of face-to-face introduction of client;
   - subsequent lack of contact, when this would normally be expected;
   - beneficial ownership is unclear;
   - position of intermediaries is unclear;
   - inexplicable changes in ownership;
   - company activities are unclear;
   - legal structure of client has been altered numerous times (name changes, transfer of ownership, change of corporate seat);

- management appear to be acting according to instructions of unknown or inappropriate person(s);
- unnecessarily complex client structure;
- reason for client choosing the firm is unclear, given the firm's size, location or specialism;
- frequent or unexplained change of professional adviser(s) or members of management;
- the client is reluctant to provide all the relevant information or the practice has reasonable doubt that the provided information is incorrect or insufficient.

ii) Transactions or structures out of line with business profile

- client instructions or funds outside of their personal or business sector profile;
- individual or classes of transactions that take place outside the established business profile, and expected activities/ transaction unclear;
- employee numbers or structure out of keeping with size or nature of the business (for instance the turnover of a company is unreasonably high considering the number of employees and assets used);
- sudden activity from a previously dormant client;
- client starts or develops an enterprise with unexpected profile or early results;
- indicators that client does not wish to obtain necessary governmental approvals/filings, etc.;
- clients who offer to pay extraordinary fees for services which would not ordinarily warrant such a premium; and
- payments received from unassociated or unknown third parties and payments for fees in cash where this would not be a typical method of payment.

iii) Higher risk sectors and operational structures

- entities with a high level of transactions in cash or readily transferable assets, among which illegitimate funds could be obscured;
- frequent involvement with PEPs;
- investment in real estate at a higher/lower price than expected;
- large international payments with no business rationale;
- unusual financial transactions with unknown source;
- clients with multijurisdictional operations that do not have adequate centralised corporate oversight; and
- clients incorporated in jurisdictions that permit bearer shares.

iv) The existence of fraudulent transactions, or ones which are improperly accounted for, should always be considered suspicious.

These might include:
- over and under invoicing of goods/services;
- multiple invoicing of the same goods/services;
- falsely described goods/services – over and under shipments (e.g., false entries on bills of lading); and
- multiple trading of goods/services.

Service risk

5. The characteristics of the services being offered, or intended to be offered, and the extent to which these may be vulnerable to ML/TF abuse, should also be considered. In this connection, it

is important to assess the risks of any new services before they are introduced and, where necessary, ensure appropriate additional measures and controls are implemented to mitigate and manage the associated ML/TF risks.

6. Factors presenting higher risk may include services that inherently provide more anonymity. Other services that may be provided by accountants and which (in some circumstances) risk being used to assist money launderers may include:

- misuse of pooled client accounts or safe custody of client money or assets;
- advice on the setting up of legal arrangements, which may be used to obscure ownership or real economic purpose (including setting up of trusts, companies or change of name/corporate seat or other complex group structures);
- misuse of introductory services, e.g. to financial institution.

Country risk[54]

7. Clients with residence in or connection with high-risk jurisdictions; for example countries:

- identified by the FATF or other credible sources as jurisdictions with strategic AML/CFT deficiencies[55];
- subject to sanctions, embargos or similar measures issued by the UN;
- identified by credible sources as having significant levels of corruption, or other criminal activity
- identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within them.

8. For this purpose, practices may make reference to publicly available information or relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations (e.g., Transparency International's "Corruption Perceptions Index", which ranks countries according to their perceived level of corruption).

Delivery channel risk

9. Consider their service delivery channels and the extent to which these may be vulnerable to ML/TF abuse. These may include, for example, delivery where a non-face-to-face approach is used. Services engaged through intermediaries may also increase risk, as the business relationship between the client and a practice may become indirect.

Part II

Variables that may impact on risk

1. Indicated below are some factors that may increase or decrease risk in relation to particular clients, client engagements or practising environments.

[54] In assessing country risk associated with a client, consideration may be given to local legislation (United Nations Sanctions Ordinance (UNSO), UNATMO), data available from the United Nations, the International Monetary Fund, the World Bank, the FATF, etc. and the practice's own experience or the experience of other group entities (where the practices is part of an international network which may have indicated weaknesses in other jurisdictions.

[55] See paragraphs 3.13.31-3.13.35.

- Involvement of financial institutions or other DNFBPs;
- sophistication of client, including complexity of control environment;
- sophistication of transaction/scheme;.
- role or oversight of another regulator;
- the regularity or duration of the relationship. Long-standing relationships involving frequent client contact throughout the relationship may present less risk;
- clients who are employment-based or with a regular source of income from a known legitimate source, which supports the activity being undertaken;
- clients who have a reputation for probity in the local communities;
- clients with a sound reputation, e.g., well-known, reputable private companies, with a long history that is well documented by independent sources, including information regarding their ownership and control;
- clarity in terms of the purpose of the relationship and the need for the practice to provide services;
- familiarity with a country, including knowledge of local laws and regulations as well as the structure and extent of regulatory oversight;
- country location of the client; and
- unexplained urgency of assistance required.

APPENDIX C: Examples of sources and content of information for client identification and verification purposes

Part I

Reliable and independent sources for client identification purposes

1. The identity of an individual physically present in Hong Kong may be verified by reference to their Hong Kong identity card or travel document. Hong Kong residents' identity may be identified and/or verified by reference to their Hong Kong identity card, certificate of identity or document of identity. The identity of non-residents can be verified by reference to their valid travel document.

2. For non-resident individuals who are not physically present in Hong Kong, their identity may be identified and/or verified by reference to the following documents:
   (a) a valid international passport or other travel document; or
   (b) a current national (i.e., government or state-issued) identity card bearing the photograph of the individual; or
   (c) current valid national (i.e., government or state-issued) driving licence[56] incorporating photographic evidence of the identity of the applicant, issued by a competent national or state authority.

3. "Travel document" means a passport or some other document furnished with a photograph of the holder establishing the identity and nationality, domicile or place of permanent residence of the holder; for example:
   (a) Permanent Resident Identity Card of Macau Special Administrative Region;
   (b) Mainland Travel Permit for Taiwan Residents;
   (c) Seaman's Identity Document (issued under and in accordance with the International Labour Organisation Convention/Seafarers Identity Document Convention 1958);
   (d) Taiwan Travel Permit for Mainland Residents;
   (e) Permit for residents of Macau issued by Director of Immigration;
   (f) Exit-entry Permit for Travelling to and from Hong Kong and Macau for Official Purposes; and
   (g) Exit-entry Permit for Travelling to and from Hong Kong and Macau.

4. A corporate client may be identified and/or verified by performing a company registry search in the place of incorporation and obtaining a full company search report.

5. For jurisdictions that do not have national ID cards and where clients do not have a travel document or driving licence with a photograph, applying an RBA, other documents may be accepted as evidence of identity. Wherever possible such documents should have a photograph of the individual.

Part II

Appropriate identification and verification information

A. Natural persons

Identification

1. Generally, the following identification information should be collected in respect of personal clients who need to be identified:

[56] International drivers' permits and licences are not acceptable for this purpose.

(a) full name;
(b) date of birth;
(c) nationality; and
(d) identity document type and number.

Verification (Hong Kong residents)

2. For Hong Kong permanent residents, an individual's name, date of birth and identity card number may be verified by reference to his/her Hong Kong identity card. A copy of the individual's identity card should be retained.

3. For minors born in Hong Kong who are not in possession of a valid travel document or Hong Kong identity card[57], their identity may be verified by reference to their Hong Kong birth certificate. Whenever establishing relations with a minor, the identity of the minor's parent or guardian representing or accompanying the minor should also be recorded and verified in accordance with the above requirements.

4. For non-permanent residents, an individual's name, date of birth, nationality and travel document number and type may be verified by reference to a valid travel document (e.g., an unexpired international passport). A copy of the "biodata" page, which contains the bearer's photograph and biographical details, should be retained.

5. Alternatively, an individual's name, date of birth, identity card number may be verified by reference to their Hong Kong identity card, and the individual's nationality by reference to:
   (a) a valid travel document;
   (b) a relevant national (i.e. government or state-issued) identity card bearing the individual's photograph; or
   (c) any government or state-issued document which certifies nationality.

   A copy of the any relevant documents should be retained.

Verification (non-residents)

6. For non-residents who are physically present in Hong Kong for verification purposes, an individual's name, date of birth, nationality and travel document number and type may be verified by reference to a valid travel document (e.g., an unexpired international passport). A copy of the "biodata" page which contains the bearer's photograph and biographical details should be retained.

7. For non-residents who are not physically present in Hong Kong for verification purposes, the individual's identity, including name, date of birth, nationality, identity or travel document number and type may be verified by reference to:
   (a) a valid travel document;
   (b) a relevant national (i.e. government or state-issued) identity card bearing the individual's photograph;
   (c) a valid national driving licence bearing the individual's photograph; or
   (d) other suitable alternatives, such as those mentioned in Part I.

[57] All residents of Hong Kong who are aged 11 and above are required to register for an identity card. Hong Kong permanent residents will have a Hong Kong Permanent Identity Card. The identity card of a permanent resident (i.e. a Hong Kong Permanent Identity Card) will have on the front of the card a capital letter "A" underneath the individual's date of birth.

8. Where a client has not been physically present for identification purposes, additional measures, such as those indicated in paragraphs 3.13.2 – 3.13.3 of these Guidelines, may need to be carried out.

Address identification and verification

9. It is suggested that the residential address (and permanent address if different) of a direct client with whom a business relationship is being established be obtained and verified, as this is useful for verifying an individual's identity and background.

10. It is the trustee of a trust who enters into a business relationship or carries out a transaction on behalf of the trust who will be considered to be the client. The address of the trustee in a direct client relationship should therefore be verified. Methods for verifying residential addresses may include obtaining:
    (a) a recent utility bill issued within the last 3 months;
    (b) recent correspondence from a government department or agency (i.e. issued within the last 3 months);
    (c) a statement, issued by an authorised institution, a licensed corporation or an authorised insurer within the last 3 months;
    (d) an acknowledgement of receipt duly signed by the client in response to a letter sent by the practice to the address provided by the client;
    (e) mobile phone or pay TV statement (sent to the address provided by the client) issued within the last 3 months;
    (f) a Hong Kong tenancy agreement which has been duly stamped by the Inland Revenue Department;
    (g) a current Hong Kong domestic helper employment contract stamped by an appropriate consulate (the name of the employer should correspond with the applicant's visa endorsement in their passport);
    (h) a letter from a Hong Kong employer together with proof of employment, which the practice is satisfied that it can place reliance on and that confirms residence at a stated address in Hong Kong;
    (i) a lawyer's confirmation of property purchase, or legal document recognising title to property; and
    (j) for non-Hong Kong residents, a government-issued photograph driving licence or national identity card containing the current residential address or bank statements issued by a bank in an equivalent jurisdiction, where the practice is satisfied that the address has been verified.

11. Some clients may be unable to produce evidence of address to the standard outlined above. In such circumstances, on a risk sensitive basis, a common sense approach may be adopted by using alternative methods such as obtaining a letter from a director or manager of a verified known overseas employer that confirms residence at a stated overseas address (or provides detailed directions to locate a place of residence).

12. There may also be circumstances where a client's address is a temporary accommodation and where normal address verification documents are not available. For example, an expatriate on a short-term contract. Flexible procedures many be adopted to obtain verification by other means, e.g., copy of contract of employment, or bank's or employer's written confirmation. However, a post office box address is not sufficient for persons residing in Hong Kong or corporate clients registered and/or operating in Hong Kong.

Other considerations

13. The standard identification requirement is likely to be sufficient for most situations. If, however, the

client, or the service, is assessed to present a higher ML/TF risk because of the nature of the client, his/her business, his/her location, or because of the product features, etc., it should be considered whether additional identity information may need to be provided, and/or whether to verify additional aspects of identity.

B. Legal persons and trusts

General

1. For legal persons, the principal requirement is to look behind the immediate client to identify those who have ultimate control or ultimate beneficial ownership over the business and the client's assets. Normally particular attention should be paid to persons who exercise ultimate control over the management of the client.

2. It is suggested that the residential address (and permanent address if different) of beneficial owners be obtained and an RBA may be adopted to determine the need to take reasonable measures to verify the address, taking account of the number of beneficial owners, the nature and distribution of the interests in the entity and the nature and extent of any business, contractual or family relationship.

3. Where the owner is another legal person or trust, the objective is to undertake reasonable measures to look behind that legal person or trust and to verify the identity of beneficial owners. What constitutes control for this purpose will depend on the nature of the institution, and may vest in those who are mandated to manage funds, accounts or investments without requiring further authorisation.

4. For a client other than a natural person, it needs to be ensured that the client's legal form, structure and ownership are fully understood and, additionally, information should be obtained on the nature of its business and the reasons for seeking the service unless the reasons are obvious.

5. Reviews should be conducted from time to time to ensure the client information held is up to date and relevant; methods by which a review could be conducted include conducting company searches, seeking copies of resolutions appointing directors, noting the resignation of directors, or by other appropriate means.

6. Many entities operate internet websites, which contain information about the entity. It should be borne in mind that this information, although helpful in providing much of the materials that might be needed in relation to the client, its management and business, may not be independently verified.

Corporations

Identification information

7. Generally, the information below should be obtained as the standard requirement; thereafter, on the basis of the ML/TF risk, it can be decided whether further verification of identity is required and if so the extent of that further verification. It should also be decided whether additional information in respect of the corporation, its operation and the individuals behind it should be obtained:
   (a) full name;
   (b) date and place of incorporation;
   (c) registration or incorporation number; and
   (d) registered office address in the place of incorporation.

   If the business address of the client is different from the registered office address in (d) above, information on the business address should be obtained and verified as far as practicable.

8. In the course of verifying the client's information mentioned in paragraph 7, the following information should also be obtained:
   (a) a copy of the certificate of incorporation and business registration (where applicable);
   (b) a copy of the company's memorandum and articles of association which evidence the powers that regulate and bind the company; and
   (c) details of the ownership and structure control of the company (e.g., an ownership chart).

9. The names of all directors[58] should be recorded and their identities be verified using an RBA.

10. As far as possible, the following should be done:
   (a) confirm the company is still registered and has not been dissolved, wound up, suspended or struck off;
   (b) independently identify and verify the names of the directors and shareholders recorded in the company registry in the place of incorporation; and
   (c) verify the company's registered office address in the place of incorporation.

11. The information in paragraph 10 above may be verified from:

   For a locally-incorporated company -
   (a) conducting a file search at the Hong Kong Companies Registry and obtaining a company report[59];

   For a company incorporated overseas -
   (a) conducting a similar company search enquiry of the registry in the place of incorporation and obtaining a company report;
   (b) obtaining a certificate of incumbency[60] or equivalent issued by the company's registered agent in the place of incorporation; or
   (c) obtaining a similar or comparable document to a company search report or a certificate of incumbency certified by a professional third party in the relevant jurisdiction, verifying that the information at paragraph 10, contained in the said document, is correct and accurate.

12. If, following paragraph 11, a company search report has been obtained, which contains information such as certificate of incorporation, company's memorandum and articles of association, etc, the same information need not be obtained again from the client pursuant to paragraph 8.

C. Beneficial owners

Corporations

1. In relation to beneficial owners of corporations, in normal, non-high risk, situations, the AMLO

[58] It may, of course, already be required to identify a particular director if the director acts as a beneficial owner or a person purporting to act on behalf of the customer (e.g., account signatories).(see subsection 3.6 and 3.7).

[59] Alternatively, a certified true copy of a company search report, certified by a company registry or professional third party may be obtained from the client. The company search report should have been issued within the last 6 months. It is not sufficient for the report to be self-certified by the client.

[60] A certified true copy of a certificate of incumbency certified by a professional third party may be accepted. The certificate of incumbency should have been issued within the last 6 months. It is not sufficient for the certificate to be self-certified by the client.

requires relevant DNFBPs to verify the identity of a beneficial owner where that person is:

(a) an individual who –
    (i) owns or controls, directly or indirectly, including through a trust or bearer shareholding, more than 25% of the issued share capital of the corporation;
    (ii) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights at general meetings of the corporation; or
    (iii) exercises ultimate control over the management of the corporation; or
(b) if the corporation is acting on behalf of another person, means that other person.

2. The identity of beneficial owners should be identified and recorded, and reasonable measures taken to verify the identity of:
    (a) all shareholders holding more than 25% of the voting rights or share capital,;
    (b) any individual who exercises ultimate control over the management of the corporation; and
    (c) any person on whose behalf the client is acting.

3. For companies with multiple layers in their ownership structures, an understanding should be obtained of the ownership and control structure of the company. The intermediate layers of the company should be identified. The manner in which this information is collected should be determined, for example by obtaining a director's declaration incorporating or annexing an ownership chart describing the intermediate layers (the information to be included should be determined on a risk sensitive basis but, at a minimum, should include company name and place of incorporation, and where applicable, the rationale behind the particular structure employed). The objective should always be to follow the chain of ownership to the individuals who are the ultimate beneficial owners of the direct client of a practice and to verify the identity of those individuals.

4. It is should not be necessary, as a matter of routine, to verify the details of the intermediate companies in the ownership structure of a company. Complex ownership structures (e.g., structures involving multiple layers, different jurisdictions, trusts, etc.) without an obvious commercial purpose pose an increased risk and may require further steps to ensure that practices are satisfied on reasonable grounds as to the identity of the beneficial owners.

5. The need to verify the intermediate corporate layers of the ownership structure of a company will therefore depend upon the overall understanding of the structure, the assessment of the risks and whether the information available is sufficient in the circumstances to consider whether adequate measures have been taken to identify the beneficial owners.

6. Where the ownership is dispersed, practices may concentrate on identifying and taking reasonable measures to verify the identity of those who exercise ultimate control over the management of the company.

<u>Partnerships and unincorporated bodies</u>

7. Partnerships and unincorporated bodies, although principally operated by individuals or groups of individuals, are different from individuals, in that there is an underlying business. This business is likely to have a different ML/TF risk profile from that of an individual.

8. In relation to beneficial owners of partnerships, in normal, non-high risk, situations, the AMLO requires DNFBPs to verify the identity of a beneficial owner, where that person is:
    (a) an individual who
        (i) is entitled to or controls, directly or indirectly, more than a 25% share of the capital or profits of the partnership;
        (ii) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights in the partnership; or

(iii) exercises ultimate control over the management of the partnership; or

(b) if the partnership is acting on behalf of another person, means the other person.

9. In relation to an unincorporated body other than a partnership, beneficial owner:
   (a) means an individual who ultimately owns or controls the unincorporated body; or
   (b) if the unincorporated body is acting on behalf of another person, means the other person.

10. Generally, the following information in relation to the partnership or unincorporated body should be obtained:
   (a) the full name;
   (b) the business address; and
   (c) the names of all partners and individuals who exercise control over the management of the partnership or unincorporated body, and names of individuals who own or control more than 25% of its capital or profits, or of its voting rights.

11. In cases where a partnership arrangement exists, a mandate from the partnership authorising the business activity and conferring authority on those who will undertake it should usually be obtained.

12. The identity of the client should be verified using evidence from a reliable and independent source. Where partnerships or unincorporated bodies are well-known, reputable organisations, with long histories in their industries, and with substantial public information about them, their partners and controllers, confirmation of the client's membership of a relevant professional or trade association is likely to be sufficient to provide such reliable and independent evidence of the identity of the client. Reasonable measures will generally still need to be taken to verify the identity of the beneficial owners of the partnerships or unincorporated bodies.

13. Other partnerships and unincorporated bodies have a lower profile, and generally comprise a much smaller number of partners and controllers. In verifying the identity of such clients, practices may have regard to the number of partners and controllers. Where these are relatively few, the client may be treated as a collection of individuals; where numbers are larger, practices may decide whether they should continue to regard the client as a collection of individuals, or whether they can be satisfied with evidence of membership of a relevant professional or trade association. In either case, practices should obtain the partnership deed (or other evidence in the case of sole traders or other unincorporated bodies), to satisfy themselves that the entity exists, unless an entry in an appropriate national register may be checked.

14. In the case of associations, clubs, societies, charities, religious bodies, institutes, mutual and friendly societies, co-operative and provident societies, satisfaction should be obtained as to the legitimate purpose of the organisation, e.g., by requesting sight of the constitution.

Trusts

General

15. A trust does not possess a separate legal personality. It cannot form business relationships or carry out one-off or ad hoc transactions itself. It is the trustee who enters into a business relationship or carries out transactions on behalf of the trust and who is considered to be the client (i.e. the trustee is acting on behalf of a third party – the trust and the individuals concerned with the trust).

16. In relation to beneficial owners of trusts, in normal, non-high risk, situations, the AMLO requires DNFBPs to verify the identity of a beneficial owner, where that person is:
   (a) an individual who is entitled to a vested interest in not less than 25% of the capital of the trust property, whether the interest is in possession or in remainder or reversion and whether it is

defeasible or not;
(b) the settlor of the trust;
(c) a protector or enforcer of the trust; or
(d) an individual who has ultimate control over the trust.

17. It is suggested that the following identification information in respect of a trust on whose behalf the trustee (i.e., the client) is acting be obtained:
    (a) the name of the trust;
    (b) date of establishment/settlement;
    (c) the jurisdiction whose laws govern the arrangement, as set out in the trust instrument;
    (d) the identification number (if any) granted by any applicable official bodies (e.g. tax identification number or registered charity or non-profit organisation number);
    (e) identification information of trustee(s), in line with guidance for individuals or corporations;
    (f) identification information of settlor(s) and any protector(s) or enforcers, in line with the guidance for individuals/corporations; and
    (g) identification information of known beneficiaries. Known beneficiaries mean those persons or that class of persons who can, from the terms of the trust instrument, be identified as having a reasonable expectation of benefiting from the trust capital or income.

Verifying the trust

18. Generally, the name and date of establishment of a trust should be verified and it is suggested that appropriate evidence to verify the existence, legal form and parties to it, i.e., trustee, settlor, protector, beneficiary, etc. should be obtained. The beneficiaries should be identified as far as possible, where defined. If the beneficiaries are yet to be determined, practices should concentrate on the identification of the settlor and/or the class of persons in whose interest the trust is set up. The most direct method of satisfying this requirement is to review the appropriate parts of the trust deed.

19. Reasonable measures to verify the existence, legal form and parties to a trust, having regard to the ML/TF risk, may include:
    (a) reviewing a copy of the trust instrument and retaining a redacted copy;
    (b) by reference to an appropriate register[61] in the relevant country of establishment;
    (c) a written confirmation from a trustee acting in a professional capacity[62];
    (d) a written confirmation from a lawyer who has reviewed the relevant instrument; or

    Reasonable measures still need to be taken to verify the actual identity of the individual parties (i.e., trustee, settlor, protector, beneficiary, etc.).

20. Where only a class of beneficiaries is available for identification, practices should endeavour to ascertain and name the scope of the class (e.g., children of a named individual).

21. Particular care should be taken in relation to trusts created in jurisdictions where there is no AML/CFT framework similar to Hong Kong's.

[61] In determining whether a register is appropriate, regard should be had to adequate transparency (e.g., a system of central registration where a national registry records details on trusts and other legal arrangements registered in that country). Changes in ownership and control information would need to be kept up-to-date.

[62] "Trustees acting in their professional capacity" in this context means that they act in the course of a profession or business which consists of or includes the provision of services in connection with the administration or management of trusts (or a particular aspect of the administration or management of trusts).

APPENDIX D: Suspicious transaction indicators and examples of situations that could give rise to suspicions

General indicators

1. The types of transactions that may be used for ML/TF are wide-ranging and so it is not possible to specify all the transactions that might arouse suspicion.

2. Practices should consider indicators of suspicious transactions, such as the nature and parties involved, including the involvement of jurisdictions that insufficiently apply FATF Rs and persons designated as terrorists published in the Government Gazette.

3. Particular care should be taken when, for example, companies have very complex ownership structures that do not seem to serve any legitimate purpose, or when a company is incorporated or administered in a jurisdiction designated by FATF among the Non-Cooperative Countries and Territories. More information on these countries/ territories can be found on the FATF website.

4. The JFIU state that common indicators of suspicious activities associated with ML/TF in Hong Kong include:[63]
   (a) large or frequent cash transactions, either deposits or withdrawals;
   (b) suspicious activity based on transaction patterns, e.g.,
      (i) accounts used as a temporary repository for funds;
      (ii) a period of significantly increased activity amid relatively dormant periods;
      (iii) "Structuring" or "smurfing" i.e., many lower-value transactions conducted when one, or a few, large transactions could be used. This is common in incoming remittances from countries with value-based transaction reporting requirements, e.g., frequent remittances just below AU$10,000 from Australia or US$10,000 from United States;
      (iv) "U-turn" transactions, i.e., where money passes from one person or company to another and then back to the original person or company; and
      (v) increased level of account activity on the first banking day after Hong Kong horse racing, normally Mondays and Thursdays, which may indicate illegal bookmaking.
   (c) involvement of one or more of the following entities, which are common in money laundering,
      (i) shelf or shell companies;
      (ii) companies registered in a known "tax haven" or "off-shore financial centre";
      (iii) company formation agent, or secretarial company, as the authorised signatory of the bank account;
      (iv) remittance agents or money changers; and
      (v) casinos.
   (d) currencies, countries or nationals of countries, commonly associated with international crime, or drug trafficking, or identified as having serious deficiencies in their AML/CFT regimes;
   (e) clients who refuse, or are unwilling, to provide explanations of financial activities, or provide explanations assessed to be untrue;
   (f) activity that is unexpected of clients, considering existing knowledge about the clients and their previous financial activity. For personal accounts, relevant considerations include clients' age, occupation, residential address, general appearance, type and level of previous financial activity. For company accounts, relevant considerations include the type and level of activity;

---

[63] http://www.jfiu.gov.hk/en/str.html

(g) countries, or nationals of countries, commonly associated with terrorist activities or the persons or organisations designated as terrorists or their associates; and
(h) international and domestic PEPs; that is, individuals who hold important positions in governments or the public sector, who may be more vulnerable to corruption and involvement in abuse of public funds.

Situations that may give rise to suspicions

5. Examples of situations that could give rise to suspicion, depending on the circumstances, include the following:
   (a) activities, service requests or transactions that have no apparent legitimate purpose and/or appear not to have a commercial rationale;
   (b) activities, service requests or transactions that involve apparently unnecessary complexity or which do not constitute the most logical, convenient or secure way to do business;
   (c) where the service or transaction being requested by the client, without reasonable explanation, is out of the ordinary range of services normally requested;
   (d) where, without reasonable explanation, the size or pattern of activities or transactions is out of line with any pattern that has previously emerged;
   (e) where the client refuses to provide the information requested without reasonable explanation or otherwise refuses to cooperate with the CDD and/or the ongoing monitoring process;
   (f) where a client that has entered into a business relationship uses the relationship for a single service or for only a very short period without a reasonable explanation;
   (g) the extensive use of trusts or offshore structures in circumstances where the client's needs are inconsistent with the use of such services;
   (h) activities or transactions involving high-risk jurisdictions without reasonable explanation, which are not consistent with the client's declared business dealings or interests; and
   (i) unnecessary routing of funds or other property from/to third parties or through third party accounts.

6. Reference can also be made to:
   (a) Suspicious transaction indicators for accountants in the publication, *Anti-Money Laundering & Counter Terrorist Financing*, published by the Narcotics Divisions, Security Bureau, June 2009 (paragraph 4.5).
   (b) Characteristics of financial transactions that may be a cause for increased scrutiny contained in Annex 1 of FATF's *Guidance for Financial Institutions in Detecting Terrorist Financing*.
   (c) Relevant overseas examples, such as the general and accountancy-specific suspicious transaction indicators in *Guideline 2: Suspicious Transactions*, issued by the Financial Transactions and Reports Analysis Centre of Canada.

APPENDIX E: <u>Glossary of key terms and abbreviations, and definitions</u>

Terms / abbreviations	Meaning
AMLO	Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap. 615)
AML/CFT	Anti-money laundering and counter financing of terrorism
Beneficial owner	(a) In relation to a corporation— (i) means an individual who— A. owns or controls, directly or indirectly, including through a trust or bearer share holding, more than 25% of the issued share capital of the corporation; B. is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights at general meetings of the corporation; or C. exercises ultimate control over the management of the corporation; or (ii) if the corporation is acting on behalf of another person, means the other person; (b) in relation to a partnership— (i) means an individual who— A. is entitled to or controls, directly or indirectly, more than a 25% share of the capital or profits of the partnership; B. is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights in the partnership; or C. exercises ultimate control over the management of the partnership; or (ii) if the partnership is acting on behalf of another person, means the other person; (c) in relation to a trust, means— (i) an individual who is entitled to a vested interest in more than 25% of the capital of the trust property, whether the interest is in possession or in remainder or reversion and whether it is defeasible or not; (ii) the settlor of the trust; (iii) a protector or enforcer of the trust; or (iv) an individual who has ultimate control over the trust; and

	(d) in relation to a person not falling within paragraph (a), (b) or (c)— (i) means an individual who ultimately owns or controls the person; or (ii) if the person is acting on behalf of another person, means the other person;
Business relationship	A business relationship between a person and a practice is a business, professional or commercial relationship: (i) that has an element of duration; or (ii) that the practice, at the time the person first contacts it in the person's capacity as a potential client of the practice, expects to have an element of duration. ***This can be distinguished from an occasional or ad hoc assignment or transaction, which is an assignment or transaction by a practice for a client with which the practice does not have a business relationship.***
CDD	Client due diligence
CO	Compliance officer
Connected parties	Connected parties to a client include the beneficial owner and any natural person having the power to direct the activities of the client. For the avoidance of doubt, the term connected party will include any director, shareholder, beneficial owner, signatory, trustee, settlor/grantor/founder, protector(s), or defined beneficiary of a legal arrangement.

DNFBP (under AMLO)	Designated non-financial businesses and professions means: (a) an accounting professional; (b) an estate agent; (c) a legal professional; or (d) a TCSP licensee; "*accounting professional*" means— (a) a certified public accountant or a certified public accountant (practising), as defined by section 2(1) of the Professional Accountants Ordinance (Cap. 50); (b) a corporate practice as defined by section 2(1) of the Professional Accountants Ordinance (Cap. 50); or (c) a firm of certified public accountants (practising) registered under Part IV of the Professional Accountants Ordinance (Cap. 50); "*TCSP licensee*" is a person licensed under AMLO to carry on a trust or company service business, i.e., those services referred to in paragraph 1.1.2 of these Guidelines.
DTROP	Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405)
EDD	Enhanced client due diligence
FATF	Financial Action Task Force
FI	Financial institution
ICO	Insurance Companies Ordinance (Cap. 41)
Individual	Individual means a natural person, other than a deceased natural person.
JFIU	Joint Financial Intelligence Unit
Minor	Minor means a person who has not attained the age of 18 years [Interpretation and General Clauses Ordinance (Cap. 1) - section 3].
MLRO	Money laundering reporting officer
Money laundering	Has the meaning given in Section 1.3 of these Guidelines
ML/TF	Money laundering and/or terrorist financing
Occasional transaction	A transaction between a DNFBP and a client who does not have a business relationship with the DNFBP

OSCO	Organised and Serious Crimes Ordinance (Cap. 455)
PEP(s)	Politically exposed person(s)
RA(s)	Relevant authority (authorities)
RBA	Risk-based approach to CDD and ongoing monitoring
RK	Record-keeping
Schedule 2	Schedule 2 to the AMLO
SDD	Simplified client due diligence
Senior management	Senior management means directors (or board) and senior managers (or equivalent) of a firm who are responsible, either individually or collectively, for management and supervision of the firm's business. This may include a firm's chief executive officer, managing director, or other senior operating management personnel (as the case may be).
SFO	Securities and Futures Ordinance (Cap. 571)
STR	Suspicious transaction report; also referred to as "report" or "disclosure"
Terrorist financing	Has the meaning given in Section 1.3 of these Guidelines
Trust	For the purposes of the guideline, a trust means an express trust or any similar arrangement for which a legal-binding document (i.e. a trust deed or in any other form) is in place.
UNATMO	United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575)
UNSO	United Nations Sanctions Ordinance (Cap. 537)