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

# MEMBERS' HANDBOOK

## Update No. 216

*(Issued 28 February 2018)*

| ***Document Reference and Title*** | ***Instructions*** | ***Explanations*** |
|---|---|---|
| **VOLUME I** | | |
| Contents of Volume I | Discard existing page i & replace with revised page i. | Revised contents pages |
| **PROFESSIONAL ETHICS** | | |
| Code of Ethics for Professional Accountants (Revised) [Part F – Guidelines on Anti-Money Laundering and Counter-Terrorist Financing for Professional Accountants] | Replace page 4 and pages 205-220 with revised page 4 and revised page 205-220. Insert pages 221-284 after page 220. | - Notes |

**Notes:**

1. Following the passage of the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Amendment Ordinance 2018, "accounting professionals", under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615)("AMLO"), i.e., practice units and members of the Institute, as defined in the Professional Accountants Ordinance (Cap. 50), are required to comply with certain customer due diligence ("CDD") and record-keeping requirements, commencing 1 March 2018. Other existing legislation also prescribes requirements to report suspicious transactions and creates certain money laundering and terrorist financing-related offences. The aforementioned legislative provisions aim to implement core anti-money laundering and counter terrorist financing ("AML/CFT") standards issued by the Financial Action Task Force ("FATF"). The FATF is the international, inter-governmental body responsible for the development and promotion of AML/CFT policies and practices. The FATF has published a set of AML/CFT measures, known as the Recommendations. The Recommendations are the source of much of the AML/CFT legislation and regulation around the world.

2. As a member of FATF, Hong Kong is required to implement a credible AML/CFT regime having regard to the Recommendations, significant parts of which apply to "designated non-financial businesses and professions ('DNFBPs')", including accountants, as well as to financial institutions. Under AMLO, accounting professionals are required to comply with the CDD and record keeping requirements when they provide specified services, that is:

When, by way of business, they prepare for or carry out for clients transactions concerning one of more of the following:

- buying or selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organization of contribution for the creation, operation or management of corporations;
- creation, operation or management of legal persons or arrangements;
- buying or selling of business entities;
- specified services for trust or company service providers ("TCSPs").

For TCSPs, when, by way of business, they prepare for or carry out for clients transactions:

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

3. Under section 7 of AMLO, the Institute, as the regulatory body for the profession, is empowered to issue guidelines to provide guidance in relation the operation of relevant provisions of AMLO. Guidelines on AML/CFT issued by the Institute, pursuant to section 7 of AMLO, are attached. Their legal standing is indicated in section 7 of AMLO and also in the guidelines themselves. The guidelines were published in the Government Gazette on 23 February 2018 and are effective as from 1 March 2018.

4. Practice units and members are expected to comply with the provisions of the guidelines, as specified in the guidelines themselves.

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

# MEMBERS' HANDBOOK
# CONTENTS OF VOLUME I

(Updated to February 2018)

# PART F – GUIDELINES ON ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING FOR PROFESSIONAL ACCOUNTANTS

## Preamble

The Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) (Amendment) Ordinance 2018, effective on 1 March 2018, extends the scope of the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap. 615)("AMLO") to cover "designated non-financial businesses and professions" ("DNFBPs"), including accountants. It implements the FATFRs as these relate to customer due diligence ("CDD") and record keeping ("RK") for DNFBPs. These Guidelines are based on AMLO as amended, now entitled the Anti-Money Laundering and Counter-Terrorist Financing Ordinance, and subsequent references to "AMLO" relate to the amended ordinance. These Guidelines are effective as from 1 March 2018.

## SECTION 600

## Overview and Application

### 600.1 Introduction and purpose of Guidelines

600.1.1 These Guidelines are published under section 7 of AMLO. They apply primarily to practices and members working in practices. Reference to "practices" in the Guidelines includes practice units under the Professional Accountants Ordinance (Cap. 50) and also trust or company service providers, where the proprietors, partners or directors are all 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].

600.1.2 In addition to AMLO, and in particular Schedule 2 of AMLO, these Guidelines also make reference to other existing legislation containing requirements relating to 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 relevant sections of the other ordinances together seek to give effect to the FATFRs. As a member of FATF, Hong Kong is required to implement a credible AML/CFT regime having regard to the FATFRs, substantial parts of which apply to DNFBPs as well as to financial institutions ("FIs").

600.1.3 It is recognised that, in contrast to certain FIs, practices are not licensed to hold client monies or process cash transactions, so generally money laundering/ terrorist financing ("ML/TF") risks may be lower for practices than for FIs.

600.1.4 At the same time, 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. Practices will therefore be expected by the community 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.

1 Members working in the financial services or other sectors specified in AMLO are advised to familiarise themselves with any guidelines issued by the appropriate relevant authority or regulatory body under AMLO to facilitate compliance with the requirements of the ordinance.

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

- Provide general guidance on AML/CFT requirements under AMLO and other relevant legislation.
- Indicate good practice on applying other relevant FATFRs.
- Summarise relevant legislative provisions on AML/CFT.
- Ensure compliance by members with prescribed requirements to prevent ML/TF activities.

600.1.6 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.

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

600.1.8 More generally, 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. 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 familiarise themselves with these Guidelines and to take on board the relevant FATFRs within their risk management programmes, including those FATFRs already implemented in legislation other than AMLO, such as the requirement to report suspicious transactions under DTROP and OSCO.

600.1.9 Use of the word "must" in these Guidelines indicates a mandatory requirement, which may be a statutory obligation, or requirement that directly flows from this, or is seen by the Institute as being necessary to implement the statutory obligation effectively. In contrast, use of the words “should”, "would" and "may" in these Guidelines is not intended to indicate a mandatory requirement, but to provide guidance on possible means of compliance with statutory and regulatory requirements, and/or suggest good practice regarding compliance with the FAFTRs. Practices should consider their own particular circumstances when determining how to apply the detailed provisions of these Guidelines, and take into account the relevant legislation and mandatory requirements.

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

## 600.2 Application of the Guidelines

| The Guidelines apply to practices (see paragraph 600.1.1) as follows: | AML/CTF policies, procedures and controls (section 610) | CDD, RK and ongoing monitoring (sections 620,630,660) | Suspicious transaction reporting and financial sanctions (sections 640,650) | Staff hiring and training (section 670) |
|---|---|---|---|---|
| When providing any service specified in paragraphs 600.2.1 or 600.2.2 | **Mandatory** | **Mandatory** | **Mandatory** | **Mandatory** |
| When providing services other than those specified in paragraphs 600.2.1 or 600.2.2 | **Good practice** | **Good practice** | **Mandatory** | **Good practice** |

600.2.1 When practices, by way of business, 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 620, 630 and 660:

(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.

600.2.2 In addition, practices that provide trust or company services must adopt CDD, ongoing monitoring and RK procedures, when, by way of business, 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.

600.2.3 The provisions of these Guidelines should be read in the context of this subsection, together with the relevant provisions of Hong Kong laws, and applied accordingly.

### 600.3 The nature of money laundering and terrorist financing

600.3.1 "Money laundering" ("ML") is defined in AMLO[2] 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.

600.3.2 "Terrorist financing" ("TF") is defined in AMLO[3] 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.

600.3.3 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 are also inclined to find ways to obscure fund movements, whether or not such funds are the proceeds of crime, in order to be able to use them without attracting the attention of the authorities.

### 600.4 Financial Action Task Force and legislation concerned with money laundering and terrorist financing

600.4.1 The FATF has issued the FATFRs as a framework to detect and prevent ML/TF activities. They 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.

600.4.2 Among the key FATFRs 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 implement statutory AML/CFT regimes to reflect the basic requirements of CDD, RK and making STRs. They apply to DNFPBs, including accountants, in relation to specified service offerings (see paragraphs 600.2.1 and 600.2.2).

600.4.3 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, under the law, 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.

600.4.4 Apart from AMLO, the three main pieces of legislation in Hong Kong that are relevant to

2 AMLO, Schedule 1, Part 1.
3 Ibid.

ML/TF are DTROP, OSCO and UNATMO. It is important that practices and their staff fully understand their obligations under the respective pieces of legislation.

600.4.5 DTROP and OSCO create an offence of ML in relation to dealing with property known or believed to represent proceeds of drug trafficking specifically (under DTROP) or of an indictable offence generally (under OSCO)[4]. This is a serious offence carrying a maximum penalty of 14 years imprisonment and a fine of five million dollars.

600.4.6 DTROP, OSCO and UNATMO also contain provisions on making STRs and specify an offence of not reporting where a person has the requisite suspicion or knowledge[5]. They also specify an offence of "tipping off" in relation to making STRs (see Section 640 of these Guidelines). Additional information on the above legislation is provided in Appendix A.

4 Section 25 of DTROP and OSCO

5 Section 25A of DTROP and OSCO, and sections 12(1) and 14 of UNATMO

# SECTION 610

## AML/CFT Policies, Procedures and Controls

## General requirements

**610.1 Practices must have in place internal policies, procedures and other controls to address ML/TF concerns, and compliance with the existing legal requirements on AML/CFT, when they carry out any of the services specified in paragraphs 600.1.2 and 600.2.2 of these Guidelines, and should consider the need to do so in relation to other services that they provide. Practices should communicate these policies and procedures, etc., clearly to employees.**

610.1.1 **Controls cover primarily the following areas:**

**(a) risk assessment and management**
**(b) customer due diligence (Section 620)**
**(c) ongoing monitoring (Section 630)**
**(d) suspicious transactions reporting (Section 640)**
**(e) record keeping (Section 660)**
**(f) compliance management, including designating a Money Laundering Reporting Officer ("MLRO") at the management level**
**(g) staff hiring, ongoing training and communication (Section 670)**
**(h) group policy, where appropriate.**

**610.2 Adopting a risk-based approach**

610.2.1 While no system can be expected to detect and prevent all ML/TF activities, practices must 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's RBA Guidance for Accountants**.

610.2.2 A risk-based approach ("RBA") is recognised as an effective way to combat ML/TF. It helps 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.

610.2.3 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.

610.2.4 The type and extent of measures to be taken in relation to the items in paragraph 610.1.1 above should be appropriate and reasonable having regard to the risk of ML/TF. There is no one-size-fits-all approach. Some of the factors to be considered include:

- The nature, size and complexity of the practice's business
- The geographical spread of client operations and the practice's operation
- The extent to which the practice is dealing directly with the customer or through other intermediaries or third parties.

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

(a) the extent of 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 620);
(b) the level of ongoing monitoring to be applied to the relationship (see Section 630); and
(c) measures to mitigate any risks identified.

610.2.6 A reasonably designed RBA should assist practices to effectively manage potential ML/TF risks, rather than prohibiting 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 business.

610.2.7 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. Practices may therefore have to adjust their risk assessment of a particular client from time to time, based upon information obtained, and also review the extent and frequency of the CDD and ongoing monitoring to be applied to the client. Further information on ongoing monitoring is contained in Section 630.

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

**610.3 Management oversight**

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

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

610.3.2 To enable the CO and MLRO to discharge their responsibilities effectively, the 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 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, the senior management to ensure that the 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 their absence.

*Indicative roles of CO and MLRO*

610.3.3 The CO would generally 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.

610.3.4 Areas which may 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 FATFRs;

(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.

610.3.5 The MLRO must play an active role in the identification and reporting of suspicious transactions. The MLRO's principal functions 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")[6];

(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 function*

610.3.6 The compliance function of a practice should review the implementation of the AML/CFT controls, (including, 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.

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

*Staff screening*

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

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

### 610.4 Business conducted outside Hong Kong

610.4.1 Practices with overseas branches/ offices, or subsidiary undertakings, must 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.

610.4.2 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 610.4.1, the practice shall (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 requirements.

# SECTION 620

## Customer Due Diligence

## General requirements

**620.1 When carrying out any of the services specified in paragraphs 600.2.1 and 600.2.2, practices must perform 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[7] 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[8], 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, 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; and**

**Practices must adopt enhanced due diligence measures in relation to high-risk clients (including foreign "politically exposed persons" or "PEPs"), and may adopt simplified due diligence measures in certain specified circumstances.**

**620.2 Introduction to CDD**

620.2.1 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.

620.2.2 Practices must, therefore, identify, and verify the identity of their clients, to the extent necessary to provide them with reasonable assurance that the information they have is an appropriate and sufficient indication of the client's true identity. In general, 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") must be applied in respect of clients or circumstances determined to be of higher ML/TF risk.

620.2.3 Practices may have other client acceptance and continuance procedures, for example, to ensure compliance with independence requirements and to avoid conflicts of interest.

7 For definitions, see Appendix E.

8 For the purpose of these Guidelines, a trust means an express trust or any similar arrangement for which a legally-binding document (i.e., a trust deed or in any other form) is in place.

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.

620.2.4 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.

**620.3 Circumstances where CDD should be applied**

620.3.1 CDD requirements must 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 HK$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; or
(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*

620.3.2 Practices must 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 620.3.1 (c) and (d):
(a) 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;
(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) when a material change occurs in the way in which the client's business in conducted.

620.3.3 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 630).

620.3.4 If a practice is unable to comply with paragraph 620.3.2, AMLO[9] requires that the business relationship with the client be terminated as soon as practicable.

**620.4 Client acceptance/risk assessment and risk categories**

620.4.1 Practices should assess the ML/TF risks of individual clients when evaluating their clients during the acceptance stage and when taking on new engagements for pre-existing clients.

620.4.2 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 ongoing monitoring a fundamental component of a reasonably designed RBA. Practices may therefore have to adjust their risk assessment

9 See AMLO, Schedule 2, section 6(2)

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.

620.4.3 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, namely, client risk, country or geographic risk, and service, including delivery channel, risk.

620.4.4 Factors that may indicate a higher level of client risk include:

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

620.4.5 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.

620.4.6 As regards country or geographic risk, this, in conjunction with other risk factors, may provide useful information as to potential ML/TF risks. 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.

620.4.7 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 620.12.22-620.12.25). While extra care may be justified in such cases, it is not a requirement to refuse to do any business with such clients or automatically to classify them as high risk and subject them to an 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.

### 620.5 Identification and verification of the client's identity

620.5.1 Practices must 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 (see Section 660). 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 620.12.4-620.12.5).

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

### 620.6 Identification and verification of a beneficial owner

620.6.1 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. For a client who is an individual, not acting in an official capacity on behalf of a legal person or trust, the client him/herself 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/her own behalf.

620.6.2 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.

620.6.3 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.

620.6.4 Practices should identify all beneficial owners of a client. 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).

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

620.7.1 If a person purports to act on behalf of the client, practices must:

(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.

620.7.2 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 Appendix C.

620.7.3 Practices should also obtain written authority[10] verifying that the individual purporting to represent the client is authorised to do so.

### 620.8 Characteristics and evidence of identity

620.8.1 If suspicions are raised in relation to the veracity any document offered, practices should take practical and proportionate steps to establish whether the document offered is genuine, or has been reported as lost or stolen (e.g., searching publicly-available information, approaching relevant authorities 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 an STR.

620.8.2 Where documents are in a foreign language, practice should take appropriate steps to be reasonably satisfied that the documents provide evidence of the client's identity.

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

**620.9 Purpose and intended nature of business relationship**

620.9.1 Unless the purpose and intended nature are obvious, practices must obtain information from all new clients to satisfy themselves 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., the services that 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.

**620.10 Timing of identification and verification of identity**

*General requirement*

620.10.1 Generally, the CDD process, i.e., obtaining information on the client and beneficial owners, and about the purpose and intended nature of the business relationship, must 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 620.10.3.

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

*Delayed client identity verification and failure to complete verification*

620.10.3 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; and
(b) it is necessary not to interrupt the normal course of business with the client;

620.10.4 This discretion must 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.

620.10.5 Verification of identity must be concluded within a reasonable timeframe thereafter. Where this cannot be done, practices shall as soon as reasonably practicable suspend or terminate the service or relationship, unless there is a reasonable explanation for the delay[11].

620.10.6 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

[11] 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.

JFIU.

*Keeping client information up-to-date*

620.10.7 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 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 when:

(a) a significant or unusual activity or transaction is to take place[12];
(b) 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[13];
(c) a practice's client documentation standards change substantially; or
(d) 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. (See also Section 630 of these Guidelines.)

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

**620.11 Application of simplified client due diligence**

*When SDD can be conducted generally*

620.11.1 Where the risks of ML/TF are lower, practices may perform 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 (see paragraph 620.11.6).
(c) Reducing the frequency of client identification updates.
(d) Reducing the degree of ongoing 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.

620.11.2 SDD measures shall 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 may fall within the scope of paragraphs 620.11.5, 620.11.9 and 620.1.10 below, or where specific higher-risk scenarios apply, e.g., where the client is from, or based in, a higher-risk country or jurisdiction.

620.11.3 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

---

12 "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.

13 Reference should also be made to AMLO Schedule 2, section 6.

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.

620.11.4 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.

*Specific types of client to which SDD may be applied*

620.11.5 AMLO indicates that it is not necessary to identify and verify the identity of any beneficial owner, in the circumstances set out in paragraph 620.3.1(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 620.15);
(c) a corporation listed on a stock exchange;
(d) an FI, as defined in AMLO;
(e) an institution incorporated or established in an equivalent jurisdiction which carries on a business similar to an FI, is subject to AML/CFT requirements consistent with standards set by the FATF and is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to a relevant authority[14];
(f) an investment vehicle where the person responsible for carrying out the CDD-related 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, which has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2 of AMLO, and is supervised for compliance with those requirements.

620.11.6 If a client not falling within paragraph 620.11.5 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 or of any person in that chain beyond that entity, in the circumstances referred to in paragraph 620.3.1(a) or (b).

*Foreign financial institutions*

620.11.7 For ascertaining whether an institution meets the criteria set out in paragraph 620.11.5(f) 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*

620.11.8 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.

*Government and public bodies*

620.11.9 Public body includes:
(a) any executive, legislative, municipal or urban council;

14 I.e., the regulators of relevant FIs in Hong Kong

(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 of the Hong Kong SAR 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*

620.11.10 It is not necessary to identify and verify the identity of any beneficial owner of the client, in the circumstances referred to in paragraph 620.3.1(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.

*Solicitor's client accounts*

620.11.11 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 620.3.1(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.

**620.12 Application of enhanced client due diligence**

*High-risk situations*

620.12.1 In situations that, by their nature, present a higher risk of ML/TF, practices must carry out additional measures or EDD[15] to mitigate the risk of ML/TF. (Examples of possible risk factors are indicated in Appendix B.) Depending upon whether the business relationship is to be or has been established, EDD must include:
(a) obtaining the approval of the senior management to commence or continue the relationship, as applicable; and
(b) taking reasonable measures to establish the relevant client's or beneficial owner's source of wealth and of the funds that are or will be involved in the business relationship, or other additional mitigation measures, e.g.:
  (i) obtaining additional information on the intended nature of the business relationship (e.g., anticipated account activity);
  (ii) obtaining additional information on the client (e.g., connected parties[16], accounts or relationships) and updating the client profile more regularly;
  (iii) 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.

*Client not physically present for identification purposes*

620.12.2 Practices must apply equally effective client identification procedures and ongoing

15 Additional measures should be documented in the practice's policies and procedures.

16 Consideration may be given to obtaining, and taking reasonable measures to verify, the addresses of directors and account signatories.

monitoring standards for clients not physically present for identification purposes as for those where the client is available for interview[17]. 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 must 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 620.5, but not previously used for the purposes of verifying the client's identity;
(b) taking supplementary measures to verify the information relating to the client that has been obtained by the practice.

620.12.3 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*

620.12.4 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 paragraphs 620.13.7-620.13.9;
(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.

620.12.5 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.

*Politically exposed persons*

General

620.12.6 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 because their office and position may render such 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, particularly where such countries do not have adequate AML/CFT standards.

620.12.7 While the statutory definition of PEPs in AMLO (see paragraph 620.12.9) includes only individuals entrusted with a prominent public function in a place outside the People's Republic of China[18], domestic PEPs may also present, by virtue of the positions they hold, a high risk situation in which EDD should be applied. Practices should therefore adopt an RBA in determining whether to also apply the measures in paragraph 620.12.14 to domestic PEPs.

620.12.8 The statutory definition does not automatically exclude sub-national political figures. In determining what constitutes a prominent public function, practices should consider

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

[18] Under the Interpretation and General Clauses Ordinance (Cap. 1), the definition of the People's Republic of China includes Hong Kong, Taiwan and Macau.

factors such as persons with significant influence in general, significant influence over or control of public procurement, state-owned enterprises, etc.

(Foreign) PEPs

620.12.9 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).

620.12.10 AMLO defines a "close associate" as:

(a) an individual who has close business relations with a person falling under paragraph 620.12.9(a) above, including an individual who is a beneficial owner of a legal person or trust of which the relevant person 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 620.12.9(a).

620.12.11 Practices should establish and maintain effective procedures for determining whether a client or a beneficial owner of a client is a PEP. Risk can be reduced by conducting EDD before establishing the business relationship and ongoing monitoring where the practice knows or suspects that the client relationship is with, or involves, a PEP.

620.12.12 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.

620.12.13 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/her public office or has been entrusted with his/her 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.

620.12.14 When practices know that a particular client or beneficial owner is a PEP, before establishing a business relationship, or continuing an existing business relationship, where the client or the beneficial owner is subsequently found to be a PEP, they must apply the following EDD measures:

(a) obtain approval from the 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.

620.12.15 It is for practices to decide the measures they deem reasonable to establish the source of funds and wealth, in accordance with their assessment of the risks,.

Domestic PEPs

620.12.16 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, 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 620.12.10).

620.12.17 Practices must take reasonable measures to determine whether an individual is a domestic PEP. If an individual is known to be a domestic PEP, a practice must perform a risk assessment to determine whether the individual poses a higher risk of ML/TF. Domestic PEP 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 must apply the EDD and monitoring referred to in paragraph 620.12.14.

620.12.18 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*

620.12.19 As regards the level of 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, where one has been appointed. In general the more potentially sensitive the PEP, the higher the approval process should be escalated.

*Periodic reviews*

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

*Bearer shares*

620.12.21 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 apply, or insufficiently apply, the FATFRs, or otherwise posing higher ML/TF risk*

620.12.22 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 apply, or which insufficiently apply, the FATFRs; and
(b) transactions and businesses connected with jurisdictions assessed as higher ML/TF risk.

620.12.23 In determining which jurisdictions either do not apply, or insufficiently apply, the FATFRs, or which 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 620.12.25);
(b) whether the jurisdiction is subject to sanctions, embargoes or similar measures imposed by, for example, the Security Council of the United Nations ("UN Security Council")(see Section 650);
(c) whether the jurisdiction is identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measures[19];
(d) whether the jurisdiction is identified by credible sources as providing funding or support for terrorist activities or 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.

620.12.24 Practices should be aware of the potential reputational risk of conducting business in jurisdictions that do not apply, or insufficiently apply, the FATFRs, or other jurisdictions known to apply inferior standards for the prevention of ML/TF. If practices established in Hong Kong have office 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.

620.12.25 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.

**620.13 Reliance on CDD performed by intermediaries**

*General*

620.13.1 Practices may rely upon an intermediary to perform any part of the CDD measures specified in subsection 620.1, subject to confirming that the intermediary has adequate AML/ CFT controls in place and the other considerations set out in this section. However, the ultimate responsibility for ensuring that CDD requirements are met remains with practices.

620.13.2 Reliance on third parties may occur through, e.g., introductions made by another member of the same network or referrals from other practices or other professionals.

620.13.3 Written confirmation shall be obtained from the intermediary that:

[19] "Credible sources" refers to information that is produced by well-known bodies generally regarded as reputable, which 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.

(a) it agrees to perform the role; and
(b) it will provide without delay a copy of any document or record obtained in the course of carrying out the CDD measures on behalf of the practice, upon request.

620.13.4 Practices should obtain satisfactory evidence to confirm the status and eligibility of the intermediary. Such evidence may comprise evidence from the intermediary of its status, regulation, policies and procedures.

620.13.5 Practices that carry out a CDD measure by means of an intermediary must as soon as possible after the intermediary has carried out that measure, obtain from the intermediary the data or information that the intermediary has obtained in the course of carrying out that measure. This does not require obtaining at the same time a copy of the document, or a record of the data or information, that is obtained by the intermediary.

620.13.6 Where these documents and records are kept by the intermediary, practice must obtain an undertaking from the intermediary to keep all underlying CDD information throughout the continuance of the practice's business relationship with the client and for at least five years beginning on the date on which the relationship of the client with the practice ends. An undertaking must also be obtained from the intermediary to supply copies of all underlying CDD information where the intermediary is about to cease trading or will no longer continue to act as an intermediary for the practice.

*Domestic intermediaries*

620.13.7 Practices may rely upon the following to perform any part of the CDD measures:
(a) certain types of FIs, as specified in AMLO, Schedule 2, section 18(3)(b) (i.e., an authorised institution, a licensed corporation, an authorised insurer, an appointed insurance agent or an authorised insurance broker); or
(b) a DNFBP, provided that the intermediary is able to satisfy the practice it has adequate procedures in place to prevent ML/TF.

*Overseas intermediaries*

620.13.8 Practices may rely upon an overseas intermediary carrying on business or practising in an equivalent jurisdiction to perform any part of the CDD measures, only where the intermediary:
(a) falls into one of the following categories of businesses or professions:
  (i) an institution that carries on in the jurisdiction a business similar to those referred to in paragraph 620.13.7(a);
  (ii) a lawyer, a notary public; an auditor, a professional accountant, a trust or company service provider, or a tax adviser practising in the jurisdiction;
  (iii) a trust company carrying on trust business in the jurisdiction;
  (iv) a person who carries on in the jurisdiction a business similar to that carried on by an estate agent; and
(b) is required under the law of the jurisdiction concerned to be registered or licensed or is regulated under the law of that jurisdiction;
(c) has measures in place to ensure compliance with CDD and RK requirements similar to those under Schedule 2 of AMLO, and is supervised for compliance with those requirements by an authority in that jurisdiction similar to any of the relevant authorities or regulatory bodies (as applicable) in Hong Kong.

**620.14 Prohibition on anonymous accounts**

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

### 620.15 Jurisdictional equivalence

*Determination of jurisdictional equivalence*

620.15.1 Jurisdictional equivalence is an important aspect in the application of CDD measures above. "Equivalent jurisdiction" is defined in 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 AMLO.

620.15.2 Practices may, therefore, need to consider which jurisdictions, other than FATF members, apply requirements similar to those imposed under Schedule 2 of AMLO (or these Guidelines) for jurisdictional equivalence purposes. When doing so practices should document their assessment, which may include consideration of the following positive or negative factors:

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

(b) mutual evaluation reports undertaken by the FATF, FATF-style regional bodies, the International Monetary Fund and the World Bank, etc., bearing 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;

(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 relation to AML/CFT, published by specialised national, international, non-governmental and commercial organisations (e.g., Transparency International’s "Corruption Perceptions Index"; and

(f) guidance provided at paragraph 620.12.25.

# SECTION 630

## Ongoing Monitoring

## General requirements

**630.1 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.**

630.1.1 **When carrying out any of the services specified in paragraphs 600.1.2 and 600.2.2, practices shall 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 of money, or unusual patterns of activity, which have no apparent economic or lawful purpose, examining the background and purposes of those transactions and recording their findings in writing.**

630.1.2 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.

630.1.3 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.

630.1.4 Practices should be vigilant for significant changes in relation to 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 introduced;
(b) new corporate or trust structures are created;
(c) the stated activity or turnover of a client changes or increases; or
(d) the nature, frequency or size of activities changes, etc.

630.1.5 Where transactions are complex, involve unusually large sums of money, or unusual patterns of activity, and have no apparent economic or lawful purpose, practices must examine the background and purpose, including, where appropriate, the circumstances, of the transactions. The findings of these examinations must 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.

630.1.6 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.

## 630.2 Risk-based approach in relation to monitoring

630.2.1 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.

630.2.2 Practices must take additional measures, such as conducting more frequent reviews, 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 public information or information in its possession, to be a PEP.

*Pre-existing clients*

630.2.3 In relation to pre-existing clients, when practices perform ongoing monitoring before they first carrying out CDD measures in relation to the client, under AMLO, practices are required only to review the documents, data and information relating to the client that are held by them at the time that they conduct the review.

# SECTION 640

## Making Suspicious Transaction Reports

## General requirements[20]

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

640.1.1 **Once knowledge or suspicion of an ML/TF transaction or activity has been established, the following general requirements apply:**

**(a) Practices must make a report to an authorised officer[21] even where no service has been provided by the practice[22] A member working in a practice may discharge his/her responsibility by making a report to the MLRO designated by his/her employer;**

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

**(c) practices must 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 the client is such that tipping off cannot be construed to have taken place.**

**Under Hong Kong laws, the requirement to make suspicious transaction reports is not limited to any particular services or situations and, therefore, it applies to all services provided by practices.**

**640.2 Legal requirements in relation to making suspicious transaction reports**

640.2.1 Under sections 25A(1) of DTROP/ OSCO, a person must 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[23];
(b) was used in connection with; or
(c) is intended to be used in connection with,

drug trafficking/ an indictable offence/.

---

20 See also the Institute's **frequently-asked questions on suspicious transaction reporting**.

21 See Footnote 1.

22 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.

23 DTROP/OSCO, section 25A(1).

640.2.2 Under section 12(1) of UNATMO, where a person knows or suspects that any property is terrorist property, the person must 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.

640.2.3 It is an offence under section 25A of DTROP/OSCO and section 14(5) of UNATMO, carrying a maximum penalty of three months imprisonment and a fine at **level 5**[24], to fail to make a disclosure to an authorised officer where a person has the requisite knowledge or suspicion.

640.2.4 Once an employee has reported his/her 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[25].

640.2.5 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 person undertakes the disclosed acts and the acts are undertaken with the consent of the JFIU; or
(b) the STR is made after a person has performed the disclosed acts and the report is made on the person's own initiative and as soon as it is reasonable for the person to do so[26].

640.2.6 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[27].

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

640.2.7 CDD and ongoing monitoring provide the basis for recognising unusual and suspicious transactions and events. The key is to know enough about a 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.

640.2.8 Practices must ensure members of staff are made aware of their statutory obligations and that sufficient guidance and training are provided to enable them to recognise when ML/TF may be taking place[28]. Staff also need to be sensitive to the risk of tipping off during their client work (see paragraphs 640.2.16-640.2.21).

640.2.9 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 proceeds themselves have definitely arisen from the criminal offence.

640.2.10 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 are only indications of the most basic ways in which money may be laundered. However, identification of any of the circumstances similar to those listed in

---

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

25 DTROP/OSCO, section 25A(4); UNATMO, section 12(4)

26 DTROP/OSCO, section 25A(2); UNATMO, section 12(2).

27 DTROP/OSCO, section 25A(3); UNATMO section 12(3).

28 See Section 8 of these Guidelines for further information on staff hiring and training.

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.

640.2.11 Practices should also be aware of elements of individual transactions that could indicate property involved in TF. The FATF has issued **Guidance for Financial Institutions in Detecting Terrorist Financing**, which may also be a useful reference for practices.

*Timing and manner of reports*

640.2.12 In making STRs to the JFIU, the use of a standard form or the use of the e-channel "STREAMS"[29] 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.

640.2.13 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.

640.2.14 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.

640.2.15 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 may arise outside Hong Kong, reporting to the JFIU may be required, but only if section 25A of DTROP/OSCO applies[30].

*Tipping off*

640.2.16 A person commits an offence of "tipping off", under DTROP/OSCO or UNATMO[31], if, knowing or suspecting that an STR has been made, 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 $500,000.

640.2.17 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 should not be made aware that relevant agencies have been alerted about his/her name.

640.2.18 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

---

29 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.

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

31 DTROP/OSCO section 25A(5); UNATMO section 12(5)

activities or transactions relate to ML/TF, they should take into account the risk of tipping off when completing the CDD process. Practices shall ensure that their employees are aware of and sensitive to these issues when conducting CDD.

640.2.19 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.

640.2.20 Therefore, unless a staff member making enquiries has knowledge or suspicion of a current or impending investigation, where a practice is seeking 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 shall not be informed or alerted.

640.2.21 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.

**640.3 Internal reporting and recording**

640.3.1 As indicated in Section 2, practices must 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 by the practice 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 for the MLRO to keep a record of discussions relating to internal reports.

640.3.2 Where staff members working in a practice have knowledge or suspicion of matters referred to in paragraphs 640.2.1 or 640.2.2, 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.

640.3.3 The MLRO should consider all internal disclosures he/she receives in the light of full access to all relevant documentation and other parties. 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 be made to the JFIU. If there are, the MLRO shall 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 must document the reasons.

640.3.4 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 there is knowledge or suspicion of ML/TF.

640.3.5 When reporting suspicious transactions to the JFIU, sufficient information should be provided, including, e.g., the following details, as applicable[32]:

(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 or company about the transaction.

640.3.6 To assist the disclosure of all relevant information, JFIU have provided **a form** on its website. An STR to the JFIU can be made through STREAMS, by email, fax, mail or telephone.

640.3.7 Practices must establish and maintain procedures to ensure that:

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

640.3.8 While practices may allow staff members to consult with supervisors or managers before deciding whether to draw up a report to the MLRO, in the normal course of events, any report 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.

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

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

640.3.11 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 must make further reports to the JFIU, if appropriate.

640.3.12 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 (e.g., as suggested in the systematic

32 See the JFIU website: https://www.jfiu.gov.hk/en/str_main.html.

approach to identifying suspicious transactions recommended by the JFIU[33]).

640.3.13 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.

640.3.14 If, after completing the evaluation, the MLRO decides that there are grounds for knowledge or suspicion, he/she must 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 the MLRO acts conscientiously and in good faith, there should not be any issue of failing to report where he/she 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.

640.3.15 In relation to section 25A(2) of DTROP/OSCO 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.

640.3.16 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, the MLRO should, nevertheless, be alerted to the situation.

640.3.17 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 640.2.5).

640.3.18 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.

640.3.19 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.

640.3.20 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 640.2.6), 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.

---

33 For details, see: **https://www.jfiu.gov.hk/en/str_ask.html**

Recording internal reports and reports to the JFIU

640.3.21 Practices must 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.

640.3.22 Practices must 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.

**640.4 Post-reporting matters**

640.4.1 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 or 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 specific 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.

640.4.2 The Institute understands that the JFIU will 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 matters on which the knowledge or suspicion is based.

640.4.3 Whilst there is no statutory requirement to provide feedback arising from investigations, the JFIU provides feedback in its quarterly report[34] and, the Institute also understands, upon request, to a disclosing practice in relation to the current status of the investigation.

[34] 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.

640.4.4 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 limits 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.

640.4.5 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.

**640.5 Organisations other than member practices**

640.5.1 Members working in organisations other than practices should ascertain whether their employers have procedures for making STRs through a CO/ MLRO. As indicated above, employees who make reports in accordance with procedures laid down by their employers are regarded as complying with the relevant laws[35]. In the absence of any employer's procedures, STRs would need to be made direct to the JFIU.

640.5.2 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 regulator. It should be noted that, under 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 AMLO. The maximum penalty 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[36].

[35] See Footnote 26.

[36] AMLO, section 5.

# SECTION 650

## Financial Sanctions and Terrorist Financing

## General requirements

**650.1 In relation to targeted financial sanctions and the financing of terrorism/ proliferation of weapons of mass destruction, practices must take note of and comply with their legal obligations, which include considering the need to make STRs.**

650.1.1 Targeted financial sanctions are a specific type of sanctions decided by the UN Security Council for freezing funds, financial assets and economic resources owned or controlled, directly or indirectly, by designated individuals or entities and for preventing funds, financial assets or economic resources from being made available to such individuals and entities. Practices may refer to sanctions lists maintained by the UN Security Council and its Sanctions Committees. The lists are available on the webpages of the **relevant committees**.

650.1.2 The United Nations Sanctions Ordinance (Cap. 537) ("UNSO") empowers the Chief Executive of the Hong Kong SAR to make regulations to implement sanctions decided by the UN Security Council, including targeted financial sanctions against individuals or entities designated by the UN Security Council or its committees. Designated individuals and entities are specified by notice published in the Gazette.

650.1.3 Under the regulations made under the UNSO, it is an offence to make available any funds or other financial assets or economic resources to, or for the benefit of, such designated person or entity, as well as those acting on their behalves, at their direction, or owned or controlled by them; or to deal with any funds, other financial assets or economic resources belonging to, or owned or controlled by, such persons and entities, except under the authority of a licence granted by the Chief Executive. Offenders are subject to a maximum sentence of 7 years' imprisonment and an unlimited amount of fine. These prohibitions are relevant not only to FIs, but also to DNFBPs, including accountants, and practices must take steps to keep themselves informed of the current list of designated individuals and entities. For enquiries about licence applications, practices should approach the Commerce and Economic Development Bureau.

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

650.1.5 Practices should conduct name checks of their clients and their beneficial owners against the latest lists of the designated individuals and entities. Practices should report to the Institute any actions taken in compliance with the targeted financial sanctions, including attempted transactions.

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

*Terrorist financing*

650.1.7 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. Initially, this was not part of the AML regime, but subsequently the AML framework was expanded to include special recommendations on TF. With ML, the focus is on the handling of criminal proceeds, i.e., the source of property is what matters.

With TF, however, the focus is on the destination or use of property, which may have originated from legitimate sources.

650.1.8 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. The **UN Counter Terrorism Committee** has issued relevant guidance in relation to the implementation of UNSCRs.

650.1.9 UN has also published the names of individuals and organisations subject to UN financial sanctions in relation to involvement with ISIL (Da'esh), Al-Qa'ida, and the Taliban under relevant UNSCRs (e.g., UNSCR 1267 (1999), 1989 (2011) and 2253 (2015)). All UN member states are required under international law to freeze the funds and economic resources of any legal persons named in this list and to report any suspected name matches to the relevant authorities.

650.1.10 UNATMO was enacted in 2002 to give effect to the mandatory elements of UNSCR 1373 and the FATFRs relating to TF.

650.1.11 The Secretary for Security of the Hong Kong SAR ("S for S") has the power to freeze suspected terrorist property and may direct that a person must not deal with the frozen property except under the authority of a licence. Contraventions are subject to a maximum penalty of seven years imprisonment and an unspecified fine.

650.1.12 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.

650.1.13 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.

650.1.14 Where a person is designated by a committee of the UN Security Council as a terrorist, generally, that person's details will subsequently be published in a notice under section 4 of UNATMO in the Government Gazette.

650.1.15 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.

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

*Proliferation of weapons of mass destruction*

650.1.17 Under the Weapons of Mass Destruction (Control of Provision of Services) Ordinance (Cap. 526), it is 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 in or outside Hong Kong. The provision of services is widely defined and includes the lending of money or other provision of financial assistance as well as the provision of professional services.

### 650.2 Database maintenance and screening (clients and payments)

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

650.2.2 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.

650.2.3 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 updating when there are changes, and made easily accessible by staff for the purpose of identifying suspicious transactions.

650.2.4 Ongoing screening by practices of their 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.

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

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

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

650.2.8 If practices suspect that an activity or transaction is terrorist related, they must 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.

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

650.2.10 Where an STR is made pursuant to paragraph 650.2.8, practices must not disclose to another person any information or matters, which are likely to prejudice the investigation, as tipping off is also an offence under UNATMO.

# SECTION 660

# RECORD KEEPING

## General requirements

**660.1 In relation to any of the services specified in paragraphs 600.2.1 and 600.2.2, practices must prepare, maintain and retain documentation and records on their business relations with, and transactions for, clients, as 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 must 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, STRs, and staff training).**

**Records in relation to particular transactions and clients must be retained for at least five years after the transaction has been completed or the business relationship has ended, as applicable.**

660.1.1 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. It 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.

660.1.2 Records must 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 clients (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.

660.1.3 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 assessments of the training needs of staff and steps taken to meet those needs be retained.

### 660.2 Retention of records relating to client identity and business relationships

660.2.1 Practices must 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[37] 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.

660.2.2 AMLO requires that all relevant documents and records must be kept throughout the business relationship with or transaction for the client and retained for a period of at least five years after the end of the business relationship or transaction, as applicable. Information relating to STRs must also be retained for at least five 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.

660.2.3 As practices need to maintain records for a wide range of purposes to 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.

660.2.4 Records of internal reports are not considered to form part of client assignment working papers, and so it is advisable that such records be 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.

### 660.3 Manner in which records are to be kept

660.3.1 AMLO states that records required to be kept must be kept in the following way[38]:

(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.

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

---

[37] 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.

[38] Schedule 2, section 21

# SECTION 670

# STAFF HIRING AND TRAINING

## GENERAL REQUIREMENTS

**670.1 Practices' AML/CTF policies, procedures and controls must cover employee hiring and training.**

670.1.1 As indicated in Section 610, 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.

670.1.2 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.

670.1.3 Practices must 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.

670.1.4 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.

670.1.5 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 those 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 those 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.

670.1.6 Depending on the seniority and nature of work of different groups of staff, training should include:

(a) an introduction of the background to ML/TF;
(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.

670.1.7 COs and other managerial staff, including internal audit, where applicable, 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.

670.1.8 MLROs[39] may require more specific training:

(a) on their responsibilities for assessing reports submitted to them and making STRs to the JFIU; and
(b) to keep abreast of AML/CFT requirements and developments generally.

670.1.9 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.

670.1.10 Practices must maintain records of staff training (e.g., who has been trained and when, and the type of the training provided).

670.1.11 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, their 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.

39 As noted in Section 610, in some practices, the CO and the MLRO may be the same person

# Appendices A – E

## Further information and examples for reference

# APPENDIX A

## Further information on the Financial Action Task Force, money laundering /terrorist financing 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 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 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. 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 case of ***HKSAR v Pang Hung Fai***[40], the Court of Final Appeal ("CFA"), referencing the judgment of the Appeal

[40] 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.

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."

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[41] or to specify an indictable offence in the charge[42].

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 DTROP/ OSCO 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 640 of these Guidelines, both DTROP and OSCO 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:
    (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.

41 *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.

42 *Lam Hei Kit v HKSAR* FAMC 27/2004.

15. "Authorised officer" means[43]:
    (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 DTROP/ OSCO, 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.[44]

20. Relevant definitions under UNATMO include the following:
    "Authorised officer" means[45]:
    (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, 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

43 In practice STRs will generally be made to the JFIU, which is a joint unit of the Hong Kong Police Force and Customs and Excise Department.

44 UNATMO, section 12(1).

45 See Footnote 44.

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[46], 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[47], it must be based on some evidence, even if that evidence is tentative.[48]

24. In the case of Queensland Bacon PTY Ltd v Rees[49], it was stated: "…A suspicion that 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**[50], 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."[51]

*Investigations and access to information*

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

---

46 The Consultative Committee of Accounting Bodies ("CCAB"), *Anti-money laundering guidance for the accountancy sector*, 2008. (**http://www.ccab.org.uk/PDFs/CCAB%20guidance%202008-8-26.pdf**, paragraph 2.25). See also the revised CCAB guidance, August 2017 (**https://www.ccab.org.uk/documents/TTCCABGuidance2017regsAugdraftforpublication.pdf**, paragraph 6.1.5).

47 Ibid.

48 Ibid., paragraph 2.26.

49 [1966] 115 CLR 266 at 303, per Kitto J

50 Da Silva [2006] EWCA Crim 1654, at16.

51 Ibid.

AMLO

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

28. Parts 2 and 3 of 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 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 and certain DNFBPs may rely on CDD conducted by some 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 and it could be, for example, an overseas network firm introducing a client to a CPA firm in Hong Kong.

# 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) <u>Reduced transparency</u>

   - 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;
- 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*[52]

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[53];
- 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.

- 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;

52 In assessing country risk associated with a client, consideration may be given to local legislation (UNSO, UNATMO, etc.), 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 practice is part of an international network which may have indicated weaknesses in other jurisdictions).

53 See paragraphs 620.12.22-620.12.25.

- 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/ 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 incorporating photographic evidence of the identity of the applicant, issued by a competent national or state authority. International drivers' permits and licences are not included for this purpose.

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 identity 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:
   (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 may be retained.

3. For minors born in Hong Kong who are not in possession of a valid travel document or Hong Kong Identity Card[54], 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 may 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, may 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.

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 may 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.

8. Where a client has not been physically present for identification purposes, additional measures may need to be carried out (see paragraphs 620.12.2–620.12.3 of these Guidelines).

[54] 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.

Address identification

9. The residential address (and permanent address if different) of a direct client with whom a business relationship is being established may be obtained, 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 may therefore be obtained.

Other considerations

11. 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 may 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 may be paid to persons who exercise ultimate control over the management of the client.

2. The residential address (and permanent address if different) of beneficial owners may be obtained.

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, the client's legal form, structure and ownership should be 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 may be obtained as the standard requirement; thereafter, on the basis of the ML/TF risk, it can be decided whether further verification of identity may be required and, if so, the extent of that further verification. It can 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 may be obtained.

8. In the course of verifying the client's information mentioned in paragraph 7, the following information may 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[55] may be recorded and their identities verified using an RBA.

10. Where possible, the following may 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
.

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[56];

*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[57] 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 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.

---

55 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 subsections 620.6 and 620.7 of these Guidelines).

56 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.

57 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.

## C. Beneficial owners

Corporations

1. In relation to beneficial owners of corporations, in normal, non-high risk, situations, AMLO requires verification of 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 would 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 be 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, the focus should be on on identifying and taking reasonable measures to verify the identity of those who exercise ultimate control over the management of the company.

Partnerships and unincorporated bodies

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, AMLO requires verification of 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 may 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 may 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, regard may be had 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, it may be decided whether to continue to regard the client as a collection of individuals, or whether to be satisfied with evidence of membership of a relevant professional or trade association. In either case, the partnership deed (or other evidence in the case of sole traders or other unincorporated bodies), may be sought to ascertain 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, AMLO requires verification of 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. The following identification information in respect of a trust on whose behalf the trustee (i.e., the client) is acting may 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 appropriate evidence to verify the existence, legal form and parties to it, i.e., trustee, settlor, protector, beneficiary, etc. may be obtained. The beneficiaries should be identified as far as possible, where defined. If the beneficiaries are yet to be determined, the focus may be on identifying 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[58] in the relevant country of establishment;
(c) a written confirmation from a trustee acting in a professional capacity[59]; or
(d) a written confirmation from a lawyer who has reviewed the relevant instrument.

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

21. Where only a class of beneficiaries is available for identification, the focus may be on seeking to ascertain and name the scope of the class (e.g., children of a named individual).

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

---

58 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.

59 "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. Indicators of suspicious transactions should be considered, such as the nature and parties involved, including the involvement of jurisdictions that insufficiently apply FATFRs 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:[60]
   - (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;

60 See the JFIU website at: **https://www.jfiu.gov.hk/en/str_screen.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 Division, 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: Glossary of key terms and abbreviations, and definitions**

| Terms / abbreviations | Meaning |
|---|---|
| AMLO | Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions and Designated Non-Financial Businesses and Professions) Ordinance (Cap. 615) |
| AML/CFT | Anti-money laundering and counter financing of terrorism |
| Beneficial owner | (a) In relation to a corporation—<br>(i) means an individual who—<br>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;<br>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<br>C. exercises ultimate control over the management of the corporation; or<br>(ii) if the corporation is acting on behalf of another person, means the other person;<br><br>(b) in relation to a partnership—<br>(i) means an individual who—<br>A. is entitled to or controls, directly or indirectly, more than a 25% share of the capital or profits of the partnership;<br>B. is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights in the partnership; or<br>C. exercises ultimate control over the management of the partnership; or<br>(ii) if the partnership is acting on behalf of another person, means the other person;<br><br>(c) in relation to a trust, means—<br>(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;<br>(ii) the settlor of the trust;<br>(iii) a protector or enforcer of the trust; or<br>(iv) an individual who has ultimate control over the trust; and<br><br>(d) in relation to a person not falling within paragraph (a), (b) or (c)—<br>(i) means an individual who ultimately owns or controls the person; or<br>(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:<br><br>(i) that has an element of duration; or<br>(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.<br><br>***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:<br><br>(a) an accounting professional;<br>(b) an estate agent;<br>(c) a legal professional; or<br>(d) a TCSP licensee;<br><br>"*accounting professional*" means—<br>(a) a certified public accountant or a certified public accountant (practising), as defined by section 2(1) of the Professional Accountants Ordinance (Cap. 50);<br>(b) a corporate practice as defined by section 2(1) of the Professional Accountants Ordinance (Cap. 50); or<br>(c) a firm of certified public accountants (practising) registered under Part IV of the Professional Accountants Ordinance (Cap. 50);<br><br>"*TCSP licensee*" is a person licensed under AMLO to carry on a trust or company service business, *"Trust or company service"* as defined in Schedule 1 Part 1 of AMLO, i.e., those services referred to in paragraph 600.2.2 of these Guidelines |
| DTROP | Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405) |
| EDD | Enhanced client due diligence |

| | |
|---|---|
| FATF | Financial Action Task Force |
| FATFR | Financial Action Task Force Recommendations |
| FI | Financial institution |
| ICO | Insurance Companies Ordinance (Cap. 41) |
| Individual | Individual means a natural person, other than a deceased natural person. |
| Institute | Hong Kong Institute of Certified Public Accountants |
| 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 | As defined in Schedule 1 of AMLO. (See also section 600.3 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 | Politically exposed person |
| Relevant authority | As defined in AMLO, Schedule 1, Part 2, which are the regulators for the FIs and licensed money service operators |
| RBA | Risk-based approach to CDD and ongoing monitoring |
| Regulatory body | As defined in AMLO, Schedule 1, Part 2, which are the regulator for the DNFBPs , including, for an accounting professional, the HKICPA |
| RK | Record-keeping |
| Schedule 2 | Schedule 2 to the AMLO |
| SDD | Simplified client due diligence |

| | |
|---|---|
| Senior management | Senior management means partners, 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 | As defined in Schedule 1 of AMLO. (See also section 600.3 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) |

# DEFINITIONS

In this *Code of Ethics for Professional Accountants* the following expressions have the following meanings assigned to them:

| | |
|---|---|
| Acceptable level | A level at which a reasonable and informed third party would be likely to conclude, weighing all the specific facts and circumstances available to the professional accountant at that time, that compliance with the fundamental principles is not compromised. |
| Advertising | The communication to the public of information as to the services or skills provided by professional accountants in public practice with a view to procuring professional business. |
| Assurance client | The responsible party that is the person (or persons) who:<br>(a) In a direct reporting engagement, is responsible for the subject matter; or<br>(b) In an assertion-based engagement, is responsible for the subject matter information and may be responsible for the subject matter. |
| Assurance engagement | An engagement in which a professional accountant in public practice expresses a conclusion designed to enhance the degree of confidence of the intended users other than the responsible party about the outcome of the evaluation or measurement of a subject matter against criteria.<br>(For guidance on assurance engagements see the Hong Kong Framework for Assurance Engagements which describes the elements and objectives of an assurance engagement and identifies engagements to which Hong Kong Standards on Auditing (HKSAs), Hong Kong Standards on Review Engagements (HKSREs) and Hong Kong Standards on Assurance Engagements (HKSAEs) apply.) |
| Assurance team | (a) All members of the engagement team for the assurance engagement;<br>(b) All others within a firm who can directly influence the outcome of the assurance engagement, including:<br>(i) those who recommend the compensation of, or who provide direct supervisory, management or other oversight of the assurance engagement partner in connection with the performance of the assurance engagement;<br>(ii) those who provide consultation regarding technical or industry specific issues, transactions or events for the assurance engagement; and<br>(iii) those who provide quality control for the assurance engagement, including those who perform the engagement quality control review for the assurance engagement. |

| | |
|---|---|
| Audit client | An entity in respect of which a firm conducts an audit engagement. When the client is a listed entity, audit client will always include its related entities. When the audit client is not a listed entity, audit client includes those related entities over which the client has direct or indirect control. |
| Audit engagement | A reasonable assurance engagement in which a professional accountant in public practice expresses an opinion whether financial statements are prepared, in all material respects (or give a true and fair view or are presented fairly, in all material respects,), in accordance with an applicable financial reporting framework, such as an engagement conducted in accordance with Hong Kong Standards on Auditing. This includes a Statutory Audit, which is an audit required by legislation or other regulation. |
| Audit team | (a) All members of the engagement team for the audit engagement;<br>(b) All others within a firm who can directly influence the outcome of the audit engagement, including:<br>(i) Those who recommend the compensation of, or who provide direct supervisory, management or other oversight of the engagement partner in connection with the performance of the audit engagement including those at all successively senior levels above the engagement partner through to the individual who is the firm's Senior or Managing Partner (Chief Executive or equivalent);<br>(ii) Those who provide consultation regarding technical or industry-specific issues, transactions or events for the engagement; and<br>(iii) Those who provide quality control for the engagement, including those who perform the engagement quality control review for the engagement; and<br>(c) All those within a network firm who can directly influence the outcome of the audit engagement. |
| Close family | A parent, child or sibling who is not an immediate family member. |
| Contingent fee | A fee calculated on a predetermined basis relating to the outcome of a transaction or the result of the services performed by the firm. A fee that is established by a court or other public authority is not a contingent fee. |
| Direct financial interest | A financial interest:<br>(c) Owned directly by and under the control of an individual or entity (including those managed on a discretionary basis by others); or<br>(d) Beneficially owned through a collective investment vehicle, estate, trust or other intermediary over which the individual or entity has control, or the ability to influence investment decisions. |

| | |
|---|---|
| Director or officer | Those charged with the governance of an entity, or acting in an equivalent capacity, regardless of their title, which may vary from jurisdiction to jurisdiction. |
| Engagement partner | The partner or other person in the firm who is responsible for the engagement and its performance, and for the report that is issued on behalf of the firm, and who, where required, has the appropriate authority from a professional, legal or regulatory body. |
| Engagement quality control review | A process designed to provide an objective evaluation, on or before the report is issued, of the significant judgments the engagement team made and the conclusions it reached in formulating the report. |
| Engagement team | All partners and staff performing the engagement, and any individuals engaged by the firm or a network firm who perform assurance procedures on the engagement. This excludes external experts engaged by the firm or by a network firm.<br><br>The term "engagement team" also excludes individuals within the client's internal audit function who provide direct assistance on an audit engagement when the external auditor complies with the requirements of HKSA 610 (Revised 2013), *Using the Work of Internal Auditors.*[*] |
| Existing accountant | A professional accountant in public practice currently holding an audit appointment or carrying out accounting, taxation, consulting or similar professional services for a client. |
| External expert | An individual (who is not a partner or a member of the professional staff, including temporary staff, of the firm or a network firm) or organization possessing skills, knowledge and experience in a field other than accounting or auditing, whose work in that field is used to assist the professional accountant in obtaining sufficient appropriate evidence. |
| Financial interest | An interest in an equity or other security, debenture, loan or other debt instrument of an entity, including rights and obligations to acquire such an interest and derivatives directly related to such interest. |
| Financial statements | A structured representation of historical financial information, including related notes, intended to communicate an entity's economic resources or obligations at a point in time or the changes therein for a period of time in accordance with a financial reporting framework. The related notes ordinarily comprise a summary of significant accounting policies and other explanatory information. The term can relate to a complete set of financial statements, but it can also refer to a single financial statement, for example, a balance sheet, or a statement of revenues and expenses, and related explanatory notes. |

[*] HKSA 610 (Revised 2013) establishes limits on the use of direct assistance. It also acknowledges that the external auditor may be prohibited by law or regulation from obtaining direct assistance from internal auditors. Therefore, the use of direct assistance is restricted to situations where it is permitted.

| | |
|---|---|
| Financial statements on which the firm will express an opinion | In the case of a single entity, the financial statements of that entity. In the case of consolidated financial statements, also referred to as group financial statements, the consolidated financial statements. |
| Firm | (a) A sole practitioner, partnership or corporation of professional accountants;<br>(b) An entity that controls such parties, through ownership, management or other means; and<br>(c) An entity controlled by such parties, through ownership, management or other means. |
| Historical financial information | Information expressed in financial terms in relation to a particular entity, derived primarily from that entity's accounting system, about economic events occurring in past time periods or about economic conditions or circumstances at points in time in the past. |
| Immediate family | A spouse (or equivalent) or dependent. |
| Independence | Independence is:<br>(a) Independence of mind – the state of mind that permits the expression of a conclusion without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity, and exercise objectivity and professional skepticism<br>(b) Independence in appearance – the avoidance of facts and circumstances that are so significant that a reasonable and informed third party would be likely to conclude, weighing all the specific facts and circumstances, that a firm's, or a member of the audit or assurance team's, integrity, objectivity or professional skepticism has been compromised. |
| Indirect financial interest | A financial interest beneficially owned through a collective investment vehicle, estate, trust or other intermediary over which the individual or entity has no control or ability to influence investment decisions. |
| Key audit partner | The engagement partner, the individual responsible for the engagement quality control review, and other audit partners, if any, on the engagement team who make key decisions or judgments on significant matters with respect to the audit of the financial statements on which the firm will express an opinion. Depending upon the circumstances and the role of the individuals on the audit, "other audit partners" may include, for example, audit partners responsible for significant subsidiaries or divisions. |
| Listed entity | An entity whose shares, stock or debt are quoted or listed on a recognized stock exchange, or are marketed under the regulations of a recognized stock exchange or other equivalent body. |

| | |
|---|---|
| Network | A larger structure:<br>(a) That is aimed at co-operation; and<br>(b) That is clearly aimed at profit or cost sharing or shares common ownership, control or management, common quality control policies and procedures, common business strategy, the use of a common brand-name, or a significant part of professional resources. |
| Network firm | A firm or entity that belongs to a network. |
| Office | A distinct sub-group, whether organized on geographical or practice lines. |
| Professional accountant | An individual who is a member of the Hong Kong Institute of Certified Public Accountants. |
| Professional accountant in business | A professional accountant employed or engaged in an executive or non-executive capacity in such areas as commerce, industry, service, the public sector, education, the not for profit sector, regulatory bodies or professional bodies, or a professional accountant contracted by such entities. |
| Professional accountant in public practice | A professional accountant, irrespective of functional classification (e.g., audit, tax or consulting) in a firm that provides professional services. This term is also used to refer to a firm of professional accountants in public practice. |
| Professional activity | An activity requiring accountancy or related skills undertaken by a professional accountant, including accounting, auditing, taxation, management consulting, and financial management. |
| Professional services | Professional activities performed for clients. |
| Public interest entity | (a) A listed entity; and<br>(b) An entity: (i) defined by regulation or legislation as a public interest entity; or (ii) for which the audit is required by regulation or legislation to be conducted in compliance with the same independence requirements that apply to the audit of listed entities. Such regulation may be promulgated by any relevant regulator, including an audit regulator. |
| Related entity | An entity that has any of the following relationships with the client:<br>(a) An entity that has direct or indirect control over the client if the client is material to such entity;<br>(b) An entity with a direct financial interest in the client if that entity has significant influence over the client and the interest in the client is material to such entity; |

(c) An entity over which the client has direct or indirect control;

(d) An entity in which the client, or an entity related to the client under (c) above, has a direct financial interest that gives it significant influence over such entity and the interest is material to the client and its related entity in (c); and

(e) An entity which is under common control with the client (a "sister entity") if the sister entity and the client are both material to the entity that controls both the client and sister entity.

**Review client** — An entity in respect of which a firm conducts a review engagement.

**Review engagement** — An assurance engagement, conducted in accordance with Hong Kong Standards on Review Engagements or equivalent, in which a professional accountant in public practice expresses a conclusion on whether, on the basis of the procedures which do not provide all the evidence that would be required in an audit, anything has come to the accountant's attention that causes the accountant to believe that the financial statements are not prepared, in all material respects, in accordance with an applicable financial reporting framework.

**Review team**

(a) All members of the engagement team for the review engagement; and

(b) All others within a firm who can directly influence the outcome of the review engagement, including:

  (i) Those who recommend the compensation of, or who provide direct supervisory, management or other oversight of the engagement partner in connection with the performance of the review engagement including those at all successively senior levels above the engagement partner through to the individual who is the firm's Senior or Managing Partner (Chief Executive or equivalent);

  (ii) Those who provide consultation regarding technical or industry specific issues, transactions or events for the engagement; and

  (iii) Those who provide quality control for the engagement, including those who perform the engagement quality control review for the engagement; and

(c) All those within a network firm who can directly influence the outcome of the review engagement.

**Special purpose financial statements** — Financial statements prepared in accordance with a financial reporting framework designed to meet the financial information needs of specified users.

**Those charged with governance** — The person(s) or organization(s) (for example, a corporate trustee) with responsibility for overseeing the strategic direction of the entity and obligations related to the accountability of the entity. This includes overseeing the financial reporting process. For some entities in some jurisdictions, those charged with governance may include management personnel, for example, executive members of a governance board of a private or public sector entity, or an owner-manager.

# Effective Date

The Code (Part A to Part D) is effective on 1 January 2011; early adoption is permitted. The Code is subject to the following transitional provisions:

## *Public Interest Entities*

1. Section 290 of the Code contains additional independence provisions when the audit or review client is a public interest entity. The additional provisions that are applicable because of the new definition of a public interest entity or the guidance in paragraph 290.26 are effective on 1 January 2012. For partner rotation requirements, the transitional provisions contained in paragraphs 2 and 3 below apply

## *Partner Rotation*

2. For a partner who is subject to the rotation provisions in paragraph 290.149 because the partner meets the definition of the new term "key audit partner," and the partner is neither the engagement partner nor the individual responsible for the engagement quality control review, the rotation provisions are effective for the audits or reviews of financial statements for years beginning on or after 15 December 2011. For example, in the case of an audit client with a calendar year-end, a key audit partner, who is neither the engagement partner nor the individual responsible for the engagement quality control review, who had served as a key audit partner for seven or more years (i.e., the audits of 2003 – 2010), would be required to rotate after serving for one more year as a key audit partner (i.e., after completing the 2011 audit).

3. For an engagement partner or an individual responsible for the engagement quality control review who immediately prior to assuming either of these roles served in another key audit partner role for the client, and who, at the beginning of the first fiscal year beginning on or after 15 December 2010, had served as the engagement partner or individual responsible for the engagement quality control review for six or fewer years, the rotation provisions are effective for the audits or reviews of financial statements for years beginning on or after 15 December 2011. For example, in the case of an audit client with a calendar year-end, a partner who had served the client in another key audit partner role for four years (i.e., the audits of 2002-2005) and subsequently as the engagement partner for five years (i.e., the audits of 2006-2010) would be required to rotate after serving for one more year as the engagement partner (i.e., after completing the 2011 audit).

## *Non-assurance services*

4. Paragraphs 290.154-290.216 address the provision of non-assurance services to an audit or review client. If, at the effective date of the Code, services are being provided to an audit or review client and the services were permissible under the June 2005 Code (revised July 2006) but are either prohibited or subject to restrictions under the revised Code, the firm may continue providing such services only if they were contracted for and commenced prior to 1 January 2011, and are completed before 1 July 2011.

## *Fees – Relative Size*

5. Paragraph 290.219 provides that, in respect of an audit or review client that is a public interest entity, when the total fees from that client and its related entities (subject to the considerations in paragraph 290.27) for two consecutive years represent more than 15% of the total fees of the firm expressing the opinion on the financial statements, a pre- or post-issuance review (as described in paragraph 290.219) of the second year's audit shall be performed. This requirement is effective for audits or reviews of financial statements covering years that begin on or after 15 December 2010. For example, in the case of an audit client with a calendar year end, if the total fees from the client exceeded the 15% threshold for 2011 and 2012, the pre- or post-issuance review would be applied with respect to the audit of the 2012 financial statements.

### *Compensation and Evaluation Policies*

6. Paragraph 290.226 provides that a key audit partner shall not be evaluated or compensated based on that partner's success in selling non-assurance services to the partner's audit client. This requirement is effective on 1 January 2012. A key audit partner may, however, receive compensation after 1 January 2012 based on an evaluation made prior to 1 January 2012 of that partner's success in selling non-assurance services to the audit client.

# APPENDIX 1

# Sample Code of Conduct under the Prevention of Bribery Ordinance

## Introduction

1. The *(name of company)* (hereafter referred to as the Company) regards honesty, integrity and fair play as our core values that must be upheld by all directors and staff [1] of the Company at all times. This Code sets out the basic standard of conduct expected of all directors and staff, and the Company's policy on acceptance of advantage and handling of conflict of interest when dealing with the Company's business.

## Prevention of Bribery

### *Prevention of Bribery Ordinance*

2. Under the Prevention of Bribery Ordinance (the Ordinance), any director or staff member who, without the permission of his employer or principal (i.e. the Company), solicits or accepts an advantage as a reward or inducement for doing any act or showing favour in relation to the latter's business, commits an offence. The person offering the advantage also commits an offence.

(The relevant provisions of Section 9 of the Ordinance and the definition of "advantage" are detailed at **Annex 1**.)

### *Acceptance of Advantage*

3. It is the Company's policy that directors and staff, in their private capacity, should not solicit or accept an advantage from any person, company or organization having business dealings with the Company, except that they may accept (but not solicit) the following advantages when offered on a voluntary basis:

   (a) advertising or promotional gifts or souvenirs of a nominal value; or

   (b) gifts given on festive or special occasions, subject to a maximum limit of $_____ in value; or

   (c) discounts or other special offers given by any person or company to them as customers, on terms and conditions equally applicable to other customers in general; or

   (d) gifts or souvenirs of nominal value presented to them in official functions.

   No director or staff member should, in his/her private capacity, accept any advantage from a subordinate, except those mentioned in paragraphs (a) and (b) above.

4. Gifts or souvenirs described in paragraph 3(d) above are deemed as offers to the Company. The directors and staff members concerned should report the acceptance to the Company and seek direction as to how to handle the gifts or souvenirs from *the approving authority* [2] using Form A (**Annex 2**). If a director or staff member wishes to accept any advantage not covered in paragraph 3, he/she should also seek permission from *the approving authority* using Form A.

---

1 "Staff" cover full-time, part-time and temporary staff, except where specified.

2 Specify the post of the approving authority in the Code and the Form.

5. However, a director or staff member should decline an offer of advantage if acceptance could affect his/her objectivity in conducting the Company's business or induce him/her to act against the interest of the Company, or acceptance will likely lead to perception or allegation of impropriety.

6. If a director or staff member has to act on behalf of a client in the course of carrying out the Company's business, he/she should also comply with any additional restrictions on acceptance of advantage that may be set by the client.

### *Offer of Advantage*

7. Directors and staff are prohibited from offering advantages to any director or staff of another company or organization, for the purpose of influencing such person or company in any dealings, or any public official, whether directly or indirectly through a third party, when conducting the Company's business.

### *Entertainment*

8. As defined in Section 2 of the Ordinance, "entertainment" refers to food or drink provided for immediate consumption on the occasion, and any other entertainment provided at the same time. Although entertainment is an acceptable form of business and social behaviour, a director or staff member should avoid accepting overly lavish or frequent entertainment from persons with whom the Company has business dealings (e.g. suppliers or contractors) or from his/her subordinates to avoid placing himself/herself in a position of obligation.

### *Records, Accounts and other Documents*

9. Directors and staff should ensure that all records, receipts, accounts or other documents they submit to the Company, give a true representation of the events or business transactions as shown in the documents. Intentional use of documents containing false information to deceive or mislead the Company, regardless of whether there is any gain or advantage involved, may constitute an offence under the Ordinance.

## Compliance with Laws of Hong Kong and in Other Jurisdictions

10. Directors or staff must comply with all local laws and regulations when conducting the Company's business, and also those in other jurisdictions when conducting business there.

## Conflict of Interest

11. Directors and staff should avoid any conflict of interest situation (i.e. situation where their private interest conflicts with the interest of the Company) or the perception of such conflicts. They should not misuse their position or authority in the Company to pursue their own private interests which include both financial or personal interests and those of their family members, relatives or close personal friends. When actual or potential conflict of interest arises, the director or staff member should make a declaration to the management through the reporting channel using Form B (**Annex 3**).

12. Some common examples of conflict of interest are described below but they are by no means exhaustive:

    (a) A staff member involved in a procurement exercise is closely related to or has financial interest in the business of a supplier who is being considered for selection by the Company.

(b) One of the candidates under consideration in a recruitment or promotion exercise is a family member, a relative or a close personal friend of the staff member involved in the process.

(c) A director of the Company has financial interest in a company whose quotation or tender is under consideration by the Board.

(d) A staff member (full-time or part-time) undertaking part-time work with a contractor whom he is responsible for monitoring.

## Use of Company Assets

13. Directors and staff in charge of or having access to any Company assets, including funds, property, information, and intellectual property, should use them solely for the purpose of conducting the Company's business. Unauthorized use, such as misuse for personal gain, is strictly prohibited.

### *Confidentiality of Information*

14. Directors and staff should not disclose any classified information of the Company without authorization or misuse any Company information (e.g. unauthorized sale of the information). Those who have access to or are in control of such information, including information in the Company's computer system, should at all times protect the information from unauthorized disclosure or misuse. Special care should also be taken in the use of any personal data, including directors', staff's and customers' personal data, to ensure compliance with the Personal Data (Privacy) Ordinance (Cap. 486).

## Outside Employment

15. Any full time staff who wish to take up employment outside the Company, must seek the prior written approval of *the approving authority*. The approving authority should consider whether the outside employment would give rise to a conflict of interest with the staff's duties or the interest of the Company.

## Relationship with Suppliers, Contractors and Customers

### *Gambling*

16. Directors and staff are advised not to engage in frequent gambling activities (e.g. mahjong) with persons having business dealings with the Company.

### *Loans*

17. Directors and staff should not accept any loan from, or through the assistance of, any individual or organization having business dealings with the Company. There is however no restriction on borrowing from licensed banks or financial institutions.

[*The Company may wish to include other guidelines on the conduct required of directors and staff in their dealings with suppliers, contractors, customers, and other business partners as appropriate to specific trades.*]

## Compliance with the Code

18. It is the responsibility of every director and staff member of the Company to understand and comply with this Code, whether performing his company duties in or outside Hong Kong. Managers and supervisors should also ensure that the staff under their supervision understand well and comply with this Code.

19. Any director or staff member in breach of this Code will be subject to disciplinary action, including termination of appointment. In cases of suspected corruption a report should be made to the ICAC and other criminal offences, to the appropriate authority.

20. Any enquiries about this Code or reports of possible breaches of this Code should be made to (post of designated senior staff).

_____

(*Name of Company*)

Date:

**Annex 1**

# Extracts of the Prevention of Bribery Ordinance

## Section 9

(1) Any agent who, without lawful authority or reasonable excuse, solicits or accepts any advantage as an inducement to or reward for or otherwise on account of his –

(a) doing or forbearing to do, or having done or forborne to do, any act in relation to his principal's affairs or business; or

(b) showing or forbearing to show, or having shown or forborne to show, favour or disfavour to any person in relation to his principal's affairs or business,

shall be guilty of an offence.

(2) Any person, who, without lawful authority or reasonable excuse, offers any advantage to any agent as an inducement to or reward for or otherwise on account of the agent's –

(a) doing or forbearing to do, or having done or forborne to do, any act in relation to his principal's affairs or business; or

(b) showing or forbearing to show, or having shown or forborne to show, favour or disfavour to any person in relation to his principal's affairs or business,

shall be guilty of an offence.

(3) Any agent who, with intent to deceive his principal, uses any receipt, account or other document –

(a) in respect of which the principal is interested; and

(b) which contains any statement which is false or erroneous or defective in any material particular; and

(c) which to his knowledge is intended to mislead the principal,

shall be guilty of an offence.

(4) If an agent solicits or accepts an advantage with the permission of his principal, being permission which complies with subsection (5), neither he nor the person who offered the advantage shall be guilty of an offence under subsection (1) or (2).

(5) For the purpose of subsection (4) permission shall –

(a) be given before the advantage is offered, solicited or accepted; or

(b) in any case where an advantage has been offered or accepted without prior permission, be applied for and given as soon as reasonably possible after such offer or acceptance,

and for such permission to be effective for the purpose of subsection (4), the principal shall, before giving such permission, have regard to the circumstances in which it is sought.

## Section 2

**'Advantage' means :**

(a) any gift, loan, fee, reward or commission consisting of money or of any valuable security or of other property or interest in property of any description;

(b) any office, employment or contract;

(c) any payment, release, discharge or liquidation of any loan, obligation or other liability, whether in whole or in part;

(d) any other service, or favour (other than entertainment), including protection from any penalty or disability incurred or apprehended or from any action or proceedings of a disciplinary, civil or criminal nature, whether or not already instituted;

(e) the exercise or forbearance from the exercise of any right or any power or duty; and

(f) any offer, undertaking or promise, whether conditional or unconditional, of any advantage within the meaning of any of the preceding paragraphs (a), (b), (c), (d) and (e),

but does not include an election donation within the meaning of the Elections (Corrupt and Illegal Conduct) Ordinance (10 of 2000), particulars of which are included in an election return in accordance with that Ordinance.

**'Entertainment' means :**

The provision of food or drink, for consumption on the occasion when it is provided, and of any other entertainment connected with, or provided at the same time as, such provisions.

## Section 19

In any proceedings for an offence under this Ordinance, it shall not be a defence to show that any such advantage as is mentioned in this Ordinance is customary in any profession, trade, vocation or calling.

**Annex 2**

Form A

# (Company Name)

# REPORT ON GIFTS RECEIVED

## Part A – To be completed by Receiving Staff

To : (Approving Authority)

Description of Offeror *:*

*Name & Title of Offeror :* _____

*Company :* _____

*Relationship (Business / Personal) :* _____

Occasion on which the Gift
was / is to be received : _____

Description & (assessed) value of the Gift :
_____

| *Suggested Method of Disposal :* | | *Remark* |
|---|---|---|
| ( ) | Retain by the Receiving Staff | _____ |
| ( ) | Retain for Display / as a Souvenir in the Office | _____ |
| ( ) | Share among the Office | _____ |
| ( ) | Reserve as Lucky Draw Prize at Staff Function | _____ |
| ( ) | Donate to a Charitable Organization | _____ |
| ( ) | Return to Offeror | _____ |
| ( ) | Others (please specify) : | _____ |

_____
(Name of Receiving Staff)

(Date) (Title)

---

## Part B – To be completed by Approving Authority

To : (Name of Receiving Staff)

The recommended method of disposal is ****approved / not approved***. *The gift(s) concerned should be disposed of by way of :

_____
(Name of Approving Authority)

(Date) (Title)

** Delete as appropriate.*

**Annex 3**

Form B

# (Company Name)

# Declaration of Conflict of Interest

## Part A – Declaration *(To be completed by Declaring Staff)*

To : (Approving Authority) via (supervisor of the Declaring Staff)

I would like to report the following actual/potential* conflict of interest situation arising during the discharge of my official duties:-

| **Persons/companies with whom/which I have official dealings** |
|---|
| |
| **My relationship with the persons/companies (e.g. relative)** |
| |
| **Relationship of the persons/companies with our Company (e.g. supplier)** |
| |
| **Brief description of my duties which involved the persons/companies (e.g. handling of tender exercise)** |
| |

_____

(Name of Declaring Staff)

(Date) (Title / Department)

---

## Part B – Acknowledgement *(To be completed by Approving Authority)*

To : (Declaring Staff) via (supervisor of the Declaring Staff)

**Acknowledgement of Declaration**

The information contained in your declaration form of (Date) is noted. It has been decided that:-

- ❑ You should refrain from performing or getting involved in performing the work, as described in Part A, which may give rise to a conflict.
- ❑ You may continue to handle the work as described in Part A, provided that there is no change in the information declared above, and you must uphold the Company's interest without being influenced by your private interest.
- ❑ Others (please specify) :

_____

(Name of Approving Authority)

(Date) (Title / Department)

** Delete as appropriate.*

# APPENDIX 2

## Comparison with The IESBA Code of Ethics for Professional Accountants

Since 2005, the Institute has adopted the IESBA *Code of Ethics for Professional Accountants* (IESBA Code) as the ethical requirements for its members. Additional guidance has been incorporated to reflect local or legal requirements in Hong Kong. This version of the Code of Ethics for Professional Accountants (Part A to Part C) is based on the IESBA Code.

This comparison appendix deals only with significant differences in the Code of Ethics for Professional Accountants with the IESBA Code, is produced for information only and does not form part of the Code of Ethics for Professional Accountants.

The following sets out the major textual differences between the Code of Ethics for Professional Accountants and the IESBA Code of Ethics for Professional Accountants and the reasons for the differences.

| | **Differences** | **Reasons for the Differences** |
|---|---|---|
| 1. | **Paragraphs 100.10, 100.11, 140.7, 290.41 and 290.49** | The Institute replaced the wording "member body" in the IESBA Code to "the Institute" to adapt for local context. |
| 2. | **Paragraph 240.7A, Footnote 1a and Appendix 1** | The paragraph reflects the legal requirement in Hong Kong and additional guidance on the application of the Prevention of Bribery Ordinance. |
| 3. | **Paragraph 290.25, Footnote 1b** | Additional guidance on the definition of "public interest entity" under the legislation of Hong Kong. |
| 4. | **Paragraph 290.107** of the IESBA Code is modified by deleting or revising certain safeguards. | The Institute takes the view that the threats created in the specified circumstances would be so significant that the safeguards should be tightened or no safeguard could reduce the threat to an acceptable level. |
| 5. | **Paragraph 290.146** of the IESBA Code is modified. | The modification reflects the legal requirement in Hong Kong. |
| 6. | (a) **Part D** on additional ethical requirements is added.<br>(b) **Paragraphs 100.2 and 100.3** of the IESBA Code are modified to refer to Part D. | Part D sets out the additional ethical requirements on specific areas which are primarily derived from local legal or regulatory requirements. |