AML/CFT Requirements for TCSP Licensees

Ms. Marie Leung
Senior Solicitor
20 November 2025

What are Customer Due Diligence (CDD) Measures?

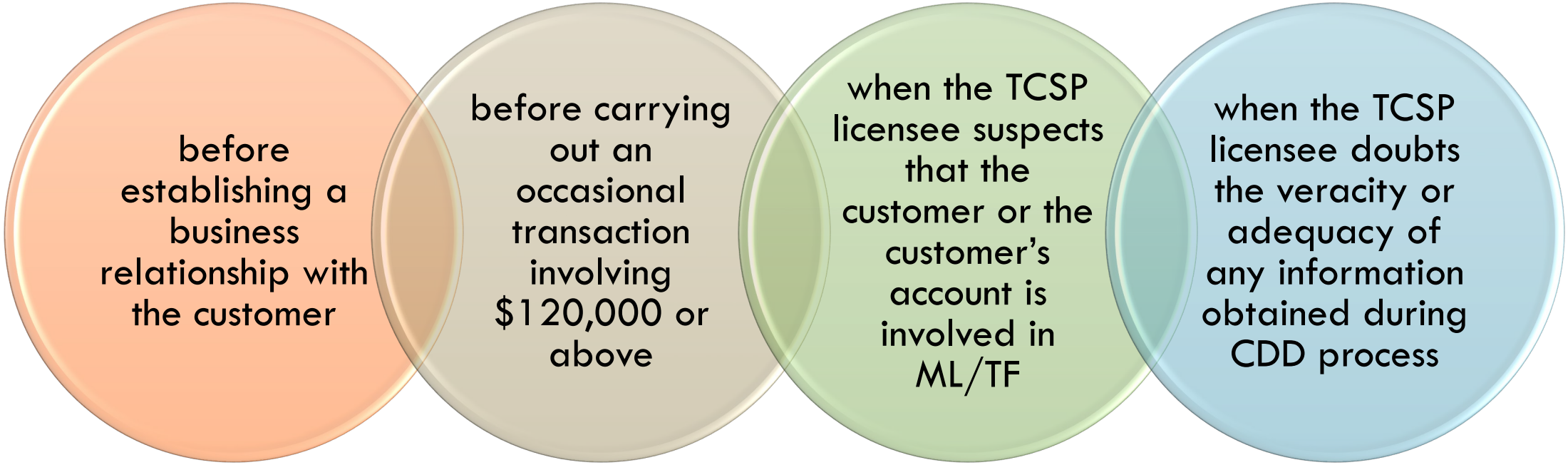
- Chapter 4 of the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism for TCSP Licensees ("AML/CFT Guideline") published in March 2025

- identify the customer and verify the customer's identity
- Identify and take reasonable measures to verify the beneficial owner's identity
- obtain information on the purpose and intended nature of the business relationship (if any) established with the licensee
- If a person purports to act on behalf of the customer, identify and take reasonable measures to verify the person's identity and verify the person's authority to act on behalf of the customer

[para. 4.1.3 of the AML/CFT Guideline]

When to Carry Out CDD Measures?

CDD measures must be carried out:



[para. 4.2.1 of the AML /CFT Guideline]

If the requirements are not complied with, the licensee **SHOULD NOT** establish a business relationship or carry out any occasional transaction with that customer. If a business relationship has been established, it should be terminated as soon as reasonably practicable.

[para. 4.13.1 of the AML /CFT Guideline]

Identification and verification of identity - customer

For identification and verification of a customer that is a:

- **natural person** – *paras. 4.3.2 to 4.3.5 (formerly Appendix A) of the AML /CFT Guideline*
- **legal person** (including a partnership or an unincorporated body) – *paras. 4.3.6 to 4.3.9 (formerly Appendices B & C) of the AML /CFT Guideline*
- **trust** or other similar legal arrangements – *paras. 4.3.10 to 4.3.12 (formerly Appendix D) of the AML /CFT Guideline*

Case Example

Transaction : acting as the company secretary of Company X

- Who is the customer?
- Is the customer a new customer or a pre-existing customer (business relationship established before 1 March 2018)?
- Company X – *paras. 4.3.6 to 4.3.7 of the AML/CFT Guideline*, should ensure documents, data or information obtained are current at the time
- Identify the beneficial owner(s) of Company X and take reasonable measures to verify their identities – *paras. 4.4.2, 4.4.6 & 4.4.9 of the AML/CFT Guideline*
- Understand the ownership and control structure of Company X, including identification of any intermediate layers – *paras. 4.4.14 to 4.4.15 of the AML/CFT Guideline*
- If a person purports to act on behalf of Company X :
  - Identify the person and take reasonable measures to verify the person's identity + verify the authority – *paras. 4.5.1 to 4.5.4 of the AML/CFT Guideline*

Additional Measures or Enhanced Due Diligence ("EDD")

Situations in which additional measures or EDD apply include:

Situations presenting a high ML/TF risk or a situation specified by the Registrar in a notice in writing given to the licensee *[paras. 4.9.1 to 4.9.6 of the AML/CFT Guideline]*

Politically exposed persons ("PEPs") *[paras.4.9.7 to 4.9.27 of the AML/CFT Guideline]*

Customers not physically present for identification purposes *[paras.4.10.1 to 4.10.5 of the AML/CFT Guideline]*

High Money Laundering/ Terrorist Financing ("ML/TF") Risks

A licensee should apply EDD measures in relation to a business relationship or transaction to mitigate and manage the high ML/TF risks in:

(a) a situation that by its nature may present a high ML/TF risk taking into account the potentially higher risk factors set out *in para. 4.9.5 of the AML/CFT Guideline* (see next slide); or

(b) a situation specified by the Registrar in a notice in writing given to the licensee.

[para. 4.9.1 of the AML/CFT Guideline]

Examples of Potentially Higher Risk Factors:

(a) **customer** risk factor:

(i) business relationship is conducted in unusual circumstances;
(ii) legal persons or legal arrangements that involve a shell vehicle without a clear and legitimate commercial purpose;
(iii) companies that have nominee shareholders/ directors, bearer shares or bearer share warrants;
(iv) cash intensive business; or
(v) the ownership structure of the legal person or legal arrangement appears unusual or excessively complex

(b) **product, service, transaction or delivery channel** risk factors:

(i) anonymous transactions (which may involve cash); or
(ii) frequent payments received from unknown or unassociated third parties

(c) **country** risk factors:

(i) countries or jurisdictions not having effective AML/CFT Systems;
(ii) countries or jurisdictions having a significant level of corruption or other criminal activity;
(iii) countries or jurisdictions subject to sanctions, embargoes or similar measures issued by, for example, the United Nations; or
(iv) countries, jurisdictions or geographical areas providing funding or support for terrorist activities, or that have designated terrorist organisations operation

[para. 4.9.5 of the AML/CFT Guideline]

Examples of EDD Measures

(a) obtaining additional information on the customer and updating more regularly the identification data of customer and beneficial owner

(b) obtaining additional information on the intended nature of the business relationship

(c) obtaining information on the source of wealth of the customer

(d) obtaining information on the source of funds of the customer

(e) obtaining information on the reasons for intended or performed transactions

(f) requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards

[para. 4.9.6 of the AML/CFT Guideline]

EDD Measures for PEPs

Definitions of different types of PEPs in the AML/CFT Guideline

(a) A non-Hong Kong PEP *[para. 4.9.7 of the AML/CFT Guideline]*
(b) A former non-Hong Kong PEP *[para. 4.9.12 of the AML/CFT Guideline]*
(c) A Hong Kong PEP *[para. 4.9.14 of the AML/CFT Guideline]*
(d) An international organization PEP *[para. 4.9.15 of the AML/CFT Guideline]*

EDD Measures for non-Hong Kong PEPs

[paras. 4.9.10 & 4.9.11 of the AML/CFT Guideline]

EDD Measures for Hong Kong PEPs and international organization PEPs

[para. 4.9.18 of the AML/CFT Guideline]

EDD Measures for former non-Hong Kong PEPs

[para. 4.9.13 of the AML/CFT Guideline]

EDD Measures for former Hong Kong PEPs and former international organization PEPs

[para. 4.9.19 of the AML/CFT Guideline]

Non-Hong Kong PEPs

Under Section 1 of Part 1 of Schedule 2 to the AMLO, ***politically exposed person*** means—

(a) an individual who is or has been entrusted with a prominent public function in a place outside Hong Kong and—

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

  (ii) 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), 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).

Former Non-Hong Kong PEPs

Under Section 1 of Part 1 of Schedule 2 to the AMLO, ***former politically exposed person*** means—

(a) an individual who, being a politically exposed person, has been but is not currently entrusted with a prominent public function in a place outside Hong Kong;

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

Treatment of Former PEPs

- Risk-based approach

- Licensee may **decide NOT TO** apply / continue to apply the **EDD measures** *(*para. 4.9.10 of the AML/CFT Guideline) **and enhanced monitoring measures** (para. 4.9.11 of the AML/CFT Guideline) to a customer who is / whose beneficial owner is

  - (i) **a former PEP**; and

  - (ii) the former PEP **does not present a high risk of ML/TF** based on appropriate assessment

[paras. 4.9.13 & 4.9.19 of the AML/CFT Guideline]

Additional Measures:
Customer not physically present for identification purposes

At least ONE of the following additional measures should be carried out :

- further verifying the customer's identity on the basis of documents, data or information referred to in para. 4.3.1 of the AML/CFT Guideline but not previously used for the purposes of verification of the customer's identity;

- taking supplementary measures to verify information relating to the customer that has been obtained by the licensee; or
- ensuring that the payment or, if there is more than one payment, the first payment made in relation to the customer's account is carried out through an account opened in the customer's name with an authorized institution, or an institution that
  - (i) is incorporated or established in an equivalent jurisdiction;
  - (ii) carries on a business similar to that carried on by an authorized institution;
  - (iii) has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2 to the AMLO; and
  - (iv) is supervised for compliance with those requirements by authorities in that jurisdiction that perform functions similar to those of the Hong Kong Monetary Authority.

[para. 4.10.1 of the AML/CFT Guideline]

Recognized Digital Identification System

Under Section 1 of Part 1 of Schedule 2 to the AMLO, ***recognized digital identification system*** means—

in relation to a financial institution or a DNFBP who is a TCSP licensee or a Category B PMS registrant, a digital identification system that is a reliable and independent source that is recognized by the relevant authority

FAQ on DIS : The Registrar recognizes iAM Smart, developed and operated by the HKSAR Government, as a digital identification system that can be used for identity verification of natural persons.

If a licensee has verified the identity of the customer on the basis of data or information provided by a digital identification system that is a reliable and independent source that is recognised by the Registrar (see para.4.3.1 of the AML/CFT Guideline), the licensee is not required to carry out the additional measures that are required for customers not physically present

[para. 4.10.2 of the AML/CFT Guideline]

Carry Out CDD Measures by means of Intermediaries

A licensee may rely upon an intermediary to perform any part of the CDD measures. **HOWEVER**, the ultimate responsibility for ensuring that CDD requirements are met remains with the licensee.

[para. 4.11.1 of the AML/CFT Guideline]

When relying on an intermediary, a licensee should :

(a) obtain **written confirmation** from the intermediary that the intermediary agrees to act as the licensee's intermediary and perform which part of the CDD measures specified in section 2 of Schedule 2 to the AMLO; and

(b) be satisfied that the intermediary will on request **provide a copy of any document, or a record of any data or information, obtained** by the intermediary in the course of carrying out the CDD measures without delay.

[para. 4.11.3 of the AML/CFT Guideline]

Carry Out CDD Measures by means of Intermediaries

Intermediaries in Hong Kong

A. Financial Institutions

- an authorized institution
- a licensed corporation
- an authorized insurer
- a licensed individual insurance agent
- a licensed insurance agency
- a licensed insurance broker company

B. Professional Intermediaries

(provided that such intermediaries satisfy the licensee that they have adequate procedures in place to prevent ML/TF and are required to comply with the requirements set out in Schedule 2 to the AMLO with respect to customers)

- an accounting professional
- an estate agent
- a legal professional
- a TCSP licensee

[para. 4.11.8 of the AML/CFT Guideline]

Ongoing Due Diligence Requirements

- Chapter 5 of the AML/CFT Guideline

A licensee should continuously monitor the business relationship with a customer in two aspects:

Ongoing CDD:

Reviewing from time to time documents, data and information relating to the customer obtained for the purpose of complying with Part 2 of Schedule 2 to ensure they are up-to-date and relevant;

Transaction monitoring:

(i) Scrutinizing the transactions of the customer to ensure that they are consistent with the licensee's knowledge of the customer and its business, risk profile and source of funds; and

(ii) Identifying transactions that are complex, unusually large or of an unusual pattern and have no apparent economic or lawful purpose, and examining the background and purposes of those transactions and setting out its findings in writing.

[para. 5.1 of the AML/CFT Guideline]

Ongoing CDD

Licensee should:

- Undertake reviews of existing CDD records of customers on a regular basis and/or upon trigger events

- Develop clear policies and procedures, especially on the frequency of periodic review or what constitutes a trigger event

High ML/TF risk customers should be subject to a minimum of an annual review, or more frequent reviews if deemed necessary, to ensure the CDD information retained remains up-to-date and relevant

[paras. 5.2 to 5.3 of the AML/CFT Guideline]

Transaction Monitoring

Licensees should:

- establish and maintain adequate systems and processes to monitor transactions

  [para.5.4 of the AML/CFT Guideline]

- regularly review the adequacy and effectiveness of their transaction monitoring systems and processes

  [para.5.8 of the AML/CFT Guideline]

- conduct transaction monitoring following the risk-based approach - the extent of monitoring should be commensurate with the ML/TF risk profile of a customer

  [para. 5.9 of the AML/CFT Guideline]

- properly document the findings and outcomes of steps taken, as well as the rationale of any decision made after taking these steps in writing and make them available to the Registrar, other competent authorities and auditors

  [para. 5.14 of the AML/CFT Guideline]

Record-keeping

➢ Chapter 8 of the AML/CFT Guideline

	Each Customer	Each transaction
What records should be kept?	(i) The original or a copy of documents and a record of the data and information obtained: • in the course of **identifying and verifying** the identity of the customer/ beneficial owner of the customer / beneficiary / persons who purport to act for the customer / other connected parties; • throughout the CDD and **ongoing monitoring process**; and • on the **purpose and intended nature** of the business relationship (ii) The original or a copy of records and documents relating to the customer's **account and business correspondence** with the customer and any beneficial owner of the customer (iii) The results of any analysis undertaken *[para. 8.3 of the AML/CFT Guideline]*	The original or a copy of the documents, and a record of the data and information obtained in connection with each transaction the licensee carries out which should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity *[para. 8.5 of the AML/CFT Guideline]*

Record-keeping

	Each Customer	Each transaction
For how long should records be kept?	Throughout the continuance of the business relationship with the customer and for a period of **at least 5 years** after the end of the business relationship. For occasional transaction involving an amount ≥ HK$120,000, **at least 5 years** beginning on the date on which the occasional transaction is completed. *[para. 8.4 of the AML/CFT Guideline]*	**At least 5 years** after the completion of a transaction regardless of whether the business relationship ends during the period. *[para. 8.6 of the AML/CFT Guideline]*

Counter-Financing of Terrorism

- **The United Nations (Anti-Terrorism Measures) Ordinance, Cap. 575 ("UNATMO")** criminalizes the provision or collection of property and making any property or financial (or related) services available to terrorists or terrorist associates.

- TCSP licensees are reminded not to have any business relationship with any sanctioned individuals or entities, or any terrorist or terrorist associate as defined under the UNATMO.

UNATMO

(a) section 6 empowers the Secretary for Security to freeze suspected terrorist property
(b) section 7 prohibits the provision or collection of property for use to commit terrorist acts
(c) section 8 prohibits any person from making available or collecting or soliciting property or financial (or related) services for terrorists and terrorist associates
(d) section 8A prohibits any person from dealing with any property knowing that, or being reckless as to whether, the property is specified terrorist property or property of a specified terrorist or terrorist associate
(e) section 11L prohibits any person from providing or collecting any property, with the intention or knowing that the property will be used, to finance the travel of a person between states for a specified purpose (i.e. the perpetration, planning or preparation of, or participation in, one or more terrorist acts (even if no terrorist act actually occurs); or the provision or receiving of training that is in connection with the perpetration, planning or preparation of, or participation in, one or more terrorist acts (even if no terrorist act actually occurs as a result of the training))

[para. 6.5 of the AML/CFT Guideline]

Financial Sanctions

It is an offence under the relevant Regulations of the **United Nations Sanctions Ordinance, Cap. 537** for any person

(a) to make available, directly or indirectly, any funds or other financial assets or economic resources to, or for the benefit of,
   (i) designated persons or entities,
   (ii) persons or entities acting on behalf or at the direction of the designated persons or entities mentioned in (i), or
   (iii) entities owned or controlled by any persons or entities mentioned in (i) or (ii); or

(b) to deal with, directly or indirectly, any funds or other financial assets or economic resources belonging to, or owned or controlled by, such persons and entities falling within paragraph (a) above.

[para. 6.7 of the AML/CFT Guideline]

Counter-Financing of Proliferation of Weapons of Mass Destruction ("PF")

United Nations Sanctions (Democratic People's Republic of Korea) Regulation, Cap. 537AE

Section 4 of **the Weapons of Mass Destruction (Control of Provision of Services) Ordinance, Cap. 526** prohibits a person from providing any services where he/she believes or suspects, on reasonable grounds, that those services may be connected to weapon of mass destruction.

[para.6.10 of the AML/CFT Guideline]

Database Maintenance & Screening

Licensees should establish and maintain effective policies, procedures and controls to ensure compliance with the relevant regulations and legislation on TF, financial sanctions and PF.

[para. 6.12 of the AML/CFT Guideline]

Licensees should:

- identify terrorist suspects and possible designated parties, and detect prohibited transactions

- maintain a database of names and particulars of terrorists and designated parties, which consolidates the various lists that have been made known to the licensee

- alternatively, subscribe to such a database maintained by a third party service provider and take appropriate measures (e.g. conduct sample testing periodically) to ensure the completeness and accuracy of the database

[para. 6.13 of the AML/CFT Guideline]

Database Maintenance & Screening

Licensees should include in the database:

(i) the lists published in the Gazette or on the website of the Commerce and Economic Development Bureau; and

(ii) the lists that the Registrar draws to the attention of TCSP licensees from time to time

[para. 6.15 of the AML/CFT Guideline]

Database Maintenance & Screening

TCSP licensees should implement an effective screening mechanism, which should include:

(a) screening its customers and any beneficial owners of the customers against current database at the establishment of the relationship; and

(b) screening its customers and any beneficial owners of the customers against all new and any updated designations to the database as soon as practicable

The screening requirements should extend to connected parties and persons purporting to act on behalf of a customer using a risk-based approach

[paras. 6.16 & 6.17 of the AML/CFT Guideline]

Reporting Suspicious Transactions

Drug Trafficking (Recovery of Proceeds) Ordinance, Cap. 405

Organized and Serious Crimes Ordinance, Cap. 455

United Nations (Anti-Terrorism Measures) Ordinance, Cap. 575

- Chapter 7 of the AML/CFT Guideline
- In cases of suspicions of ML, TF, PF or sanctions violations, a suspicious transaction report ("STR") should be made to the Joint Financial Intelligence Unit ("JFIU")
- TCSP licensees must establish and maintain a record of all ML/TF reports made to the money laundering reporting officer and all STRs made to the JFIU

[paras. 7.29 to 7.30 of the AML/CFT Guideline]

The End