The Hong Kong Association of Banks

Frequently Asked Questions in relation to Anti-Money Laundering and Counter-Financing of Terrorism

These Frequently Asked Questions (**FAQs**) in relation to Anti-Money Laundering and Counter-Financing of Terrorism (**AML/CFT**) have been developed by the Hong Kong Association of Banks (**HKAB**) with input from the Hong Kong Monetary Authority (**HKMA**). This document does not form part of the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Authorized Institutions) (**AML/CFT Guideline**) and it is designed to be read in conjunction with the AML/CFT Guideline. Terms and acronyms used in this document have the same meanings as in the glossary to the AML/CFT Guideline.

These FAQs aim to assist Authorized Institutions (**AIs**) regulated by the HKMA in understanding relevant AML/CFT requirements. AIs are expected to be fully conversant with these FAQs, and to have regard to them in meeting their AML/CFT legal and regulatory obligations. These FAQs are, however, by their nature framed as general statements and do not take into account the particular circumstances of an AI. AIs should therefore consider the money laundering and terrorist financing risks to which they are exposed and their own circumstances (among others) before taking action on matters to which these FAQs may be relevant. These FAQs should not be regarded as a substitute for obtaining legal or other professional advice on AML/CFT requirements.

This document will be kept under review and updated from time to time as necessary.

Note: This new set of FAQs will supersede the version issued 5 October 2022.

	Relevant provisions	Question	Answer
AML/CFT Systems			
1.	Paragraph 2.9 of the AML/CFT Guideline	**Trigger events for an updated IRA** What is regarded as a "trigger event" for the purpose of determining when an AI should undertake a review of its institutional ML/TF risk assessment?	An AI should conduct its institutional ML/TF risk assessment every two years and when material trigger events occur. Non-exhaustive examples of such trigger events may include when: (a) there is a significant breach of the AI's AML/CFT Systems detected; or (b) one of the following has occurred and the AI has assessed that it will materially impact upon its assessment of the institutional ML/TF risks to which it is exposed: (i) the AI acquires a new customer segment or delivery channel; (ii) the AI launches new products or services; or (iii) there is a significant change of operational processes (eg use of new technology).
2.	Paragraphs 3.2 and 3.3 the AML/CFT Guideline	**Simplified and enhanced AML/CFT Systems** Paragraphs 3.2 and 3.3 of the AML/CFT Guideline state that AML/CFT Systems can be simplified or enhanced, what does this mean?	These two paragraphs refer to enhancing or simplifying the AML/CFT policies, procedures and controls (ie AML/CFT Systems), as distinct from EDD or SDD measures articulated in Chapter 4. They set out the basis for an AI to adopt a risk-based approach in its overall AML/CFT Systems across the institution. The application of these two paragraphs should be based on the AI's institutional ML/TF risk assessment. Depending on how the AI assesses its ML/TF risks, a risk-based approach can be applied on a specific customer segment, a specific line of business, or a specific product or service offered. For example, subject to other criteria set out in paragraphs 3.2 and 3.3, a line of business assessed to have lower ML/TF risks may be subject to less frequent internal audit reviews, less frequent/onerous reporting requirements to senior management, or have simpler AML/CFT procedures etc.
3.	Paragraph 5.8 of the AML/CFT Guideline	**Independent validation** Who can independently validate an AI's transaction monitoring systems and processes?	Such validation can be performed by an external party or the internal audit function of the AI (see paragraph 3.11 of the AML/CFT Guideline).

	Relevant provisions	Question	Answer
Identification and verification of identity – natural persons			
4.	Paragraph 4.3.3 of the AML/CFT Guideline	**Hong Kong residents** What documents would be regarded as "*reliable and independent*" for verifying the identity information of a natural person customer who is a Hong Kong resident?	The following are examples of documents that would be considered to be reliable and independent for Hong Kong residents (both permanent and non-permanent residents). **Hong Kong residents aged 12 or above:** Hong Kong identity card **Children under 12 born in Hong Kong:** the child's Hong Kong identity card, birth certificate or valid travel document. In such circumstance an AI should generally regard the minor's parent or guardian as a person acting on behalf of the child and conduct the relevant CDD measures.
5.	Paragraph 4.3.3 of the AML/CFT Guideline	**Non-Hong Kong residents** What documents would be regarded as "*reliable and independent*" for verifying the identity information of a natural person customer who is not a Hong Kong resident?	The following are examples of documents that would be considered to be reliable and independent for non-Hong Kong residents: (a) a valid travel document; (b) a national (ie Government or State-issued) identity card bearing the photograph of the natural person; or (c) a valid national (ie Government or State-issued) driving licence incorporating photographic evidence of the identity of the natural person.
6.	Paragraph 4.3.3 of the AML/CFT Guideline	**Travel documents** What are acceptable "*travel documents*" for the purpose of paragraph 4.3.3?	The following documents are examples of travel documents for the purpose of identity verification: (a) Passport (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 (g) Exit-entry Permit for Travelling to and from Hong Kong and Macau

	Relevant provisions	Question	Answer
7.	Paragraph 4.3.3 of the AML/CFT Guideline	**Travel documents** What part of the "*travel documents*" should be kept on file?	An AI should retain a copy of the "biodata" page of the travel documents, containing the bearer's photograph and biographical details, for the purpose of the record-keeping requirements in the AMLO and the AML/CFT Guideline.
8.	Paragraphs 4.3.3 and 4.5.3 of the AML/CFT Guideline	**British National (Overseas) passport (BN(O))** Can an AI use (BN(O)) passport for identity verification?	Reference should be made to the announcement made by the HKSAR Government dated 29 January 2021 (https://www.info.gov.hk/gia/general/202101/29/P2021012900763.htm) that BN(O) passport would not be recognised as a valid travel document and any form of proof of identity in Hong Kong with effect from 31 January 2021.
9.	Paragraph 4.3.4 of the AML/CFT Guideline	**Documents that do not have photographs** Can an AI verify the identity of a natural person customer on the basis of a document that does not contain a photograph?	This is acceptable only in exceptional circumstances where the customer's associated ML/TF risk has been addressed and mitigated. Exceptional circumstances include where the customer is an asylum seeker who does not have proper identification documents with photographs but has a recognizance form issued by the Hong Kong Immigration Department. If exceptional circumstances apply, an AI may validate a customer's identity with reference to a government-issued document (without a photograph). In such circumstances, additional measures (eg setting appropriate limits to the account; limiting the product and services provided; or conducting enhanced monitoring etc) should be taken to mitigate increased risk.
10.	Paragraph 4.3.2 of the AML/CFT Guideline	**Change of name of a natural person customer** If a natural person customer's name has changed, what measures should be taken by an AI?	If a natural person customer changes their name, an AI should verify the new name by reference to documents, data or information provided by a reliable and independent source following paragraph 4.3.3 of the AML/CFT Guideline. To mitigate the risk of impersonation, the AI should corroborate other identification information (eg date of birth, Hong Kong Identity Card number) on the new identification documents against its existing records. In case of doubt, the AI may request a copy of applicable documentation regarding the name change (eg marriage certificate or deed poll). For the avoidance of doubt, if a customer's name has changed before the establishment of a business relationship, only the current name is required to be identified and verified.

	Relevant provisions	Question	Answer
Identification and verification of identity – natural persons (using iAM Smart)[1]			
11.	Paragraphs 4.3.1 and 4.3.3 of the AML/CFT Guideline	**iAM Smart for identity verification** Can an AI verify the identity of a natural person using iAM Smart?	Yes, the HKMA recognises iAM Smart, developed and operated by the Hong Kong Government, as a digital identification system that can be used for identity verification of natural persons.
12.	Paragraphs 4.1.3 and 4.3.1 of the AML/CFT Guideline	**iAM Smart for remote on-boarding** How can iAM Smart facilitate the remote on-boarding of individual customers?	As stated in the preceding FAQ, iAM Smart can be used as an alternative to the physical identification document used for the purpose of meeting the customer identification and verification requirements in the context of remote on-boarding. However, iAM Smart by itself cannot generally help AIs in meeting the broader CDD requirements that go beyond customer identification and verification. When designing their remote on-boarding model, AIs should have regard to the latest features of iAM Smart to determine how their own CDD or customer on-boarding policies and procedures can be met. This may necessitate the collection of additional documents or other information where it is considered necessary for the purpose of CDD, ongoing monitoring or other compliance and risk management.
13.	Paragraph 4.3.4 of the AML/CFT Guideline	**Additional identity document that contains a photograph** When iAM Smart is used for identity verification, do AIs need to obtain additional identification documents that contain a photograph to verify the identity of a natural person?	To satisfy customer identification and verification requirements under the AMLO, where iAM Smart is used, there is no additional requirement to obtain other identification documents or separately obtain a photograph of the natural person customer. For the avoidance of doubt, paragraph 4.3.4 requires the identity document obtained by an AI to contain a photograph of the customer to mitigate impersonation risks. In the context of iAM Smart, impersonation risks are mitigated by the access controls of the iAM Smart mobile application (e.g. biometric authentication to log in iAM Smart).
14.	Paragraph 8.3 of the AML/CFT Guideline	**Retention of records** When iAM Smart is used for identity verification, what kind of records relating to CDD	Paragraph 8.3 requires AIs to keep 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 the customer. When iAM Smart is used for identifying and verifying the identity of the customer, relevant data and information should be kept. This may include all the specific data or information obtained from iAM Smart through API, showing the

[1] The FAQs under this section are to assist AIs in understanding how iAM Smart can be used in complying with the relevant AML/CFT requirements. AIs should have regard to the latest features and key components of iAM Smart, which can change over time, as well as their own AML/CFT policies and procedures, before using iAM Smart.

	Relevant provisions	Question	Answer
		should AIs retain?	customer's iAM Smart authentication result and verified Hong Kong Identity Card data. The objective is to permit reconstruction of the customer's identity. For the avoidance of doubt, AIs do not need to obtain additional identification documents solely for record keeping purposes.
Identification and verification of identity – legal persons			
15.	Paragraph 4.3.6 of the AML/CFT Guideline	**Non-Hong Kong company registered in Hong Kong** What minimum identification information should be obtained for a non-Hong Kong company registered in Hong Kong under the Companies Ordinance?	For a non-Hong Kong company registered in Hong Kong under section 776 of the Companies Ordinance[2], taking into account the registration made in Hong Kong, an AI should obtain at least the following identification information for the purpose of fulfilling paragraph 4.3.6 of the AML/CFT Guideline: (a) Full name (b) Date of incorporation, establishment or registration (c) Place of incorporation, establishment or registration (d) Address of the registered office (or its equivalent) in the place of incorporation (e) Unique identification number and document type in the place of incorporation or company registration (f) Address of principal place of business in Hong Kong
16.	Paragraph 4.3.6 of the AML/CFT Guideline	**Principal place of business** What is the "*principal place of business*" of a legal person?	The "principal place of business" means the location where a legal person primarily operates or the place of its main activities. It can be the same as, or differ from, the address of registered office. Legal persons, depending on their business nature, may operate in various locations of different natures. If the address of the principal place of business of a legal person is not in in line with the AI's understanding of the legal person's business nature or customer profile, an AI should seek to understand the rationale for why that address is provided to the AI.
17.	Paragraph 4.3.6 of the AML/CFT Guideline	**Address of registered office** Are AIs required to ask the customer to provide "*address of registered office*" information?	Paragraph 4.3.6 requires AIs to obtain the address of registered office of a legal person. As this address is usually included in the document provided by a reliable and independent source (eg certificate of incumbency) being obtained for verification of the legal person's identity, an AI may, instead of asking the customer to provide the information on address of registered office, just copy the address from the document obtained.

[2] Under section 776 of the Companies Ordinance, a non-Hong Kong company is required to register as a registered non-Hong Kong company within one month after the establishment of the place of business in Hong Kong

	Relevant provisions	Question	Answer
18.	Paragraph 4.3.7 of the AML/CFT Guideline	**Business registration** When should a record of business registration be obtained for the purpose of verifying the identity of a legal person?	A record of business registration, which is a type of "record of registration" as stated in paragraph 4.3.7 of the AML/CFT Guideline, is usually regarded as the primary document to verify the identity of a legal person customer that is not required to register with the Hong Kong Companies Registry or similar authority, such as a sole proprietorship, partnership or a unincorporated body etc. It is worth noting that AIs are not required to obtain a record of business registration for every customer that is a legal person. For instance, for a Hong Kong incorporated company, an AI can generally rely on the company record filed at the Hong Kong Companies Registry to verify the identity of the customer without the need to obtain its record of business registration.
19.	Paragraphs 4.3.7 and 4.3.8 of the AML/CFT Guideline	**Partnership details** What documents need to be obtained to verify the identity of a partnership?	The identity of a partnership can be verified by a record of registration or a partnership agreement or deed (which may be an extract or redacted version for customers / circumstances that are not deemed to present a high ML/TF risk). However, if a record of registration is obtained, an additional document may be required to understand the powers that regulate and bind the partnership, which may not be covered by that record itself. If the customer (ie the partnership) is a well-known, reputable organisation with a long history in its industry and there is substantial public information about the customer, its partners and controllers, then confirmation of the customer's membership of a professional or trade industry is likely to be sufficient to verify the identity of the customer.
20.	Paragraphs 4.3.6 to 4.3.9 of the AML/CFT Guideline	**Start-ups and SMEs** Are there any specific CDD requirements for start-ups and small and medium-sized enterprises?	Similar to AML/CFT requirements in other jurisdictions, the requirements in the AML/CFT Guideline are principle-based in order to provide flexibility to AIs to apply them to different types of customer. There are no specific requirements for, or mention of, start-ups or small and medium-sized enterprises. However, AIs should not adopt a one-size-fit-all approach in the application of CDD requirements. AIs should ensure that the design and implementation of their CDD requirements reflect both the operation and profile of these legal persons, the risk level as assessed by the AI concerned and any other relevant considerations.
21.	Paragraph 4.6.1 of the AML/CFT Guideline	**Non-Hong Kong customers** Are there additional CDD requirements (eg understanding the rationale to establish a business relationship in Hong Kong) for a company which is incorporated outside Hong Kong or has non-resident	Obtaining information to understand the purpose and intended nature of the business relationship being established, including the reason for establishing the relationship, is a standard CDD measure applicable to all types of customers and cascades from international standards with which Hong Kong is required to apply. In some cases, the purpose and intended nature will be obvious or self-evident and therefore may not need to be provided by the customer, having regard to the types of accounts to be established or services/products to be used. Applications for account opening should not be rejected merely because the customer is incorporated or established offshore, or because the beneficial owners or directors of a corporate customer are non-residents. AIs' on-boarding procedures should recognise that offshore establishment and non-resident directors, etc are common profiles for many corporates seeking banking services in an international financial centre, like Hong

	Relevant provisions	Question	Answer
		directors/beneficial owners?	Kong. Similarly, in addition to collecting the information, AIs should view residence of beneficial owners or directors as only one part of the CDD and risk profiling exercise, and understand the rationale why a particular type of business relationship is sought, taking into account the customer's business model or mode of operation.
Beneficial owners			
22.	Paragraphs 4.4.2 of the AML/CFT Guideline	**Identification information** As far as possible, AIs should endeavour to obtain the name, date of birth, nationality and unique identification number (and document type) of a beneficial owner. What is meant by "*as far as possible*"?	AIs should generally obtain the name, date of birth, nationality and unique identification number (and document type) of a beneficial owner. However, there may be situations where not all the identification information of a beneficial owner can be obtained by the AI (eg only year of birth, not the date of birth, can be obtained). Given the legal and regulatory requirement is for the AI to be satisfied that it knows who the beneficial owner is, if the AI cannot obtain all the identification information of a beneficial owner, it should assess whether the information obtained is sufficient to identify the beneficial owner, and where necessary, consider whether additional steps are required to ensure it is satisfied that it knows who the beneficial owner is.
23.	Paragraph 4.4.6 of the AML/CFT Guideline	**Definition of beneficial owner** Who should be considered as an individual who "*exercises ultimate control over the management of the corporation*"?	The following are some examples of natural persons who could be considered as beneficial owners on the basis that they exercise ultimate control[3] over the management of the corporation: (a) A natural person who exerts control of a legal person through means such as personal connections to persons who would be beneficial owners due to owning more than 25% of the shares or voting rights. (b) A natural person who exerts control without ownership by participating in the financing of the enterprise, or because of close and intimate family relationships, historical or contractual associations, or if a company defaults on certain payments. Furthermore, control may be presumed even if control is never actually exercised, such as using, enjoying or benefiting from the assets owned by the legal person. There is no requirement to actively identify a person exercising ultimate control over a customer where nothing obtained during the CDD process suggests that such a person exists.

[3] As described in the third limb of the definition of an individual who is defined as a beneficial owner in relation to a corporation in paragraph 4.4.6(a) of the AML/CFT Guideline.

	Relevant provisions	Question	Answer
24.	Paragraph 4.4.9 of the AML/CFT Guideline	**Senior managing official** Who is to be regarded as having a "*position of senior managing official*" for the purpose of paragraph 4.4.9?	Examples of positions of senior managing officials of legal persons include chief executive officer, chief financial officer, managing or executive director, president, or natural person(s) who has significant authority over a legal person's financial relationships, the ability to establish material business relationships (including with FIs that hold accounts on behalf of a legal person) and the ongoing financial affairs of the legal person. When there is no natural person who is a "beneficial owner" as defined in the AMLO, AIs should identify the relevant natural persons who hold the position of senior managing official, and take reasonable measures to verify their identities. AIs can rely on the information provided by the customer to identify who holds these positions.
25.	Paragraph 4.4.3 and footnote 29 of the AML/CFT Guideline	**Register of beneficial owners** Can an AI rely on a register of beneficial owners for identification purposes?	This will depend on the jurisdiction involved, the AI's assessment of ML/TF risk related to the jurisdiction (including with reference to FATF evaluations) and the definition of beneficial owner under the laws of the jurisdiction. Note that if the definition of beneficial owners in that jurisdiction differs from the AMLO and the AML/CFT Guideline (eg different threshold is adopted), the Hong Kong standard applies in relation to all business relationships established or maintained by the AI concerned.
26.	Paragraphs 4.5 and 4.10.5 of the AML/CFT Guideline	**Presence of directors or beneficial owners at account opening** Is there a requirement that directors and beneficial owners of a legal person be present at account opening?	The presence of two or more, or all, directors or beneficial owners at the time of account opening is not required by the HKMA. Generally, a corporate account is opened in the name of a legal person by a natural person who is authorised to act on behalf of that legal person to establish business relationship with an AI. The basic requirement is for an AI to identify and verify the identity of that natural person as well as obtaining the written authority to verify that the natural person has the authorisation of the legal person to establish a business relationship with the AI concerned. For the avoidance of doubt, if such natural person is not physically present for identification purposes, the AI should mitigate any increased risk in accordance with paragraph 4.10.5 of the AML/CFT Guideline.

	Relevant provisions	Question	Answer
27.	Footnote 56 of the AML/CFT Guideline	**New legal entity customer where the beneficial owner is already known** Where a new-to bank-legal person customer is to be onboarded, and the beneficial owner is already known to the bank (and has been subject to identification and verification processes previously) does the beneficial owner have to provide updated ID for the purposes of on-boarding the new legal person customer?	If the identity of a beneficial owner of a new-to-bank legal person customer has previously been verified by an AI (eg the beneficial owner is the AI's existing customer; or the beneficial owner is a beneficial owner of the AI's existing customer), AIs do not generally need to re-verify their identities unless doubts arise as to the veracity or adequacy of the information previously obtained - for example, if it is no longer current.
Ownership and control structure			
28.	Paragraph 4.4.14 of the AML/CFT Guideline	**Ownership charts** Is it mandatory to obtain and verify an ownership chart for a legal entity customer?	An AI is obliged to understand the ownership and control structure of its customers. Although obtaining an ownership chart from the customer is the most convenient way of doing this, there is no strict requirement to do so. In deciding whether an ownership chart should be obtained, an AI should take into account the risk profile of the customer and the complexity of the ownership or control structure. Although an AI needs to identify any intermediate layers, it needs not, as a matter of routine, verify the details of the intermediate companies in the ownership structure. Whether this is necessary will depend upon the AI's overall understanding of the structure, the customer's risk profile and whether the information available is adequate in the circumstances for the AI to consider if it has taken adequate measures to identify the beneficial owners.
29.	Paragraph 4.4.14 of the AML/CFT Guideline	**Ownership charts** Is it a requirement to obtain a director's declaration on the ownership chart obtained?	No, it is not a requirement. Since an ownership chart is a document prepared by the customer, a declaration by the customer's director may not make the chart more reliable. However, as a director declaration evidences that a person with authority over the customer and who should have a close knowledge of its structure has signed it off, it may be considered to mitigate the risk of inaccurate or out-of-date information being presented. If an AI has doubt about the integrity of an ownership chart provided by the customer, it should take other steps to understand the ownership and control structure (eg obtain additional information or verify the details of the

	Relevant provisions	Question	Answer
			intermediate companies in the ownership structure).
30.	Paragraph 4.4.14 of the AML/CFT Guideline	**Intermediate layers** Do AIs need to obtain all identification information listed in paragraphs 4.3.6 and/or 4.3.11 of the AML/CFT Guideline in relation to each legal person or legal arrangement in the intermediate layer of a customer's ownership and control structure?	An AI should determine on a risk-sensitive basis the amount of information to be collected to identify each legal person or legal arrangement in the intermediate layer of a customer's ownership and control structure, which at a minimum should include their names. Further information, such as the place of incorporation and/or rationale behind the particular structure adopted, may be required on a risk-based approach.
Identification and verification of identity – trust or other similar legal arrangements			
31.	Paragraphs 4.3.10 and 4.4.11 of the AML/CFT Guideline	**Identifying and verifying the identity of a trustee of a customer that involves a trust** Where the customer involves a trust or other similar arrangement, how should an AI identify, and verify the identity of, a trustee?	Where the customer involves a trust or other similar arrangement, AIs should: (a) take the CDD measures in respect of the trust as required by the AMLO and AML/CFT Guideline; and (b) where the trustee is: (i) regarded as the AI's customer (which would normally be the case), identify and verify the identity of the trustee having regard to the usual standards for customers that are individuals or legal persons, as applicable; or (ii) not regarded as the AI's customer (eg where the trust has its own legal personality; or where the trust appears as part of an intermediate layer), identify and take reasonable measures to verify the identity of the trustee. Reasonable measures may include corroborating the undertaking or declaration obtained with publicly available information.
32.	Paragraph 4.4.4 and footnote 30 of the AML/CFT Guideline	**A trust appears as part of an intermediate layer** How should an AI identify and verify a trustee if the trust appears as part of an intermediate layer?	If a trust or other similar legal arrangement appears as part of an intermediate layer, the AI should identify and take reasonable measures to verify the identity of the trustee. For example, where a trustee is acting in its professional capacity (ie acting as a trustee in the course of profession or business) (eg a TCSP licensee) it may be appropriate to verify the identity of the trustee by checking the relevant regulatory register (eg the Register of TCSP Licensees made available by the Companies Registry).

	Relevant provisions	Question	Answer
33.	Paragraphs 4.4.1, 4.4.10 and 4.4.11 of the AML/CFT Guideline	**Beneficial owners of a trust customer** Where a settlor, trustee, protector or enforcer of a trust customer is a legal person, who should an AI identify and take reasonable measures to verify the identity of, as a beneficial owner?	Beneficial owner refers to the natural person(s) who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted. Where a settlor, trustee, protector or enforcer of a trust customer is a legal person, the objective remains to follow the chain of ownership or control to the beneficial owner (ie a natural person) in accordance with paragraph 4.4.14 of the AML/CFT Guideline, and to identify and take reasonable measures to verify the identity of such natural person.
34.	Paragraph 4.4.12 and footnote 32 of the AML/CFT Guideline	**Trust beneficiary** For a beneficiary of a trust designated by characteristics or by class, what other examples of information concerning the beneficiary can be obtained by the AI in addition to the one provided in footnote 32 of the AML/CFT Guideline?	Examples of information concerning the beneficiary designated by characteristics or class may include: (a) the nieces, nephews, cousins or grandchildren of certain persons as at the time of their death; (b) certain award recipients approved by a prescribed charity as at a certain date; (c) one or more charities relating to a particular cause that are selected by a prescribed person. The aim is to satisfy the AI that it will be able to establish the identity of that beneficiary at the time of payout or when the beneficiary intends to exercise vested rights.
Person purporting to act on behalf of the customer (PPTA)			
35.	Paragraph 4.5.1 of the AML/CFT Guideline	**Identifying the PPTA** Who should be treated as a PPTA?	A person may utilise a business relationship established between an AI and another person (natural or legal person) or legal arrangement to conduct ML/TF activities. FATF Recommendation 10 requires financial institutions to identify and verify the identity of any person purporting to act on behalf of the customer (PPTA), and the AMLO adopts the same requirement. Neither the FATF Recommendations nor the AMLO define the scope of PPTA. The AML/CFT Guideline explains that *whether the person is considered to be a PPTA should be determined based on the nature of that person's roles and the activities which the person is authorised to conduct, as well as the ML/TF risks associated with these roles and activities*. At a minimum, a person who is authorised to act on behalf of a customer to establish a business relationship with an AI should always be treated as a PPTA.

	Relevant provisions	Question	Answer
			AIs should adopt a framework of procedures for assisting their employees in assessing who would ordinarily be considered a PPTA for each customer segment. The approach and rationale should be consistent across departments and customer segments, to the extent possible. As a general proposition, each legal person customer should have at least one PPTA (ie the person acting on behalf of a customer to establish the business relationship with the AI as mentioned above) but there may be multiple PPTAs. PPTAs may also act alone or jointly. However, it is recognised that there may be some scenarios where no PPTA will be identified where this is unavoidable by virtue of the nature of the arrangements. Examples may include: correspondent banking relationships where account opening/payment instructions are provided via authenticated payment platform like SWIFT; or where the customer is onboarded solely due to the involvement of local staff, but no account is opened and no contract is signed with an AI in Hong Kong, and relevant instructions come from another branch in the AI's group.
36.	Paragraph 4.5.1 of the AML/CFT Guideline	**Account signatory** Should all account signatories of a customer be considered as PPTAs?	Account signatory refers to an individual authorised by a customer to transact on behalf of the customer or operate the customer's account / business relationship. While AIs have to guard against unauthorised transactions, this risk mainly relates to fraud and is different from ML/TF risk. AIs normally obtain names, specimen signatures and written authorisation of all account signatories to guard against this risk. Therefore, not every account signatory is required to be identified and verified for AML/CFT purposes (ie not every account signatory should be considered as a PPTA). The AML/CFT Guideline explains that *whether the person is considered to be a PPTA should be determined based on the nature of that person's roles and the activities which the person is authorised to conduct, as well as the ML/TF risks associated with these roles and activities*. For example: • Example 1: Person A appoints Person B as the account signatory of their bank account and provides Person B with unlimited authority to direct how funds move in and out of the account. Person B is a PPTA. • Example 2: Company Y appoints a number of staff as the account signatories (including Person E). Person E is not authorised to move funds in Company Y's account but is authorised to issue a cheque up to a reasonable amount if it is co-signed by another staff member. In this case, Person E is unlikely to be a PPTA given the ML/TF risk associated with Person E's role is limited.
37.	Paragraphs 4.5 and 4.8 of the AML/CFT Guideline	**Lists of signatories** Is an AI required to identify and verify the identity of all account signatories?	Account signatories are only required to be identified and verified if they are a PPTA. Instead of verifying the PPTAs' identities by reference to the identification document, data or information for each PPTA, AIs may take other reasonable measures (ie appropriate measures which are commensurate with the ML/TF risks). For example, where a business relationship is assessed to present a low ML/TF risk, an AI could verify the PPTAs' identities by reference to a list of PPTAs, whose identities and authority to act have been confirmed by a

	Relevant provisions	Question	Answer
			department or person within that customer which is independent to the persons whose identities are being verified (for example, compliance, audit or human resources).
38.	Paragraph 4.5.1 of the AML/CFT Guideline	**Persons purporting to act on behalf of the customer** Should dealers and traders in an investment bank or asset manager be considered as PPTAs?	Dealers and traders in an investment bank or asset manager who are authorised to act on behalf of the investment bank or asset manager would *not ordinarily* be considered as PPTAs. However, there is no "one size fits all" approach given the differences in roles and ML/TF risks involved. An AI should have a documented policy that applies a reasonable approach, having regard to the ordinary meaning and other FAQs relating to PPTAs.
Connected parties			
39.	Paragraphs 4.3.18 and 4.3.19 of the AML/CFT Guideline	**Connected parties** Why does an AI need to obtain the names of all the connected parties of the customers that are legal persons or legal arrangements?	The purpose of obtaining the names of all the connected parties of a customer is to facilitate the sanction screening requirements set out in paragraph 6.17 of the AML/CFT Guideline.
40.	Paragraph 4.3.19 of the AML/CFT Guideline	**Connected parties** Who is to be regarded as "*holding a senior management position or having executive authority in a customer*" for the purpose of paragraph 4.3.19(d)?	Paragraph 4.3.19(d) only applies to customers that are not corporations, partnerships, or trust or other similar arrangements, so these customers may include, for example associations, clubs, societies, charities etc. Whether a natural person is regarded as holding a senior management position or having executive authority of these customers depends significantly on the management structure of the customers concerned. It is generally for the AI to determine based on its understanding of the customer's management structure obtained through the CDD process. Examples of person holding a senior management position or having executive authority may include the president, vice-president, secretary or treasurer of the customer.
Reliability of documents data or information			
41.	Paragraph 4.3.14 of the AML/CFT Guideline	**"Current" data etc** An AI should ensure that documents, data or information obtained is	Whether a document provided by a customer should be regarded as "current" depends on the nature of the document. The following examples may give AIs some guidance: (a) for a document with an expiry date (eg passport), it cannot be expired at the time of verification;

	Relevant provisions	Question	Answer
		current at the time they are provided to the AI. What is meant by the term "*current*"?	(b) for a document that will be updated on a frequent and specified basis (eg an annual return), the AI may generally accept the latest version of the document; (c) for a document that does not have an expiry date and is not required to be regularly updated (eg certificate of incumbency or certificate of good standing issued by the registered agent of a company incorporated outside Hong Kong), unless there is an independent and reliable public source of information to verify its reliability, the AI should only accept the document if it was issued within a reasonable timeframe (ie a reasonable timeframe from the date it is received or obtained by the AI. 6 months is generally regarded as reasonable but this can be adjusted taking an RBA). AIs may also obtain a written assurance that the document obtained is current from the customer, its PPTA or a reliable third party. AIs should also be aware of any inconsistencies between the document obtained and those that have been determined by the AI to be current. The above guidance equally applies if data or information (eg digital identity recognised by government) is used for identity verification.
42.	Footnote 56 of the AML/CFT Guideline	**Expired documents** If a previously obtained identity document such as passport of a customer is expired, does the AI need to re-verify any aspect of customer identification by obtaining a current identity document?	AIs do not need to re-verify any aspect of customer identification just because of the expiry of a previously obtained identity document. According to footnote 56 of the AML/CFT Guideline, once the identity of a customer has been satisfactorily verified, there is no obligation to re-verify identity unless in specified circumstances; however, AIs should take steps from time to time (ie during a periodic or trigger event CDD review) to ensure that the customer information that has been obtained is up-to-date and relevant.

<table>
<tr><th></th><th>Relevant provisions</th><th>Question</th><th>Answer</th></tr>
<tr><td>43.</td><td>Paragraph 4.3.16 of the AML/CFT Guideline</td><td>Electronic documents

What measures are AIs expected to take to ensure the reliability of identification documents which are in electronic form?</td><td>The AML/CFT Guideline recognises that some commonly used original identification documents can be in electronic form. The AI should take appropriate measures to ensure the reliability of the electronic documents. The appropriateness of the measures to be taken will depend on the type of identification document in question. The following examples may apply:

<table><tr><th>Electronic document</th><th>Appropriate measure to ensure reliability</th></tr><tr><td>Original certificate of incorporation issued by the Hong Kong Companies Registry in electronic form</td><td>When accepting a print copy of an electronic Certificate of Incorporation, an AI can corroborate with other identification document or information (eg record of company registries) to ensure the reliability of the print copy.</td></tr></table>
Note: For the avoidance of doubt, corroboration would not be required for instances where the AI itself has downloaded a particular document (as opposed to having received a print copy of it) from a reliable source (eg Hong Kong Companies Registry’s website).</td></tr>
<tr><td>44.</td><td>Paragraph 4.3.17 of the AML/CFT Guideline</td><td>Document in foreign language

Does the translation need to be performed by a professional third party (eg solicitor)?</td><td>There is no requirement that the translation has to be performed by a professional third party (eg solicitor) or someone who is qualified; AIs may obtain a translation from a reliable source, which may include technology solutions and commonly used translation tools.</td></tr>
<tr><td>45.</td><td>Paragraph 4.10.4 of the AML/CFT Guideline</td><td>Certification

Who would be regarded as an appropriate certifier for the purpose of paragraph 4.10.4 of the AML/CFT Guideline?</td><td>The following is a list of non-exhaustive examples of appropriate persons to certify verification of identification documents:

(a) an intermediary specified in section 18(3) of Schedule 2;

(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;

(d) a Justice of the Peace; and

(e) other professional person such as certified public accountant, lawyer, notary public or chartered secretary Note.</td></tr>
</table>

	Relevant provisions	Question	Answer
			Note: a chartered secretary refers to a person who is a current full member of the Chartered Governance Institute or its designated divisions.
46.	Paragraph 4.10.4 of the AML/CFT Guideline	**Certification** If an AI decides to use certification as a supplementary measure to fulfil the requirement of section 9 of Schedule 2, what types of documents should be certified?	In general, only the identification document used for the purpose of identity verification (eg official document such as an identity card, passport, certificate of incorporation, or certificate of incumbency issued by registered agent etc) should be subject to certification. Certification can be time consuming and costly, so there is no need or expectation to require certification for all other CDD information or documents provided by the customer; or to require certification if an AI is able to check the documents against public sources. As a general principle, customers should always be provided with the opportunity, if they wish to do so, to present their original documents to the staff of the AI.
Simplified due diligence			
47.	Paragraph 4.8 of the AML/CFT Guideline	**Specific customers in non-equivalent jurisdiction** SDD in relation to beneficial owners is permitted in relation to public bodies, AIs and investment vehicles in Hong Kong or "equivalent" jurisdictions. Is an AI entitled to conduct SDD on such entities in non-equivalent jurisdictions?	If the customer is in a non-equivalent jurisdiction this should be taken into account in determining the risk level of the customer, and the extent of customer due diligence measures to be applied should be commensurate with the assessed level of risk. If the level of ML/TF risk is assessed as low, SDD under paragraphs 4.8.1 to 4.8.8 (except paragraph 4.8.8(b)) can be applied (ie *reducing the extent* of CDD measures taken). However, appropriate identification and verification measures in relation to the beneficial owners must still be undertaken, as this scenario does not involve a customer of the type specified in section 4 of Schedule 2 to the AMLO. It is simply that the *extent* of measures undertaken might be less, on an RBA.
48.	Paragraph 4.8.12 of the AML/CFT Guideline	**Listed company beneficial owner transparency** How does an AI establish if a listed company is subject to disclosure requirements that ensure adequate transparency of beneficial ownership?	In determining whether a listed company is subject to disclosure requirements that ensure adequate transparency of the company's beneficial ownership, an AI could take into account the following factors, for example: (a) whether there is a statutory regime that requires the disclosure of interests in listed companies above a certain threshold, either by the shareholder concerned or by the listed company in question; (b) the existence of penalties for non-compliance (pecuniary or otherwise) with the disclosure requirements; (c) a clear minimum shareholding threshold that triggers disclosure – in general, it should be at least the beneficial ownership threshold under the AMLO (more than 25%), or lower if needed to reflect the AI's

	Relevant provisions	Question	Answer
			internal standards; (d) a specified timeframe for disclosure – in general, it would normally be expected that disclosures should be made within a limited number of days of the relevant triggering event; and (e) public access to the shareholder information.
Enhanced due diligence			
49.	Paragraph 4.9.5 of the AML/CFT Guideline	**Customer risk factor** Where a customer, or in the case of a legal person customer, its connected parties, PPTAs or beneficial owners, are located outside Hong Kong, must the customer be considered high risk?	No, this should be determined on a case-by-case basis. Where a customer's main business and areas of focus are in another jurisdiction, if the AI is satisfied with the reason for opening / maintaining an account in Hong Kong, the difference in location does not necessarily have to be considered a high ML/TF risk indicator.
50.	Paragraphs 4.6.1, 4.9.6, 4.9.10 and 12.3 of the AML/CFT Guideline	**Source of wealth** Do AIs need to establish source of wealth for every customer?	No. The requirement to collect source of wealth information ordinarily applies to higher risk situations and therefore AIs are not expected to establish source of wealth for each and every customer. For most customers that are non-high risk customers, certain information obtained by an AI to understand the purpose and intended nature of the business relationship (eg occupation of individual customers, or business nature of corporate customers) should be sufficient for the AI to have a basic understanding of the customer's profile and accordingly be able to monitor that the account balance, and value and volume of transactions, is in line with their expected wealth and customer's profile. Even when establishment of source of wealth is required, there is no expectation to apply the same source of wealth procedures to all relevant customers in the same manner, or collect evidence dating back decades when the risk does not justify doing so, as it is often impractical.
51.	Paragraphs 4.9.2, 4.9.6, 4.9.10, 4.9.18 and 4.9.25, of the AML/CFT	**Source of wealth** How do AIs adopt a risk-based approach in relation to establishing the source of	When an AI is required to establish the source of wealth of an individual, it should adopt an RBA to determine the extent of measures (ie the extent of measures should be commensurate with the level of ML/TF risk of the customer concerned). It is not necessary for the AI to obtain evidence to corroborate the information provided to the AI or to verify the individual's net worth in all cases. Where appropriate, the AI may seek evidence from a reliable, independent source that can corroborate the gist of the source of wealth information (eg publicly

	Relevant provisions	Question	Answer
	Guideline	wealth of an individual?	available property registers, land registers, asset disclosure registers or company registers). Further guidance in relation to understanding the source of wealth of a customer that presents a higher risk of ML/TF is set out at **Appendix 1** to these FAQs.
52.	Paragraph 4.15 of the AML/CFT Guideline	**Jurisdictions subject to a call by the FATF** Which jurisdictions are subject to a call by the FATF?	Only jurisdictions listed in the FATF statement: "*High-Risk Jurisdictions subject to a Call for Action*" should be regarded as "jurisdictions for which this is called for by the FATF" under paragraph 4.15.1 of the AML/CFT Guideline. EDD measures that are proportionate to the risks should be conducted on business relationships and transactions with customers from these jurisdictions. For the avoidance of doubt, conducting EDD measure is not mandatory for customers connected to jurisdictions listed in the FATF statement: "*Jurisdictions under Increased Monitoring*". However, the fact that a customer is connected to such a jurisdiction should be taken into account in determining the overall risk profile of the customer.
Politically Exposed Persons (PEPs)			
53.	Paragraph 4.9.15 of the AML/CFT Guideline	**International organisation PEPs** Are agencies of the UN considered to be "international organisations" for the purposes of establishing PEP status?	Yes, agencies of the UN are international organisations and such agencies are listed on the UN website currently available at the following website: https://www.un.org/en/sections/about-un/funds-programmes-specialized-agencies-and-others/index.html
54.	Paragraph 4.9.16 of the AML/CFT Guideline	**International organisations PEPs** Should individuals with a prominent function at all kinds of international organisations be regarded as a PEP?"	"*International organisations*" are defined in the AML/CFT Guideline as entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as resident institutional units of the countries in which they are located. As such, individuals at organisations that do not meet these criteria are not international organisation PEPs. However, if an individual holds a prominent function at an organisation that may have certain similarities to, but which nevertheless does not meet the prescribed definition of, an "international organisation" (eg an international sport association), the AI should consider whether this impacts the risk profile of the customer.
55.	Paragraphs 4.9.10 and 4.9.24 of the	**Senior management approval**	It is for individual AIs to determine this question, as organisational structures vary from AI to AI. AIs should maintain clear and documented policies setting out the persons within the institution who are able to approve PEP customer onboarding and a continued business relationship. In any event, it should only include those

	Relevant provisions	Question	Answer
	AML/CFT Guideline	Who qualifies as "senior management" for the purposes of being able to approve establishing / continuing a business relationship with a PEP?	with sufficient seniority. The number and title of such persons will vary according to the size, type and institutional risk assessment of the AI. Senior management may include personnel in another jurisdiction if this reflects the AI's organisational structure and risk management practices.
56.	Paragraphs 4.9.13 and 4.9.19 of the AML/CFT Guideline	**Former non-Hong Kong PEPs** Does an AI need to obtain senior management approval if an AI decide not to apply, or not to continue to apply the EDD measures to a former non-Hong Kong PEP who no longer presents a high risk of ML/TF after stepping down?	No. The decision for not applying EDD does not require senior management. However, AI should conduct an appropriate assessment on the ML/TF risk associated with the previous PEP status taking into account various risk factors, including but not limited to: (a) the level of (informal) influence that the individual could still exercise; (b) the seniority of the position that the individual held as a PEP; or (c) whether the individual's previous and current function are linked in any way (e.g. formally by appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters).
Intermediaries			
57.	Footnote 48 of the AML/CFT Guideline	**Using intermediaries for ongoing monitoring** Can an intermediary be relied upon to conduct ongoing monitoring as per section 5 of Schedule 2 to the AMLO?	No. Section 18 of Schedule 2 only allows an AI to carry out any CDD measures set out in section 2 of Schedule 2 by means of an intermediary but does not allow an AI to rely on an intermediary to continuously monitor relevant business relationships as required by section 5 of Schedule 2. Therefore, an AI cannot rely on an intermediary to continuously monitor its business relationships with a customer (ie ongoing CDD and transaction monitoring). However, the AI may use an intermediary to collect further documents, data and information, and provide or coordinate relevant updates, to assist the AI in ensuring that the CDD records maintained by the AI remain up-to-date and relevant.
Correspondent banking			
58.	Paragraph 11.1 of the AML/CFT	**"Another institution"** In the definition of correspondent banking, what	While the AMLO does not define what "*another institution*" means in the definition of correspondent banking, section 7 and section 14 of Schedule 2 only apply to correspondent banking relationship with an institution located in a place outside of Hong Kong that carries on a business similar to that carried on by an AI.

	Relevant provisions	Question	Answer
	Guideline	is meant by the term "*another institution*"?	
59.	Paragraph 11.2 of the AML/CFT Guideline	**Non-customer relationships** A correspondent banking relationship does not include occasional transactions or the mere exchange of SWIFT RMA keys in the context of "*non-customer relationships*". What is considered a non-customer relationship for the purposes of this requirement?	"Non-customer relationship" refers to a relationship that does not fall under the definition of business relationship in the AMLO and the counterparty is not regarded as a "customer" of the AI (also see paragraph 4.1.5 of the AML/CFT Guideline). A non-customer RMA relationship is generally created when there is a request that the bank sends or receives SWIFT messages to/from a third party (ie the non-customer) in support of a customer's business and where the bank has no other relationship with that third party. This can include both transactional and non-transactional messages. Such arrangements are sometimes referred to as "network banks," which facilitate the continuing ability to meet customer global trading expectations and requirements. Network banks are non-customer banks and have no accounts, facilities or dedicated relationship manager. They are sponsored by a global line of business and interactions are limited to document exchanges and restricted SWIFT RMA message interactions. The settlement of any transaction is decoupled from the document exchange and always made via a customer bank. Some examples of where non-customer RMAs may be established to facilitate activities for existing customers include, but are not be limited to, the following: (a) Cash management: receipt of balance and transaction information on a corporate customer's account at another bank, so that the corporate customer can view activity through its bank's reporting tool (b) Cash management: relaying payment instructions from a corporate customer to their third party bank (c) Custody: provision of information from a sub custodian bank to the global custodian at the request of the client (d) Trade Finance (eg letters of credit): exchange of messages with banks that do not otherwise have direct payment relationships (e) Exchange of messages with payments and securities markets infrastructure entities, eg exchanges and depositories (f) Message relaying intermediary bank: serving as an intermediary bank only to relay transactional or non-transactional measures without any accounts opened (g) Principal to principal and treasury transactions: the relationship facilitates principal to principal transactions or treasury deals only, such as foreign exchange trading or bond trading

	Relevant provisions	Question	Answer
60.	Paragraph 11.6 of the AML/CFT Guideline	**Responsibilities of each party** AIs are required to understand and document clearly the agreed lines of responsibility for AML/CFT in a correspondent banking relationship. Must this be in written form?	It is not mandatory for the two AIs to reduce their respective responsibilities to a written contract provided there is a clear understanding as to which institution will perform the required measures in relation to AML/CFT and this is documented (eg through an exchange of correspondence or where responsibilities are bound by SWIFT terms and conditions).
61.	Paragraph 11.8 of the AML/CFT Guideline	**Additional measures** Is an AI required to obtain and record all the jurisdictions in which a respondent bank has its subsidiaries and branches?	No. The information that has been taken into account in determining the extent of additional measures to be applied should be recorded. Factors that increase risk and mitigating factors should all be recorded if they have informed the decision-making process regarding the additional steps to be taken, this will not always involve recording all jurisdictions in which the respondent bank is present.
Private banking			
62.	Paragraph 12.6 of the AML/CFT Guideline	**Adverse news screening** In addition to the private banking customer, on whom should an AI perform adverse news screening?	An AI should conduct adverse news screening on a private banking customer, and any other persons known by the AI to be associated with that customer as far as practicable, before establishing the private banking relationship. For the purposes of this requirement, "*any other persons known by the AI to be associated with the customer*" may include known living family members and known living business associates who are known to have contributed to the source of wealth of the customer.
63.	Paragraph 12.10 of the AML/CFT Guideline	**Meetings** How often is an AI required to meet their private banking customers?	An AI is required to meet their private banking customers on a regular basis as far as possible. The frequency of meetings should be commensurate with the customer's assessed ML/TF risk profile.

	Relevant provisions	Question	Answer
64.	Paragraph 12.8 of the AML/CFT Guideline	**Using technology to facilitate meetings** What technology can an AI use in order to conduct a meeting with a customer?	An AI can use technology to facilitate a meeting with a private banking customer, eg real-time video conferencing call, provided that the audio-visual quality enables effective communication.
Customer due diligence reviews			
65.	Paragraph 5.2 of the AML/CFT Guideline	**Trigger events** What could constitute a "*trigger event*" for the purposes of requiring a CDD review?	Trigger events include: (a) when a significant[4] transaction is to take place; (b) when a material change occurs in the way the customer's account is operated; (c) when the AI's customer documentation standards change substantially; or (d) when the AI is aware that it lacks sufficient information about the customer concerned.
66.	Paragraphs 4.12.2, 5.2 and footnote 57 of the AML/CFT Guideline	**Re-activation of a dormant relationship** When a dormant relationship is re-activated, is the AI required to complete a trigger event CDD review before re-activating the relationship?	AIs should adopt appropriate risk management policies and procedures to manage the risks associated with the reactivation of dormant relationships. These policies and procedures should include, for example, establishing a reasonable timeframe for the completion of CDD review on an RBA, and if account use is permitted before completion, imposing risk mitigating controls such as restricting account functions; imposing transaction limits or implementing enhanced transaction monitoring measures before completing the CDD review.
Suspicious transaction report (STR)			
67.	Chapter 7 of the AML/CFT Guideline	**Reporting requirement under National Security Law (NSL)** Who should NSL-related STRs be filed to?	All STRs should continue to be filed to the Joint Financial Intelligence Unit (JFIU) following existing reporting mechanism, i.e. STREAMS, and the "consent / no consent" systems will remain. AIs can click the box "National Security Law" under the "Reason for Disclosure" column in the STR Proforma, where appropriate. Note: While it is recognised that AIs may not be able to have full knowledge of the exact nature of the underlying crime, it is expected that these categories are selected on a best effort basis.

[4] The word "significant" is not necessarily linked to monetary value. It may include transactions that are unusual or not in line with the AI's knowledge of the customer.

	Relevant provisions	Question	Answer
68.	Chapter 7 of the AML/CFT Guideline	**Reporting requirement under NSL** What are AIs' reporting requirements under the NSL? Is the reporting threshold the same as OSCO?	The obligation for reporting under the NSL will be triggered when an AI "knows" or "suspects" that any property is offence related property. The threshold for reporting is the same as under existing arrangements under the Organized and Serious Crimes Ordinance (OSCO), the Drug Trafficking (Recovery of Proceeds) Ordinance (DTROP) and the United Nations (Anti-Terrorism Measures) Ordinance (UNATMO). The time frame for reporting is also the same, ie AIs should file an STR to the JFIU as soon as reasonably practicable.
69.	Chapter 7 of the AML/CFT Guideline	**Offence related property** What is the definition of "offence related property" in NSL and under what circumstances should an AI disclose this property to the JFIU?	"Offence related property" as defined under section 1 of Schedule 3 to the Implementation Rules of the NSL refers to the property of a person who commits or attempts to commit, or participates in or facilitates the commission of, an offence endangering national security; or property used / intended to be used for financing or assisting the commission of an offence endangering national security. "Offence endangering national security" refers to offence of that nature under the NSL and the laws of the HKSAR safeguarding national security. Pursuant to section 5 of Schedule 3 to the Implementation Rules of the NSL, the following non-exhaustive scenarios can be regarded as circumstances that trigger a disclosure obligation: (a) When it comes to AIs' attention that a person is arrested / charged for an offence endangering national security; and/or (b) When AIs have knowledge or suspicion that a property is "offence related property" after receiving information from law enforcement agencies. The AIs MUST make a disclosure of the property held by the persons specified in (a) or the circumstance in relation to (b) to JFIU. For the avoidance of doubt, such property includes all kind of property regardless of the portion of shareholdings by the persons specified in (a). If an AI wishes to contact the National Security Department of the Hong Kong Police Force (NSD) for advice, the AI can do so by the following means: NSD Hotline for Financial Institutions: 2896 3270 Email: enquiry3@police.gov.hk
Requests from law enforcement agencies and crime-related intelligence			
70.	Paragraph 7.31 of the	**Law enforcement requests** Would AIs be requested	No. As with the existing practice under OSCO, DTROP and UNATMO, requests by the law enforcement agencies for information of an account managed in other jurisdictions will be made through Mutual Legal

	Relevant provisions	Question	Answer
	AML/CFT Guideline	under search warrants related to NSL to submit information of customer's accounts in their branches or subsidiaries in other jurisdictions?	Assistance (involving the Department of Justice). Such requests will not be made through the AIs.
71.	Paragraph 7.31 of the AML/CFT Guideline	**Law enforcement requests** It is noted that, under exceptional circumstances, a warrant is not required for the search of places for evidence under NSL. How are AIs able to ascertain if authority has been conferred for such actions?	A search warrant will ordinarily be obtained by law enforcement agencies when searching an AI's records. Under exceptional circumstances where it would not be reasonably practicable to obtain such a search warrant, a police officer at or above the rank of Assistant Commissioner of Police may authorise the search. In such cases a formal written document will be produced to the AI on spot, with the name and contact details of the authorized officer clearly stated. Similar arrangements also exist under various other existing ordinances, such as the Gambling Ordinance.
72.	Paragraph 7.31 of the AML/CFT Guideline	**Law enforcement requests** Where an AI is made aware that certain transactions have a high ML/TF risk, what measures are the AI expected to take?	From time to time, law enforcement agencies inform AIs that certain transactions pose a high risk of being connected to activities which are illegal under the laws of Hong Kong. In such cases, AIs are expected to take effective and timely steps to manage the risk and to understand the full details of the transaction(s) in question. This will likely involve the identification of parties to the transactions including the underlying originators and final recipients of payments made via intermediary service providers or platforms. Depending on the types of information provided by the law enforcement agencies and additional information obtained by the AIs, appropriate risk-based measures should be taken to mitigate risks and to meet all relevant legal and regulatory requirements.
73.	Paragraphs 7.31 and 7.35 of the AML/CFT Guideline	**Crime-related intelligence requests** When an AI receives notification letters from law enforcement agencies, what measures would the AI be expected to take?	From time to time, law enforcement agencies may inform an AI of intelligence suggesting that potential suspicious transactions may have been conducted through particular bank account(s) maintained with the AI, e.g. through a notification letter. The AI should take necessary actions with regard to the contents of the notification letter from a law enforcement agency, for example, conducting a review in a timely manner. Appropriate risk mitigating measures including those required under relevant laws and regulations should be taken based on the review results. If the case information in a notification letter has also been made known to the public by law enforcement agencies (e.g. Scameter), the AI should assess the potential risks that may arise (e.g. reputational risks), and if necessary, take timely and effective measures to mitigate the risks.

	Relevant provisions	Question	Answer
Wire transfers			
74.	Paragraph 6.16(c) of the AML/CFT Guideline	**"Relevant party"** In a cross-border wire transfer, who must be screened as a "*relevant party*"?	An AI should, at a minimum, screen the following relevant parties in a cross-border wire transfer: (a) originator; (b) recipient; (c) ordering institution; (d) intermediary institution; (e) beneficiary institution; and (f) named parties (eg individuals, companies, banks etc) in the payment message.
75.	Paragraph 10.8 of the AML/CFT Guideline	**Accuracy of originator information** How should an ordering institution ensure that the required originator information is accurate?	The required originator information is deemed to be accurate if the identity of the originator has been verified in compliance with the AMLO and the AML/CFT Guideline. No further verification of the originator information is normally required, although ordering institutions may exercise their discretion to do so in individual cases.
76.	Paragraph 10.8 of the AML/CFT Guideline	**Originator's address** For wire transfers over $8,000,can the originator's address accompanying the wire transfer be a PO box address?	The address information accompanying the wire transfer should be sufficient to identify clearly the location of party / parties for sanctions screening and AML/CFT monitoring purposes. Therefore, having a Post Office (PO) Box as an address should be avoided except where no alternative exists.
Record-keeping			
77.	Chapter 8 of the AML/CFT Guideline	**Record-keeping of unsuccessful applicants** For cases of unsuccessful application for business, is an AI required to retain the	Under the AMLO, there is no requirement for an AI to maintain records and documents involving unsuccessful applicants. This, however, does not preclude the AI from retaining the relevant records and documents in order to meet its other statutory obligations.

	Relevant provisions	Question	Answer
		identification records and documents in relation to the unsuccessful applicants?	
Issues relating to financial group			
78.	Paragraph 4.1.6 of the AML/CFT Guideline	**Managed in substance** What is meant by the term "managed in substance" within the meaning of paragraph?	The term "managed in substance" refers to the substantive aspects of the business relationship, rather than the performance of mere administrative or back-office functions. Such a determination has to take into account the particular circumstances of an AI. In general, if an AI carries out relationship management for a customer whose account is booked outside Hong Kong, the AI will have a business relationship with the customer (see definition of business relationship in Part 1 of Schedule 2 to the AMLO). For the avoidance of doubt, relationship management may take place from more than one location.
79.	Paragraph 3.15 of the AML/CFT Guideline	**Subsidiaries incorporated outside Hong Kong** With reference to section 22(1)(b) of Schedule 2, where a bank incorporated in Hong Kong has a subsidiary that carries on a securities or insurance business outside Hong Kong, will section 22 apply to such a subsidiary ie is the subsidiary regarded as "carrying on the same business as a financial institution in a place outside Hong Kong"?	It should be noted that section 22(1)(b) of Schedule 2 states "the same business as an FI" but not "the same business as the FI". The term "FI" refers to an FI as defined in the AMLO, including authorized institution, licensed corporation, authorized insurer, etc. Therefore, so long as the subsidiary incorporated outside Hong Kong carries out the business as any type of FI (not necessarily as the same type of the business of the parent company), then this provision will apply.
80.	Paragraph 3.17 the AML/CFT Guideline	**Group-wide information sharing** Article 63 of the NSL stipulates that the relevant institutions, organisations	As with existing obligations under the OSCO, DTROP and UNATMO, AIs should also observe information confidentiality requirements under the NSL and must not disclose to another person any information or other matter which is likely to prejudice any investigation which might be conducted. The sharing of information with head offices/branches/subsidiaries outside Hong Kong for risk management purposes, as global financial institution lawfully do now, will not be affected.

	Relevant provisions	Question	Answer
		and individuals who assist with the handling of a case shall keep confidential any information pertaining to the case. Would the sharing of information with head offices/branches /subsidiaries outside Hong Kong for risk management purposes breach this requirement?	
Dual-use goods			
81.	Not referenced in the AML/CFT Guideline	**Dual-use goods** What are dual-use goods and what controls should AIs have in place in respect of dual-use goods?	"Dual-use goods" are items that have both commercial and military or proliferation applications.[5] Further guidance for AIs in handling customers and transactions involving dual-use goods is set out at Appendix 2 to these FAQ.

[5] Paragraph 6.8, Guidance Paper on Combating Trade-based Money Laundering developed by HKAB with input from the HKMA (**TBML Paper**).

Appendix 1 – Establishing source of wealth[6]

Good practice

The below sets out a sample of good practices to be taken in relation to establishing the source of wealth of an individual.

Good practices	Details
Obtaining information	• (**When the type or level of business activity diverges from the customer's source of wealth**) Promptly conducting further assessments on the customer's source of wealth and reconsidering how to manage the business relationship with the customer (for example, establishing, maintaining or terminating business relationship) • (**Where there is an absence of information to ascertain the source of wealth**) Considering information on publicly disclosed assets – for example, asset disclosure systems which allow public access to information in the disclosure made by certain PEPs[7] • (**When obtaining information from a self-declaration**) Verifying the accuracy of the customer's declaration about the source of wealth through reliable sources such as: o publicly available property registers; o land registers, asset disclosure registers, company registers; o past transactions with AIs (for existing customers); and o other sources of information about legal and beneficial ownership. These are examples only. Where such sources are not available, AIs may take other reasonable measures to verify the accuracy of the customer's declaration.
New customer approval	• Challenging the source of wealth information (where appropriate) during the customer due diligence process • Conducting validation and corroboration (where appropriate)
Establishing policies and procedures	• Establishing effective escalation and advisory procedures to ensure that high risk customers, including PEPs, are appropriately identified and handled, and that staff responsibilities are clear • Establishing other clear risk-based policies and procedures, such as setting out the EDD measures required for higher-risk and PEP customers and on source of wealth
Reviews	• Proactively following up gaps in, and updating, source of wealth information for higher-risk relationships during the course of the relationship • Reviewing relationships periodically to ensure due diligence information remains current, and the risk assessment and associated controls remain appropriate

[6] Attention is also drawn to the "Wolfsberg Source of Wealth and Source of Funds (Private Banking/Wealth Management) FAQs" published on 7 August 2020, available here: https://wolfsberg-principles.com/articles/publication-source-wealth-and-source-funds-private-bankingwealth-management-faqs

[7] Note that not all jurisdictions have such an asset disclosure system. It is often the case that there is only summary of information filed by these PEPs is made publicly available.

Poor practices

The below are examples of measures that would *not* generally be acceptable:

(a) ***failing to properly apply risk-based approach*** - source of wealth requirements (particularly when conducting verification) are not sufficiently risk-based, such as applying the same measures to customers of varying risks or collecting too little or too much information;

(b) ***taking information provided by clients at face value*** - always accepting a customer's explanation and material provided for source of wealth at face value, without probing further even where red flags are raised or raising insufficient challenge to source of wealth information;

(c) ***over-reliance*** - on undocumented information, particularly, relying on a self-declaration by the customer as to its source of wealth without verifying the information in the customer declaration through reliable external or internal sources;

(d) ***relying on intra-group introductions*** - where relevant standards are not equivalent to Hong Kong's or where due diligence data is inaccessible because of legal constraints;

(e) ***granting waivers*** from establishing source of wealth where it is mandatory; and

(f) ***failing to distinguish*** - between a customer's source of wealth and source of funds.

Source of wealth examples

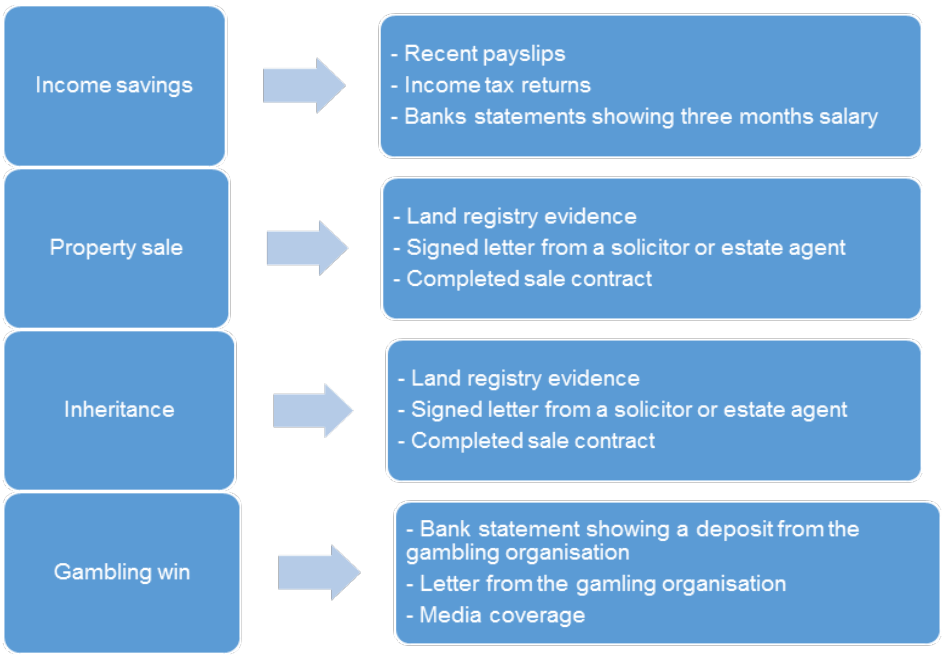
Source of wealth information should give an indication as to the size of wealth the customer would be expected to have, and a picture of how the individual acquired the wealth. It may be possible to gather this information from:

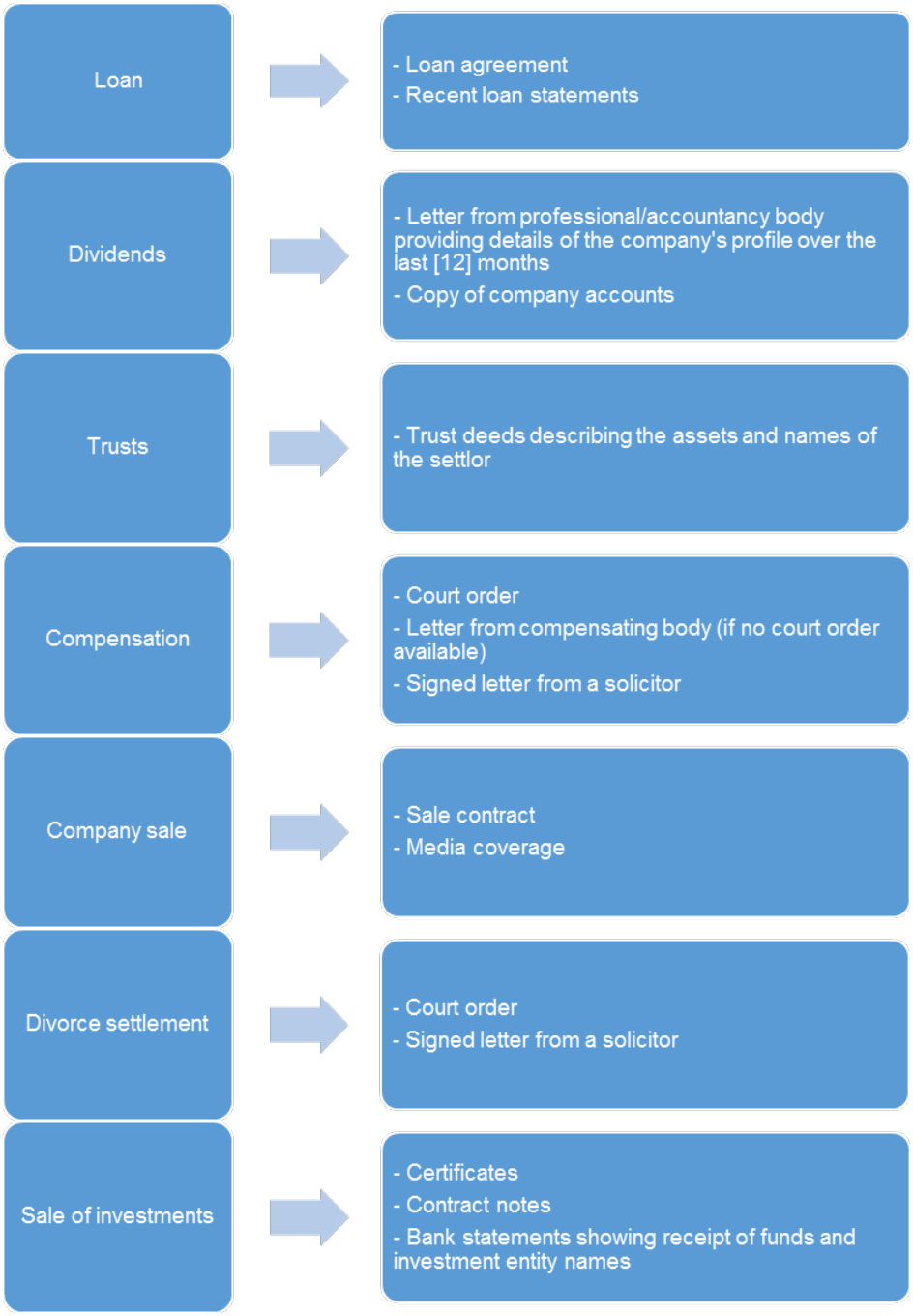
(a) official documents issued by a government or public body;

(b) public information and open sources, such as reputable sources on the Internet;

(c) confirmation from a professional service provider with knowledge of the customer (such as an accountant, lawyer, professional trustee or company services provider); or

(d) copies of primary sources, for example:




Loan
- Loan agreement
- Recent loan statements
Dividends
- Letter from professional/accountancy body providing details of the company's profile over the last [12] months
- Copy of company accounts
Trusts
- Trust deeds describing the assets and names of the settlor
Compensation
- Court order
- Letter from compensating body (if no court order available)
- Signed letter from a solicitor
Company sale
- Sale contract
- Media coverage
Divorce settlement
- Court order
- Signed letter from a solicitor
Sale of investments
- Certificates
- Contract notes
- Bank statements showing receipt of funds and investment entity names

Appendix 2 – Guidance on dual-use goods

Introduction

Certain AIs may face elevated ML/TF, financial sanctions and proliferation financing risks (**Relevant Risks**) due to their involvement in trade-related financial services and/or their exposure to various international touchpoints as part of their customer relationships and their customer's own supply chains, relationships and transactions.

Of particular complexity are "dual-use goods", which involve products and materials that can have both legitimate commercial applications, as well as military or proliferation applications. Transactions involving dual-use goods can carry heightened Relevant Risks.

Under the TBML Paper, AIs are recommended:

- to implement screening procedures that provide guidance on dealing with alerts relating to "hits" on dual-use goods to identify and escalate (for further review) trade transactions involving dual-use goods, taking into account other relevant red flags in a transaction;[8]
- to adopt appropriate policies and procedures as commensurate with the nature and scale of their trade-related activities;[9] and
- to refer to the "Dual-use Goods List" [10] maintained under the Import and Export (Strategic Commodities) Regulations (Cap. 60G)[11] (**Dual-use Goods List**).

AIs may also need to consider the application of other dual-use good lists and other trade-related rules in applicable jurisdictions which may affect their operations.

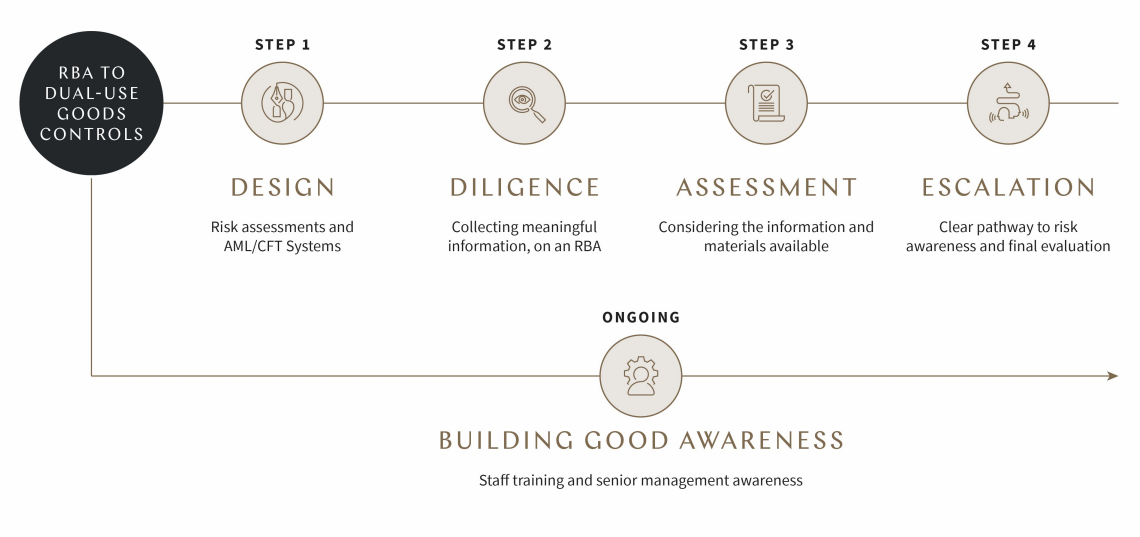
This Appendix 2 sets out guidance for AIs in handling customers whose business or transactions may involve dual-use goods. Specifically, it summarises good practices that AIs may consider implementing, having regard to the nature, size and complexity of their business and the Relevant Risks to which they are exposed.

For clarity, the sample good practices in this Appendix 2 are intended to support the development of AIs' own controls and **not** as a prescriptive minimum or maximum standard. AIs should consider them on an RBA, having regard to their own circumstances and their assessment of Relevant Risks.

Sample good practices

Mitigating the Relevant Risks presented by dual-use goods generally requires a thoughtful approach across several key elements of the design and execution of an AI's AML/CFT Systems. The following sample good practices are therefore set out in the following sequence to illustrate how dual-use goods may be taken into account at relevant junctures, with an illustrative chart to summarise the key steps.

[8] Paragraphs 6.2 and 6.9, TBML Paper.
[9] Paragraph 6.9 and Annex B Part 2 Suggested Best Practices, TBML Paper.
[10] See the "Strategic Commodities Control List of HKSAR" at: https://www.stc.tid.gov.hk/english/checkprod/sc_control.html.
[11] Annex B Part 2 Suggested Best Practices, Trade-based Money Laundering Guidance Paper.



Key steps	Sample good practices
Step 1: Design **Risk assessments and AML/CFT Systems**	✓ As part of the **institutional ML/TF risk assessment** under Chapter 2 of the AML/CFT Guideline, consider whether dual-use goods are likely to be involved in relation to the AI's customers and their transactions. ✓ If so, consider bolstering the **AML/CFT Systems** implemented under Chapter 3 of the AML/CFT Guideline to help address this possibility. For example, this may include: ▪ (**policy and procedure**) implementing a specific dual-use goods policy and procedure. This may be standalone, or embedded in other policies and procedures, with specific guidance and expected standards for staff on dual-use goods; ▪ (**customer frameworks**) customising the AI's customer risk assessment framework to support meaningful case-by-case customer risk assessments and customer due diligence. This might include, for example, questions specifically addressing dual-use goods and/or other questions that can help the AI better understand expected funds flows, transactional patterns and the potential extent of involvement of dual-use goods. Please also refer to Step 2, which contains several sample questions; and/or ▪ (**tools**) using internally developed or third-party tools to support the AI's identification and assessment of dual-use goods and management Relevant Risks. These could range from simple data sources and tools to help ensure relevant data is captured and can be assessed efficiently, through to more sophisticated screening and analytical tools.[12]
Step 2: Diligence **Collecting meaningful information, on an RBA**	✓ As part of **each customer ML/TF risk assessment** under Chapter 2 of the AML/CFT Guideline, consider whether dual-use goods are likely to be involved. This may, for example: ▪ consider whether the proposed business relationship with the AI may give rise to the Relevant Risks, for example, by using trade-related financial services; and ▪ include a number of questions for the customer to confirm. For example,

[12] Automated technologies have employed by certain institutions to conduct screening procedures such as computerised extraction of goods description from trade documents, conversion to universally applicable goods classification, screening against dual-use goods lists and market price analytics. Such automated technology solutions are also used for continuously monitoring customer accounts and transaction activities to identify unusual payment flows. This then signals targeted manual reviews and may warrant the filing of suspicious activity reports. However, for clarity, there is no mandatory one-size-fits-all approach, and there is no general expectation that sophisticated tools must be used by all AIs. Any tools and compliance approach selected are subject to the RBA and circumstances of the AI.

Key steps	Sample good practices
	these may include the following, on an RBA: Q Whether they are involved in any high-risk industries.[13] Q Whether they are involved in cross-border trade activity and if so, with which countries. Q Whether any products imported or exported by the customer are subject to import or export controls restrictions or require licensing in Hong Kong[14] or other relevant jurisdictions. Q The intended use or purpose of any goods and services that form part of the customer's business, and what steps, if any, the customer takes to ensure that only legitimate uses and purposes are involved (eg based on the customer's contractual, policy, monitoring or other controls). [15] Q Whether the customer has any government, military or paramilitary (or similar) customers. Q Whether the customer has faced any enforcement action or investigations in relation to dual-use goods, military or paramilitary activities or import/export controls. An AI may consider, on an RBA, whether it is appropriate to rely on a self-certification of these matters from the customer, or whether to request additional information or materials required. ✓ If so, as part of **customer due diligence** conducted under Chapter 4 of the AML/CFT Guideline, consider implementing EDD measures to support a closer review of the relationship and relevant transactions. Paragraph 4.9.6 of the AML/CFT Guideline provides a number of options for EDD measures. In the case of dual-use goods, these may include, for example, additional information about: ▪ the expected use of the dual-use goods; ▪ the jurisdictions that may be involved; ▪ any expected counterparties (including the potential end-user of the dual-use goods); and ▪ any internal policies, procedures, standard contractual terms or other controls that the customer has in place to address the risk of dual-use goods. ✓ Any additional contextual information obtained may also be used to help refine the risk level, as well as to support ongoing monitoring and review. **NB.** As a general principle, before onboarding a customer or enabling an AI's existing customer to use the AI's services, the AI should ensure it has enough information on hand to assess, as part of its customer risk assessment and customer due diligence:[16] ▪ the potential extent of involvement of dual-use goods; and ▪ whether any potential dual-use goods are used for ML/TF, sanctioned activities or proliferation financing purposes.

[13] For example, these may include those engaged in (a) military- or war-related goods or activities; or (b) any one or more of the 10 categories of dual-use goods on the Dual Use Goods List, being nuclear materials, facilities and equipment, special materials and related equipment, materials processing, electronics, computers, telecommunications, information security, sensors and lasers, navigation and avionics, marine and aerospace and propulsion. Further details of each of these categories is provided on the Strategic Commodities Control System website of the Trade and Industry Department, available at: https://www.stc.tid.gov.hk/english/hksarsys/Scope_Control_List.html. Each AI may develop an appropriate list of high-risk industries, on an RBA, having regard to its institutional risk assessment and its tools and other controls in place.

[14] AIs may refer to the Trade and Industry Department's webpage regarding Import and Export Licensing System for details (https://www.stc.tid.gov.hk/english/hksarsys/licensing.html), and if applicable, confirm with the customer if relevant licences have been obtained.

[15] This could be a general question in the customer risk assessment, with further details requested as part of EDD measures (if a risk of dual-use goods is identified). See below.

[16] See also Step 3 below in relation to customer due diligence.

Key steps	Sample good practices
Step 3: Assessment **Considering the information and materials available**	✓ As part of **customer due diligence** under Chapter 4, and **ongoing monitoring** under Chapter 5 of the AML/CFT Guideline: ▪ consider the information and materials available to the AI. To achieve this, it may be helpful to: o map relevant data sources within the organisation and broader group (as appropriate);[17] and o implement pre- and post-transaction risk indicators for certain transactions, taking an RBA.[18] Where a risk indicator is triggered, a further check can be undertaken to see whether any related goods are dual-use goods;[19] and ▪ if dual-use goods are involved, consider them in context. For example, some questions about a transaction involving dual-use goods could include:[20] Q Which counterparties or other third parties are involved? Q What is the expected use of the dual-use goods? Q Which jurisdictions are involved? This may include places relevant to the physical location of goods (origin, destination, transshipment) as well as jurisdictions of incorporation, flag state etc. Q Does the transaction appear commensurate with other information known about the customer? For example, does a particular chemical appear to be necessary for their manufacturing business, based on information provided by the customer or otherwise reasonably ascertainable from publicly available materials? Is the transaction consistent with any licences held by the customer? ✓ Additional steps may include, depending on the circumstances: ▪ screening counterparties and other third parties not previously screened; ▪ checking whether the transaction is also commensurate with desktop checks or other screening of any counterparties or jurisdictions; ▪ requesting additional information from the customer; ▪ considering any additional information available regarding prevailing circumstances relating to geopolitical events or other events relevant to a jurisdiction and/or the customer;[21] and/or ▪ seeking internal or external legal advice on the lawfulness of the transaction or other arrangements, where the AI considers it appropriate to do so. For clarity, AIs are only expected to consider information they have reasonable available to them and only to pursue additional information on an RBA.
Step 4: Escalation **Clear pathway to risk awareness and final evaluation**	✓ Implementing a clear escalation and review procedure in relation to: ▪ dual-use goods matters generally; and ▪ individual elevated risk scenarios. This may be a standalone procedure, or may be integrated into other policies and procedures, but in any case, should be clear and accessible to relevant

[17] See paragraph 3.17 of the AML/CFT Guideline in relation to intra-group sharing of information.
[18] See Part 3 of the TBML Paper for sample red flags in relation to trade-based money laundering. AIs may also establish additional indicators and parameters having regard to their institutional risk assessment, other AML/CFT Systems and industry knowledge (eg if they commonly serve a particular sector).
[19] For example, this could involve a check if a particular indicator may be discounted on closer review of the source material, or considering if additional information may be available to make an assessment. Please also refer to the HKMA's Guidance paper on Transaction Monitoring, Screening and Suspicious Transaction Reporting for additional guidance.
[20] Responses to such questions should be considered holistically to help support a meaningful understanding of the risk that the dual-use goods may be intended for illegitimate purposes.
[21] This generally refers to events that may elevate the risk that a dual-use good may be used for nefarious purposes such as the development of weapons of mass destruction or other military supplies.

Key steps	Sample good practices
	staff.[22] ✓ Involving senior management in sign-off before establishing or continuing a business relationship with customers with known exposure to dual-use goods. Given the variety of dual-use goods, this may not necessarily be required in all cases.[23] ✓ As part of **STRs** made under Chapter 7 of the AML/CFT Guideline and related statutory requirements, disclosing any known dual-use goods, where appropriate.
Ongoing: Building good awareness **Staff training and senior management awareness**	✓ As part of **staff training** providing in accordance with Chapter 9 of the AML/CFT Guideline, providing training on dual-use goods. This might include, for example: ▪ (**general**) general information about dual-use goods, so that staff are aware of their existence and key red flags to watch out for, even if no dual-use goods are expected; and ▪ (**specific**) more specific in-depth information about dual-use goods, including: ○ how to identify and assess them; ○ how to critically assess their legitimacy; and ○ how to apply relevant policies, procedures and tools. This training may be particularly appropriate for staff involved in onboarding customers, assessing dual-use goods or handling trade-related transactions, those with access to other relevant materials such as trade invoices and those involved in the design of relevant AML/CFT Systems and/or assessments. It may also be appropriate to extend this training more broadly when there is an elevated risk of dual-use goods being involved as part of the institutional risk assessment or a customer risk assessment. ✓ Briefing senior management on dual-use goods. ✓ In general, designing training in a way that is appropriate to the AI, its business and the risks to which it is exposed. For example, depending on all the facts: ▪ an AI may have a particular business sector focus (eg it may focus on customers in certain industries) that make in-depth training in relation to particular types of dual-use goods more relevant than others; and ▪ certain training may be appropriately provided as part of on-the-job guidance, rather than in structured training seminars. Ultimately, an AI should consider what is most appropriate, having regard to its institutional risk assessment,[24] AML/CFT Systems and Chapter 9 of the AML/CTF Guideline.

[22] These principles also apply to other controls referenced in this Appendix 2.

[23] In general, senior management sign-off is required where there is a high ML/TF risk (per paragraph 4.9.3 of the AML/CFT Guideline) or where a PEP is involved (per paragraphs 4.9.10 and 4.9.18 of the AML/CFT Guideline). By implication, where the risk is low and no PEPs are involved, no sign-off may be required. For example, if relevant goods have a clear civilian purpose and information supplied by the customer and otherwise sourced by the AI is consistent with that purpose, the customer is reputable, the customer operates in a low-risk jurisdiction, all other information appears credible, the customer has adequately responded to any AI queries and there are no PEPs or other elevated risk factors involved, then no sign-off may be required. However, it is open to each AI to adopt a more conservative approach to senior management sign-off, taking into account its own circumstances and risks.

[24] An AI may also consider whether it needs additional staff resources. In this respect, paragraph 2.5(e)(i) of the AML/CFT Guideline requires each AI to take into account, as part of its institutional risk assessment, "*the nature, scale and quality of available ML/TF risk management resources, including appropriately qualified staff with access to ongoing AML/CFT training and development*". As such, in addition to training, an AI may consider whether it requires additional staff (specialised in dual-use goods or other areas considered necessary) to support the implementation of its AML/CFT Systems to Relevant Risks.

Record-keeping

Irrespective of the approach taken, AIs should ensure they document their approach on dual-use goods and maintain appropriate records in accordance with Chapter 8 of the of the AML/CFT Guideline.