ALT Capital Limited

Anti-Money Laundering and Counter-Financing of Terrorism Policy & Procedures for Trust & Company Service Providers in Hong Kong (“Policy”)

Version 1.0- Last Updated 20 May 2024

Table of Contents

FOREWORD

In accordance with the laws of the Hong Kong in respect of the prevention of money laundering, terrorism financing, and the proliferation of nuclear weapons and other weapons of mass destruction, the Company hereby sets out the following policy and procedures.

As a trust company, the Company is aware of the risks of, and vulnerabilities to, financial crime, and the need to ensure business is conducted in a legal and compliant manner. The position of Hong Kong as an international financial and trading centre, the sixth-largest banking centre in terms of external transactions and the fourth-largest foreign exchange trading centre adds to the worldwide scrutiny of business conducted in the city.

It is incumbent upon all personnel to read and understand this document for the effective performance of their duties to the Company in playing its role in preventing such criminal activities and/or allowing criminals to use the Company's services to criminal ends.

This document should be read in conjunction with group Code of Conduct, Anti-Corruption & Bribery, and other associated Compliance policies, and the staff handbook.

A copy of this document shall be made available to all personnel. If any part of this document is unclear to any member of staff and any sub-contractors used by the Company, you are reminded to refrain from making your own interpretation, instead it is recommended that you speak to your line manager, or a member of the Company's Compliance team.

I. Introduction to the Policy

A. Basic Principles

A.1 Background

Hong Kong, SAR is a member of the Financial Action Task Force ("FATF"), an inter-governmental body established in 1989 which sets standards on combatting money laundering ("ML"), terrorism financing ("TF") and proliferation financing ("PF") for governments, financial institutions, and designated non-financial businesses and professions ("DNFPB"), a term which, among others, includes trust and company service providers ("TCSP").

As part of its commitment to the 40 Recommendations of FATF, Hong Kong, SAR has promulgated laws requiring relevant financial businesses to take all reasonable measures to instigate policies, procedures, and safeguards to prevent and mitigate the risks of money laundering, terrorism financing, and proliferation financing.

The Companies Registry ("CR") is the regulatory body responsible for the supervision and regulation of TCSPs and for monitoring compliance with anti-money laundering regulations. To this end, CR issues guidelines on policies and procedures, and issues other rules and statements of guidance and principle.

The Anti Money Laundering and Counter Terrorist Financing (Financial Institutions) Ordinance ("AMLO") and the Guideline on Compliance of Anti-Money Laundering and Counter-Terrorist Financing Requirements for Trust or Company Service Providers ("AMLG") provide that, as a TCSP, the Company should take all reasonable measures to ensure that proper safeguards exist to mitigate the risk of ML/TF and to prevent any contravention of the requirements under the AMLO. In doing so, it is the responsibility of every TCSP to put in place its own policies, procedures and controls to mitigate the risks of ML/TF.

Therefore, the Company has adopted the policies and procedures set out in this Policy in order to ensure its compliance with the relevant regulatory regime in Hong Kong.

A.2. Money Laundering, Terrorist Financing, and Proliferation Financing

A.2.1. What is Money Laundering?

Money laundering is the act of engaging in specific financial transactions with the intention of concealing the identity, source and/or destination of funds. Money launderers act to alter the identity of the source of illegally obtained money to create the appearance that it originates from legitimate sources.

Three stages of the process of money laundering are identified during which there may be numerous transactions for the Company to identify money laundering activities:

(a) Placement - the physical disposal of cash proceeds derived from illegal activities, e.g. by giving this money to an intermediary who is already legitimately taking in large amounts of cash.
(b) Layering – separation of illicit proceeds from their sources by creating complex layers of financial transactions designed to disguise the financial sources of the funds, subvert the audit trail, and provide anonymity.
(c) Integration – creating the impression of apparent legitimacy of criminally derived wealth. In the event of successful layering processes, integration schemes effectively return the laundered proceeds back into the financial system as if the proceeds are from legitimate business actions.

A.2.2. What is Terrorist Financing?

Terrorists or terrorist organizations require financial support in order to achieve their aims. Terrorist financing refers to the carrying out of transactions involving funds or property that are owned or controlled by terrorists or terrorist organizations or transactions that are linked to, or likely to be used in, terrorist activities.

Like the three stages of money laundering, there are three defined stages in terrorist financing, namely:

(a) Collection – in contrast to money laundering, funds or assets can be collected from entirely legitimate sources.
(b) Movement – either physically moving goods or assets across national borders and/or using simple and/or complex financial transactions and/or markets to obscure the trail from the origin to the destination of funds.
(c) Use – putting the funds to use in purchasing materials and services and other non-tangible assets and items to carry out terrorist activities. This could include buying black market weapons and materials, to seemingly legitimate ends such as paying rent, utilities, public & private transportation costs.

Terrorist groups, regardless of whether funds or assets are from illicit or legitimate sources, are constantly seeking new ways to be able to collect, move, and use funds and assets without attracting the attention of the authorities.

A.2.3. What is Financing of proliferation of weapons of mass destruction?

Financing of proliferation of weapons of mass destruction (‘PF”) is the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical, radiological or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for illegitimate purposes), in contravention of national laws or, where applicable, international obligations.

Measures for countering proliferation financing are implemented at supranational and national levels, for example through the implementation of targeted financial sanctions, and general economic and sectoral sanctions.

A.3 Anti-Money Laundering Legislation in Hong Kong

Money laundering is a criminal offence and the Company and its employees are obliged to report suspected instances of money laundering. Any employee who knows or suspects that a customer/ client is engaged in money laundering must notify the Money Laundering Reporting Officer ("MLRO") immediately who will be responsible for contacting the relevant authorities.

A.3.1 United Nations (Anti-Terrorism Measures) Ordinance ("UNATMO")

This Ordinance implements the mandatory elements of the United Nations Security Council Resolution 1373 to counter terrorism and the Financial Action Task Force on Money Laundering (FATF) 8 Special Recommendations on terrorist financing. In particular:

(a) s6 empowers the Secretary for Security to freeze suspected terrorist property;
(b) s7 prohibits the provision or collection of property for use to commit terrorist acts;
(c) s8 prohibits any person from making available or collecting or soliciting property or financial (or related) services for terrorists and terrorist associates;
(d) s8A prohibits any person from dealing with any property knowing that, or being reckless as to whether, the property is specified terrorist property or property of a specified terrorist or terrorist associate; and
(e) s11L prohibits any person from providing or collecting any property to finance the travel of a person between states with the intention or knowing that the travel will be for a specified purpose, i.e. the perpetration, planning or preparation of, or participation in, one or more terrorist acts (even if no terrorist act actually occurs); or the provision or receiving of training that is in connection with the perpetration, planning or preparation of, or participation in, one or more terrorist acts (even if no terrorist act actually occurs as a result of the training).

A.3.2 Drug Trafficking (Recovery of Proceeds) Ordinance ("DTROP")

This Ordinance contains provisions for the investigation of assets that are suspected to be derived from drug trafficking activities, the freezing of assets on arrest and the making of confiscation orders upon conviction.

A.3.3 Organized and Serious Crimes Ordinance ("OSCO")

This Ordinance gives the police and customs the ability to investigate the financial transactions connected to a wide range of crimes, allows the confiscation of the proceeds of these crimes and creates an offence of money laundering in relation to the proceeds of indictable offences.

A.3.4 Anti Money Laundering and Counter Terrorist Financing (Financial Institutions) Ordinance ("AMLO")

This Ordinance makes it an offence to fail to identify and verify clients of financial institutions including the Company.

A.3.5 United Nations Sanctions Ordinance ("UNSO")

The UNSO provides for the imposition of sanctions against persons and against places outside the People's Republic of China arising from Chapter 7 of the Charter of the United Nations. Most UNSCRs are implemented in Hong Kong under the UNSO.

A.3.6 The Weapons of Mass Destruction (Control of Provision of Services) Ordinance ("WMD(CPS)O")

The WMD(CPS)O controls the provision of services that will or may assist the development, production, acquisition or stockpiling of weapons capable of causing mass destruction or that will or may assist the means of delivery of such weapons. Section 4 of WMD(CPS)O prohibits a person from providing any services where he believes or suspects, on reasonable grounds, that those services may be connected to PF. The provision of services is widely and includes the lending of money or provision of other financial assistance.

A.4 Offences Under the Laws

A person commits an offence if he deals with a piece of property that he knows or has reasonable grounds to believe represents the proceeds of drug trafficking.

The maximum penalty is 14 years imprisonment and a HK$5 million fine.

Dealing with property means: -

(a) Receiving or acquiring the property;
(b) Concealing or disguising the nature, source, location, disposition, movement or ownership of the property;
(c) Disposing of or converting the property;
(d) Bringing the property into or taking it out of Hong Kong; or
(e) Using the property to borrow money or as security.

A person who knows or suspects that any property represents the proceeds of or was used in connection with or will be used in connection with drug trafficking must disclose that information either to the police or in accordance with his/her employer's procedures. Failure to disclose is punishable by imprisonment of 3 months and a fine of HK$50,000.

It is an offence for any person who knows or suspects that such a disclosure has been made to disclose to anyone else any matter that might prejudice any investigation that might result from the disclosure ('tipping off"). This is punishable by imprisonment for 3 years and a fine of HK$500,000.

The Company may receive restraint orders and charging orders on the property of a defendant of a drug trafficking offence or an offence under OSCO. The Company is required to co-operate with these orders and failure to do so is an offence.

It is an offence to make available, directly or indirectly, any funds, or other financial assets, or economic resources, to, or for the benefit of, individuals and entities designated by the UNSC (a designated person) or entity, as well as those acting on their behalf, at their direction, or owned or controlled by them; or to deal with any funds, other financial assets or economic resources belonging to, or owned or controlled by, such persons and entities, except under the authority of a licence granted by the Chief Executive.

A person with knowledge or suspicions of terrorist property must report this to an authorised officer (e.g. the police). Failure to disclose is an offence punishable by imprisonment and a fine.

Failure to comply with the various Anti-Money Laundering and Counter Financing of Terrorism ("AML/CFT") laws or the AMLG in Hong Kong may affect the fitness and properness to hold a license in Hong Kong.

II. AML/CFT Framework in Hong Kong

A. Culture & Values

The Company takes reasonable measures to ensure that proper safeguards exist to mitigate the risks of ML and TF and to prevent a contravention of any requirement under the AMLO.

The Company has established and implements adequate and appropriate AML/CFT policies, procedures and controls taking into account factors including types of customers, products and services offered, delivery channels and geographical locations involved.

B. Roles & Responsibilities

B.1 Board of Directors

The Board of Directors has the ultimate responsibility for the conduct, operations and financial soundness of the Company. The Board works with senior management to achieve the objective of a soundly and efficiently run organization, and senior management is accountable to the Board. The Board shall appoint a Compliance Officer and a Money Laundering Reporting Officer.

Any member of the Board, regardless of whether he or she has an executive or non-executive role, has a duty to exercise independent judgement in relation to the execution and delegation of the Board's powers.

The Board retains responsibility for delegated decisions.

B.2 Senior Management

Senior Management includes, but is not limited to:

(a) The Board of Directors
(b) Nominated Officers, including the Compliance Officer ("CO") and Money Laundering Reporting Officer ("MLRO")
(c) Managers-in-Charge

The Company's senior management periodically conducts risk assessments to evaluate any ML/TF risks the Company may face and how these risks are to be managed. Risk assessments are conducted on at least an annual basis.

The roles of Compliance Officer and Money Laundering Reporting Officer may be assumed by the same person.

B.2.1 Compliance Officer and Money Laundering Reporting Officer

In order that the Compliance Officer and Money Laundering Reporting Officer can discharge their responsibilities effectively, senior management shall, as far as practicable, ensure that the Compliance Officer and Money Laundering Reporting Officer are:

(a) appropriately qualified with sufficient AML/CFT knowledge

(b) subject to constraint of size of the Company, independent of all operational and business functions;
(c) normally based in Hong Kong;
(d) of a sufficient level of seniority and authority within the company;
(e) provided with regular contact with, and when required, direct access to senior management to ensure that senior management is able to satisfy itself that the statutory obligations are being met and that the business is taking sufficiently robust measures to protect itself against the risks of ML/FT;
(f) fully conversant in the Company`s statutory and regulatory requirements and the ML/FT risks arising from the Company's business;
(g) capable of accessing, on a timely basis, all available information (both from internal sources such as customer due diligence records and external sources such as circulars from regulatory authorities ("RAs"); and
(h) equipped with sufficient resources, including staff and appropriate cover for the absence of the CO and MLRO (i.e. an alternate or deputy CO and MLRO who should, where practicable, have the same status).

Compliance Officer

The Compliance Officer ("CO") shall act as a focal point for the oversight of all activities relating to the prevention and detection of ML/TF, and providing support and guidance to the senior management to ensure that ML/TF risks are adequately identified, understood and managed. The CO shall assume responsibility for, but not limited to:

(a) developing and/or continuously reviewing AML/CFT Systems, to ensure they remain up-to-date, meet current statutory and regulatory requirements and are effective in managing ML/TF risks
(b) overseeing all aspects of AML/CFT Systems which include monitoring effectiveness and enhancing the controls and procedures where necessary;
(c) communicating key AML/CFT issues with senior management, including, where appropriate, significant compliance deficiencies; and
(d) ensuring AML/CFT staff training is adequate, appropriate and effective.

Money Laundering Reporting Officer

The Money Laundering Reporting Officer ("MLRO") shall be the central reference point for reporting suspicious activities to the Joint Financial Intelligence Unit of the Hong Kong Police Force and Hong Kong Customs ("JFIU"). The MLRO reports directly to the Board of Directors and shall have unfettered access to all business lines, support departments and information necessary to appropriately perform the function. Principal functions performed are expected to include, but not limited to:

(a) reviewing internal disclosures and exception reports and, in light of all available relevant information, determining whether or not it is necessary to make a report to the JFIU;
(b) maintaining all records related to such internal reviews; and
(c) providing guidance on how to avoid 'tipping off' if any disclosure is made.

B.3 Business Conducted Outside of Hong Kong

The Company has no branch companies or subsidiaries outside of Hong Kong.

The Company is part of a group of companies, where affiliated companies conduct similar activities outside of Hong Kong. To the best of the Company's knowledge, all such companies operate under similar policies and procedures.

B.4 Compliance and Audit Function

The Company shall establish an independent compliance and audit function with a direct line of communication to the senior management. The compliance and audit function shall regularly review the Company's AML/CFT systems to ensure its effectiveness. Alternatively, the Company could choose a reliable and professional third-party to conduct independent compliance audit.

B.5 Employee Screening

Before a staff is hired as an employee, the Company shall conduct adequate and appropriate the screening.

III. Customer Due Diligence Policy

A. Risk-Based Approach

The Company employs a Risk-Based Approach ("RBA") at an institutional level. Risks faced at an institutional level broadly fall into four categories:

- Country / Geographic
- Customer
- Product or Service
- Transaction or Delivery channel

Consideration is given to the Hong Kong National Risk Assessment: a periodic review of the threats to, and vulnerabilities of, the Territory in respect of money laundering and terrorist financing.

The ML/TF risk to TCSPs is "Medium High" as per the National Risk Assessment framework. The overriding threat and vulnerability of the sector is the abuse of shell companies and their bank accounts as repositories of crime proceeds. This can be both domestically within Hong Kong and as part of wider cross-border and/or international network or syndicate.

The Company shall apply the RBA to identify and assess the ML/TF risks that may arise due to the development of new products or business lines, as well in respect of the use or development of technology for both existing and new products and business lines. This shall be done prior to launch of any such new products or business lines.

A.1 Risk-Based Approach Applied to Customer Due Diligence

The Company extends the RBA to customer due diligence ("CDD"). Prior to commencing business activities with new customer, the Company shall perform CDD and assign a risk rating to each customer of LOW, MEDIUM, or HIGH. The outcome of this assessment shall determine the level of mitigation required for each customer as well as the frequency of the regular review.

A.1.1 Timing of Customer Due Diligence

CDD shall be carried out:

- at the outset of a business relationship
- before performing any occasional transaction:
    (a) equal to or exceeding an aggregate value of HK$120,000, whether carried out in a single operation or several operations that appear be linked; or
    (b) a wire transfer equal to or exceeding an aggregate value of HK$8,000, whether carried out in a single operation or several operations that appear to be linked;

- when suspects that the customer or the customer's account is involved in ML/TF; or
- when doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or for the purpose of verifying the customer's identity.

Furthermore, each customer is subject to ongoing and regular review. The timing of regular reviews shall be subject to the risk rating.

- Low – subject to regular review every five years
- Medium – subject to regular review every three years
- High – subject to annual regular review

A.1.2 Risk Factors in Customer Due Diligence

The Company considers, among others, the following key factors in determining the risk rating for its customers:

- Type & Profile: e.g. natural vs legal persons; associated parties
- Geographic Risk: e.g. country of incorporation or nationality/citizenship of natural persons; countries of major operations & sources of revenue
- Activities & Nature of Business
- Sources of funds and wealth
- Reputation: e.g. adverse media; tax issues
- Behaviour: e.g. unusual requests; reticence to provide CDD information

A.1.3 Due Diligence Conducted by Intermediaries

Note, reliance on intermediaries does not apply to:

- Outsourcing or agency relationships, i.e. where the agent is acting under a contractual arrangement with the Company to carry out its CDD function. In such a situation the outsourced party or agent is to be regarded as synonymous with the Company (i.e. the processes and documentation are those of the Company itself); and
- Business relationships, accounts or transactions between TCSP licensees for their clients.

The Company may have cause to place reliance on intermediaries to perform due diligence. In such instances the Company shall request written consent from the intermediary that it agrees to acting in the capacity and that it shall on request provide a copy of any document, or a record of any data or information, obtained by the intermediary in the course of carrying out the CDD measures.

The Company shall obtain, and keep on record, proof of the intermediary's eligibility to perform the role. Eligible intermediaries in Hong Kong are:

- An authorized bank in Hong Kong
- An SFC licensed corporation in Hong Kong
- An authorized insurer, an appointed insurance agent or an authorized insurance broker in Hong Kong

- An accounting professional
- An estate agent
- A legal professional
- Another TCSP licensee

For intermediaries outside Hong Kong, the above list shall apply provided the entity is registered in a jurisdiction that the Company has deemed to uphold standards AML/CFT equivalent to those in Hong Kong.

The Company shall, from time-to-time, conduct sample checks on CDD information collected by intermediaries by requesting copies of the underlying documentation collected by the intermediary.

B. Subjects of Customer Due Diligence

CDD shall be conducted on the facing customer. In applying CDD measures to legal persons, relevant parties shall also be identified and verified. These include:

- Beneficial owners, i.e. those natural persons ultimately holding greater than or equal to 25% of the facing customer either directly or deemed (in the case of trusts the beneficial owners shall be deemed to be the trustees and named beneficiaries or class of beneficiaries, and no threshold applies)
- Shareholders holding greater than or equal to 25% either directly or deemed
- All Directors shall be identified and the number of Directors to be verified shall be determined on a risk-based approach
- Account signatories
- In the case of trusts: trustees, beneficiaries, settlors

If the facing customer is a natural person, but in the course of CDD it is determined that the individual is a front person for another natural or legal person, the Company shall consider that person to be a beneficiary and shall perform CDD accordingly.

C. Simplified Due Diligence in Respect of Beneficial Owners

Under certain circumstances the AMLG permits the application of Simplified Due Diligence (“SDD”), provided no high-risk factors pertain to the customer.

The Company shall exercise its right to apply SDD.

The Company shall apply, and document the rationale for applying, SDD in the case of a customer which falls under one of the following categories.

- an Financial Institution (“FI”) as defined in the AMLO;
- an institution that-
  (a) is incorporated or established in an equivalent jurisdiction;
  (b) carries on a business similar to that carried on by an FI as defined in the AMLO;
  (c) has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2 of the AMLO; and

(d) is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the RAs;

- a corporation listed on any stock exchange;
- an investment vehicle where the person responsible for carrying out measures that are similar to the CDD measures in relation to all the investors of the investment vehicle is-
  (a) an FI as defined in the AMLO;
  (b) an institution incorporated or established in Hong Kong, or in an equivalent jurisdiction that-
    - has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2 of the AMLO; and
    - is supervised for compliance with those requirements.
- the Government or any public body in Hong Kong; or
- the government of an equivalent jurisdiction or a body in an equivalent jurisdiction that performs functions similar to those of a public body.

The Company shall apply, and document the rationale for applying, SDD in the case of a solicitor or a firm, and meeting the following categories:

- the client account is kept in the name of the customer;
- moneys or securities of the customer's clients in the client account are mingled; and
- the client account is managed by the customer as those clients' agent.

Enhanced Due Diligence

In the event of an automatic high-risk factor, or of the combination of risk factors resulting in a risk rating of HIGH, the Company shall apply enhanced due diligence ("EDD").

Customer rated as HIGH risk require final sign off by a senior manager.

D. CDD Not Completed Prior to Commencement of Business

The Company shall always endeavour to complete CDD verification prior to the commencement of business. However, it is acknowledged that in certain circumstance, especially within the securities transaction and life insurance businesses, this is not always possible. Senior Management shall understand and document the reasons behind any delay to the completion of CDD prior to commencement of business.

The customer and all known associated parties must be screened prior to acceptance of such a delay in verification.

CDD measures should be completed with 30 days of the commencement of business.

If CDD measures remain incomplete after 60 working days, the Company must suspend business relations and refrain from carrying out further transactions for the customer;

If CDD measures remain incomplete after 120 working days, then the Company must terminate the business relationship and consider if the circumstances are suspicious as to warrant the filing of a suspicious activity report ("SAR").

E. Third-Party Payments

All third-party payments must be approved in advance by Senior Management, who may approach the CO / MLRO for further advice. The Company must identify and verify the entity or individual making or receiving the third-party payment and establish the relationship between the third-party and the customer. The Company shall also enquire as to the rationale behind the third-party payment.

F. Numbered, Anonymous or Fictitious Accounts

The Company shall not allow the opening or maintenance of anonymous accounts, nor allow for accounts under fictitious names for any new or existing customers. Such requests shall be declined and reported to senior management and the MLRO to decide if a suspicious activity report is warranted. Where numbered accounts exist, the Company shall properly identify and verify the identity of the customer.

G. Customers Issuing Bearer Shares

The Company shall not accept any customer which issues bearer shares, nor establish a company on behalf of a customer where bearer shares would be permitted.

H. Nominee Shareholders

For a customer identified to have nominee shareholders in its ownership structure, the Company must identity and verify the nominees, and the persons on whose behalf they are acting, as well as the details of arrangements in place, in order to determine who the beneficial owner is.

I. Declined Business

The Company reserves the right to refuse business. The Company shall always refuse business that it deems or suspects to be illegal in origin or intent.

Where a prospective customer is hesitant or fails to provide adequate CDD documentation (including the identity of any beneficial owners or controllers), consideration shall be given to filing an SAR. Where an attempted transaction gives rise to knowledge or suspicion of ML/TF/PF, that attempted transaction shall be reported to the JFIU.

IV. Onboarding – Customer Procedure

A. Introduction

This chapter sets out the procedures for onboarding new customers. Should there still be existing customers where customer due diligence ("CDD") has not been carried out, the following procedures should apply.

CDD shall be carried out on all new customers and each shall be assigned a risk rating of HIGH, MEDIUM, or LOW depending on the outcome of the due diligence.

B. Collection of Documentation

B.1 Reliable and Independent Source

The Company should identify and verify the customer by reference to documents, data or information provided by a reliable and independent source:

(a) a governmental body;
(b) the CR or any other RA;
(c) an authority in a place outside Hong Kong that performs functions similar to those of the CR or any other RA;
(d) a digital identification system that is reliable and independent source that is recognized by the Registrar[1]; or
(e) any other reliable and independent source that is recognized by the CCE.

In summary types of reliable data as defined in the AMLO are as follows:-

(a) For individuals physically in Hong Kong:-
- Hong Kong ID card; or
- Valid travel document for non–residents (Macau / Taiwan / sailors);

(b) For non-resident individuals not physically in Hong Kong:-
- Valid international passport;
- Current national ID card or drivers licence with photo;

(c) For minors born in Hong Kong without ID card:-
- Birth certificate;

(d) For corporate customers:-
- Company registry search in place of incorporation; or
- Full company search (not an extract).

[1] As of 1 June 2023 the only such system is the iAM Smart system as launched by HKSARG

B.2 Documentary Standards

Documents should be provided in either original form or as certified true copies. Copies should be clearly legible and photographs visible, i.e. the facial features should be clear and not blacked out by low quality copying.

Documents with a given expiry date must be valid at the time of collection. Documentary proof of address should be no older than 3 months old at the time of collection.

Other documentary evidence, e.g. registry submissions used for verifying directors, proof of ownership, etc, should be no older than 12 months, unless it becomes apparent that new information supersedes that given in the document. For example, an Annual Return may show the names of the directors, but the list of documents submitted to the registry shows a new director had been added since the submission of the Annual Return.

The modern trend towards e-bills means that not all customers will have a printed proof of address. Where possible, customers should supply versions of e-bills which utilities and banks provide in secured PDF format.

B. 3 Certification

The Company is liable for failure to carry out prescribed CDD even if a third party has been involved and therefore must exercise caution when considering accepting certified copy documents, especially where such documents originate from a country perceived to represent a high risk, or from unregulated entities in any jurisdiction.

Before the Company accepts certification in the case of non-face to face verification, it must ensure:-

(a) The certifier has actually have seen the original documentation. If this is not clear, then the Company should contact the certifier to check this.
(b) The certifier is a suitable person.
(c) The certifier must sign and date the copy document (printing his/her name clearly in capitals underneath) and indicate clearly his/her position or capacity on it.
(d) The certifier must state that it is a true copy of the original (or words to similar effect).
(e) The documents must be so certified in the last 6 months.

Suitable persons for certifying verification of identity documents include:

(a) A Hong Kong bank, Securities and Futures Commission ("SFC") licensed firm or insurance company or broker regulated by the IA or the equivalent types of licensed firms[2], in other FATF countries ;
(b) An accounting professional, a legal professional, a notary public, a chartered secretary or other appropriate professional person;

[2] specified in section 18(3) of Part 2 of Schedule 2 to the AMLO

(c) A member of the judiciary in Hong Kong or an equivalent jurisdiction;
(d) An officer of an embassy, consulate or high commission of the country of issue of documentary verification of identity; and
(e) A Justice of the Peace in Hong Kong or an equivalent jurisdiction.

The certifier should sign and date the copy of the document, print his/her name clearly underneath, clearly indicate his/her position or capacity together with a contact address and phone number.

Employees, or employees of third parties delegated to perform CDD measures, may copy original documents provided to them. When certifying documents, the certifier should print their name and title, alongside the words “I have sighted the original document” (or similar) and sign and date the document. A digital signature for a copy scanned directly to a hard drive should also carry the same information.

B.4 Foreign Language Materials

Documents which are not in the English or are in non-Chinese language must be translated by a suitably qualified translator. This does not have to be a professional out-of-house translator but may be conducted by an employee proficient in the language in question. The translator should highlight and translate the pertinent information and provide their name, position, date of translation, and the type and source of the document being translated (e.g. Hong Kong Electric electricity bill).

C. Non-Face-to-Face Onboarding

The AMLO does not prohibit non-face-to-face onboarding; however, the practice does pose higher risks of forgery and impersonation. If a customer has not been physically present for identification purposes, the Company must carry out at least one of the following additional measures to mitigate the risks posed:

(a) further verifying the customer’s identity on the basis of documents, data or information;
(b) taking supplementary measures to verify information relating to the customer that has been obtained by the company; or
(c) ensuring that the first payment made into the customer’s account is received from an account in the customer’s name with an authorised bank in Hong Kong or a bank operating in an equivalent jurisdiction to Hong Kong that has measures in place to ensure compliance with requirements similar to those in the AMLO and is supervised for compliance with those requirements by a banking regulator in that jurisdiction.

If a customer’s identity has been verified on the basis of data or information provided by a digital identification system that is recognized by the Registrar, then no additional measures as prescribed above needs to be taken.

D. Conducting Customer Due Diligence Analyses

The aim of conducting customer due diligence is to ascertain the potential risk factors a customer poses to a company. This is achieved by understanding the nature of the

customers, the business and geographical spheres in which it operates, and the entities and individuals who benefit from its activities.

D.1 Preliminary Customer Risk Rating ("CRR")

Unless there are clear indicators that a customer is eligible for Simplified Due Diligence, or that a customer will have to be subject to Enhanced Due Diligence, the initial indicative risk rating for all new customers shall be MEDIUM.

D.2 Simplified Due Diligence ("SDD")

Under certain circumstances, the GAML allows for the performance of Simplified Due Diligence (SDD) when lower risks are identified. This can only be carried out when no HIGH-risk factors present themselves, including jurisdictional risk factors. When performing SDD, the rationale for opting for SDD must be included in the file.

As per company policy only the following institutions are eligible for SDD:

(a) customer risk factors:

- Another financial institution regulated or supervised in Hong Kong or a country equivalent to Hong Kong;
- A listed company;
- Financial Institution ("FI") as defined in the AMLO, or other FI incorporated or established in an equivalent jurisdiction and is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF; or
- a collective investment scheme authorised for offering to the public in Hong Kong or in an equivalent jurisdiction.

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

- a provident, pension, retirement or superannuation scheme (however described) that provides retirement benefits to employees, where contributions to the scheme are made by way of deduction from income from employment and the scheme rules do not permit the assignment of a member's interest under the scheme;
- an insurance policy for the purposes of a provident, pension, retirement or superannuation scheme (however described) that does not contain a surrender clause and cannot be used as a collateral; or
- (a life insurance policy in respect of which:
  - an annual premium of no more than HK$8,000 or an equivalent amount in any other currency is payable; or
  - a single premium of no more than HK$20,000 or an equivalent amount in any other currency is payable.

(c) country risk factors:

- countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT Systems; or
- countries or jurisdictions identified by credible sources as having a lower level of corruption or other criminal activity.

E. Identification & Verification

E.1 General Definition

The general principle of identification and verification ("ID&V") is to understand who the individual or entity is and confirm that understanding via a set of independent reliable documents or other information.

E.2 Identification & Verification of Natural Persons

The following information shall be identified and verified in respect of natural persons.

(a) Full name
(b) Date of birth
(c) Place of birth
(d) Nationality
(e) Unique identification number (e.g. identity card number or passport number) and document type.

Documents include:

(a) Hong Kong identity card or other national identity card;
(b) valid travel document (e.g. unexpired passport); or
(c) other relevant documents, data or information provided by a reliable and independent source (e.g. document issued by a government body).

Verification of the customers name, date of birth, nationality should be carried out against a government issued ID or passport. For residents of Hong Kong born in Hong Kong (code AZ), Macau (code AW), or China (code AX), this can be with their Hong Kong ID card, where the code indicates the country of birth.

In certain circumstances, the Company may be required to obtain the residential address information of a customer. The Company should communicate clearly to the customer the reasons of requiring verification of address.

E.3 Identification & Verification of Legal Persons

ID&V of legal persons is dependent upon the type of legal person. This can include companies, bodies corporate, foundations, anstalt, partnerships, associations or other relevantly similar entities.

Note that not all jurisdictions have equivalent documentation, so allowances should be made, under reasonable circumstances, when requesting documents pertaining to jurisdictions outside those with which an employee or delegate is already familiar.

The Company must collect the following information about the customer: -

(a) Full name of the company
(b) Date and place of incorporation, establishment or registration;
(c) Registration or incorporation number; and
(d) Address of registered address in place of incorporation and business address

E.4 Corporations

Corporations, other than those listed on a stock exchange in an equivalent jurisdiction, shall be identified and verified against their founding or licencing documents, or against records from the company registry in which the corporation is incorporated. Documents include:

(a) Certificate of Incorporation / Registration
(b) Certificate of Incumbency
(c) Business Registration Certificate
(d) Company Registry Extract (e.g. ACRA, Handelsregister, Zefix, K-Bis, etc.)
(e) Certificate of Good Standing
(f) Memorandum or Articles of Associations

HONG KONG ONLY: For Hong Kong companies, the Articles of Association (or equivalent for non-Hong Kong corporations) are effectively a mandatory document, in order to show the powers that bind the company.

The nature of business should, where possible, be taken from independent documents; however, in some countries this is not a requirement when registering a business, in which case public sources should be used. Where this is still not possible, confirmation from the customers shall be necessary. This should be given by a director, or from a person purporting to act on behalf of the company where a director is also included in the correspondence.

I. Signatories

The customers should provide a board resolution stating the names of the signatories and a specimen signature.

All signatories to the account should be identified and verified as per the instructions for natural persons, although no proof of source of funds (or wealth in the event of HIGH risk) is required for these individuals, unless they are also beneficial owners.

II. Beneficial Owners

The AMLG defines a beneficial owner as a natural person holding a stake in the corporation equal to or greater than 25%. Beneficial owners shall be subject to ID&V as per the procedures for natural persons.

In order to identify beneficial owners, the due diligence analyst should seek to understand the ownership structure of the corporation using information from registries or an organization chart prepared and signed by a director of the corporation. Using a top down approach, each natural person owning equal to or greater than a deemed 25% shall be deemed a beneficial owner. Where a legal form other than a corporation

is encountered in the ownership structure, the method for assessing beneficial owners specific to that form shall be applied on a risk-based approach.

III. Directors / Controlling Persons

All directors should be identified by obtaining a list of their names, ideally with nationality and domicile to aid the screening process, and verified against an independent document, such as a registry filing or company register extract. Where this is not possible, a notarised list can be accepted.

ID&V of directors or controlling persons shall be done on a risk-based approach. In situations where the requisite number of directors are not also signatories of the account, at least one director should be subject to ID&V for LOW-risk customers and two directors for MEDIUM- and High-risk customers.

E.5 **Corporations Listed on Stock Exchange in an Equivalent Jurisdiction**

For corporations listed on a stock exchange in an equivalent jurisdiction, CDD material may be gathered from public sources. As a minimum, proof of listing from the stock exchange website should be collected, in addition to the following:

(a) Most recent Annual Report
(b) List of directors

I. Signatories

The customers should provide a board resolution stating the names of the signatories and a specimen signature.

All signatories to the account should be identified and verified as per the instructions for natural persons, although no proof of source of funds (or wealth in the event of HIGH risk) is required for these individuals, unless they are also beneficial owners.

II. Beneficial Owners

For corporations listed on a stock exchange in an equivalent jurisdiction, where there are no high-risk factors, it is not required to ID&V beneficial owners. However, if the information provided on the corporation contains the names of shareholders with a greater than 25% share in the company, these shareholders should be screened against the relevant sanctions lists.

In the event of high-risk factors, beneficial owners holding greater than or equal to 25% should be identified using public sources, e.g. stock exchange shareholder lists, company annual report, Bloomberg Terminal report, and be screened as per screening procedures.

III. Directors / Controlling Persons

All directors or other controlling individuals (e.g. CEO, CFO, Managing Director) should be identified by obtaining a list of their names, ideally with nationality and domicile to aid the screening process. This can be obtained from public sources.

ID&V of directors or controlling persons shall be done on a risk-based approach. In situations where the requisite number of directors are not also signatories of the account, at least one director should be subject to ID&V for LOW-risk customers and two directors for MEDIUM- and High-risk customers.

E.6 Partnerships

Partnerships shall be identified and verified against their founding or licencing documents, or against records from the company registry of the jurisdiction in which the partnership is founded. Documents include:

(a) Partnership Agreement or deed
(b) Certificate of Incorporation / Registration
(c) Certificate of Incumbency
(d) Certificate of Good Standing
(e) Business Registration Certificate
(f) Company Registry Extract (e.g. ACRA, Handelsregister, Zefix, K-Bis, etc.)

I. Signatories

The customers should provide a board resolution stating the names of the signatories and a specimen signature.

All signatories to the account should be identified and verified as per the instructions for natural persons, although no proof of source of funds (or wealth in the event of HIGH risk) is required for these individuals, unless they are also beneficial owners.

II. Beneficial Owners

In the case of a partnership the beneficial owners are the partners. The partners should be identified with reference to the Partnership Agreement. Moreover, an understanding of the liability of the partners should be considered, e.g. partners whose liability is limited to their capital contribution vs partners with unlimited liability.

As a minimum standard at least two partners and the general partner must be identified and verified; however, the beneficial ownership threshold still applies.

III. Directors / Controlling Persons

Where the partnership has directors who are not partners, all directors should be identified by obtaining a list of their names, ideally with nationality and domicile to aid the screening process, and verified against an independent document, such as a registry filing or company register extract. Where this is not possible, a notarised list can be accepted.

ID&V of directors or controlling persons shall be done on a risk-based approach. In situations where the requisite number of directors are not also signatories of the account, at least one director should be subject to ID&V for LOW-risk customers and two directors for MEDIUM- and High-risk customers.

E.7 Trusts

In contrast to the legal persons in previous sections, due diligence on trusts requires deeper background into the nature and workings of the trust. The trust should be identified and verified using the Deed of Trust or similar document.

The Company should seek to understand if the trust is a revocable or non-revocable / irrevocable trust. The core difference is that in the case of an irrevocable trust the terms are set at the time of the drawing up of the Deed of Trust and cannot be changed except in exceptional circumstances, whereas in the case of a revocable trust, the settlor can change the terms at any time and withdraw any funds or assets placed under the care of the trust.

With respect to related parties, the Company should identify:

(a) The settlor
(b) The trustee(s)
(c) The protector (if any)
(d) The enforcer (if any)
(e) The beneficiaries or class of beneficiaries
(f) Any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership)

The Company must obtain the following identification information:-

(a) the name of the trust or legal arrangement;
(b) date of establishment/settlement;
(c) the jurisdiction whose laws govern the arrangement, as set out in the trust instrument;
(d) the identification number (if any) granted by any applicable official bodies (e.g. tax identification number or registered charity or non-profit organisation number);
(e) address of registered office (if applicable)

Verification documents include:

(a) Deed of Trust
(b) Reference to an appropriate register in the relevant country of establishment;
(c) Written confirmation from a trustee acting in a professional capacity; or
(d) Written confirmation from a lawyer who has reviewed the relevant instrument.

The Deed of Trust should outline the level or responsibility the relevant roles entail which will determine the need to verify the trust-related parties.

Although trusts may seem to be tax efficient vehicles, the presence of a trust should not be understood to imply tax avoidance or tax evasion. Furthermore, with respect to revocable trusts, the assets are not protected from creditors of the settlor, nor from the auspices of the relevant tax authorities.

I. Settlor

The settlor should be identified and verified using the same methods as for any other natural or legal person, up to and including beneficial owners. In the event of the settlor being deceased, the priority is to understand the initial purpose of the formation of the trust and to ascertain, as far as is reasonably possible, that the assets held under trust are not of criminal origin. Such information may be available from public sources, otherwise written statements from the trust Board, or similar, would be sufficient.

In addition, the Source of Funds should be identified as far as is reasonably practicable, bearing in mind that the original placement of funds may no longer be a matter of record.

II. Trustee

The trustee should be identified and verified using the same methods as for any other natural or legal person.

Full CDD on person purporting to act on behalf of the customer ("PPTAs"), directors, and beneficial owners is only required, when the trustee is deemed to be customer, i.e. it is apparent that it is the trustee giving directions on the use of the trust's assets.

Where the trustee and the settlor are the same natural or legal person, the CDD procedures for settlors applies.

III. Beneficiaries

An individual or a class or set or subset of beneficiaries is stated, whether the interest is possession or in remainder or reversion and whether it is defeasible or not, the Company should acquire reasonable information as to the potential influence those beneficiaries have on the distribution of the assets.

In the case of legal persons, identification and verification should follow the appropriate guidelines in these procedures for that category of legal person.

IV. Directors / Controlling Persons

ID&V of directors and/or controlling persons shall be carried out as per the general guidelines on legal persons. Ideally, the chair of the board of directors should be one of those directors identified and verified.

The Company should distinguish between those directors with executive functions and those who act in advisory and non-executive capacities. Furthermore, the voting rights of directors should be considered, e.g. rights of veto, requirement for unanimous decisions, etc.

V. Other Trust-Related Parties

Special attention must be given to any other parties who can contribute or control assets. These natural or legal persons should be identified and verified and their contributions and/or settlements be subject to transaction monitoring.

E.8 Other Legal Forms

Legal forms vary the world over and a risk-based approach must be taken to legal forms not generally known or used in the jurisdictions in which the company operates. The same basic tenets apply to those legal forms:

(a) Why has that particular legal form been adopted?
(b) Who controls the legal person?
(c) Where do the assets come from and where do they go?
(d) Who benefits from the assets and do they have any control as to how and when they receive the assets?
(e) What is the potential for money laundering, terrorist financing, proliferation financing, tax evasion (or avoidance), or any other illicit activity or the disguising of illicit activity?

E.9 Non-Profit Organizations and/or Charities

Non-Profit Organizations and charities and their associated parties should be identified and verified in accordance with their legal form, with the additional aspects considered:

(a) An explanation of the nature of the entity's purpose and operations
(b) The registered number of the charity
(c) The relevant governing or overseeing body, e.g. Charities Commission; or an independent information service provider, e.g. GuideStar

FATF guidelines suggest that NPOs pose a low TF risk; however, the opaque nature of their source of funds (charitable donations) and the impracticality of researching all donors means that CDD Analysts must be mindful of the broader connections of the NPO or charity and document their reputation and key activities, including the jurisdictions in which they are most active.

NPOs and charities should not automatically lead to a HIGH-risk rating; however, extra documentary evidence to support a risk rating should be sought. This can be sourced from reliable organs in the public domain.

In lieu of named beneficiaries, ID&V of at least 2 key controllers or directors is required.

F. Source of Funds

Source of Funds refers not only to the immediate origin of any transfer, e.g. a self - named bank account, but to how the remitter came to acquire those funds. For natural persons this would ordinarily include, but is not limited to:

(a) Salary
(b) Dividends

(c) Inheritance / legacy
(d) Returns on investments
(e) Severance payments
(f) Damages

Acceptable documents include payslips, letters from human resources, bank statements, and relevant legal documents.

For legal persons this would ordinarily include, but is not limited to:

(a) Sales revenue
(b) Commission
(c) Proceeds from sales of property & equipment
(d) New share capital

Examples of unacceptable proof of source of funds would include proceeds from insurance pay-outs, gambling, and even cryptocurrency holdings.

G. Source of Wealth

Source of Wealth refers to an individual or entity's accumulated assets over time and where it came from. In terms of individuals, salary (leading to savings) and property are the two main sources, plus investments, depending on the individual's entry point into the financial system. Since Source of Wealth for individuals is generally a factor when that person is a PEP or high net worth individual, acceptable documentary sources may be from the public domain, e.g. Forbes, Bloomberg.

For legal persons, this is generally tied to their accumulated profits and total equity and should be verified against their audited financial statements.

H. High-Risk Industries

High-risk industries subject to an automatic HIGH CRR include:

(a) Casinos
(b) Debt servicing businesses (including Factoring)
(c) Money services businesses
(d) Oil & Gas
(e) Virtual Asset Providers
(f) Weapons Manufacturers & Distributors

Other industries that deal primarily in cash transactions shall be assessed on a risk-based approach; however, employees should endeavour to obtain audited financial statements from such customers.

I. Complex Structures

Complex structures and ones involving bearer shares are often used to obscure the chain of ownership and thus the flow of funds from their origin to the ultimate beneficiary. Structures containing more than three layers, with no obvious economic

or functional purposes shall be considered high risk and enhanced due diligence shall be applied.

Where a company has multiple layers the due diligence Analyst should seek to understand the reason for the structure. Multiple layers may have perfectly legitimate uses including, but not limited to:

(a) Joint ventures
(b) Segregation of liability, especially in jurisdictions that have stringent nationality requirements on company ownership
(c) Regional & global holding companies
(d) Division of family holdings

J. Bearer Shares

Whilst many jurisdictions have abolished bearer shares, there are still jurisdictions where they can be issued. Bearer shares can be either “mobile”, i.e. a person can hold the share certificate and transfer it at will to another person (although from a legal standpoint, a bought-sold note or instrument of transfer should also be drawn up), or “immobile”, i.e. the share certificates must be held by a trustee, generally a bank, who hold the name and the address of the bearer on file.

The Hong Kong does not permit the issuance of bearer shares (also known as warrants to bearer).

Companies issuing bearer shares, other than those issued on the stock exchange in an equivalent jurisdiction, should be requested to provide confirmation from the registered agent. The confirmation should state:

(a) That an authorised/registered custodian holds the bearer shares;
(b) The identity of the authorised/registered custodian;
(c) The full name and address of the person who has the right to the entitlements carried by the share.

Beneficial owners shall be identified and verified and screened as per procedures relating to natural persons.

Where the bearer shares are mobile, i.e. they are not deposited with an authorised/registered custodian, the Company must obtain declarations prior to account opening from each beneficial owner holding more than 25% of the share capital and ID&V and screen the beneficial owners as per procedure.

The customer shall be deemed HIGH risk and shall be subject to EDD.

K. Sanctions Screening

The Company shall screen the facing customers and all associated parties (i.e. signatories, directors, shareholders, beneficial owners, trust-related parties, etc) against a consolidated sanctions database from a third-party provider. The Company uses World Check and Onfido (ID Verification) to screening its customers and their associated parties.

Hits should not be discounted based on name alone but should incorporate at least one other factor with the understanding that some factors are stronger than others. Examples of more reliable factors include:

(a) Date of birth
(b) Place of birth (not to be confused with nationality due to the potential for dual citizenship)
(c) Sex
(d) Whether the individual is in prison, or has been in prison at a time when the individual being screened could not have been in prison
(e) For corporations: place of incorporation & registration number

Further factors that can be considered in combination with another factor:

(a) Residency
(b) Nationality
(c) Career history

K.1 Screening for Politically Exposed Persons ("PEP")

The Company shall screen the names of connected individuals against a PEP database from a third-party provider. The Company uses World-Check to screening its customers and their associated parties. Employees conducting screening are advised that the results from such databases should be deemed as advisory. The absence of a hit does not mean that an individual is not a PEP; conversely, a true hit does not necessarily mean an individual is a material or active PEP.

L. Politically Exposed Persons ("PEP")

Unless an individual customer who is deemed to be a PEP is a sanctioned individual, a business relationship is not precluded. However, enhanced due diligence must be applied.

Similarly, the presence of a PEP in a company's structure or controlling bodies does not preclude the possibility of a business relationship.

A risk-based approach can be applied where a customer is a former non-Hong Kong PEP. The decision of applying EDD can only be taken after considering the level of influence the former PEP has, seniority position that the PEP used to hold or if he is still linked formally or informally with position held.

L.1 Definition of a PEP

AMLO classifies and defines PEPs as follows:

"Non-Hong Kong PEPs are individuals who are or have been entrusted with prominent public function in a place outside the Hong Kong Special Administrative Region, for example Heads of State or Government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

Former Non-Hong Kong PEPs are individuals who were entrusted but are not currently entrusted with prominent public function in a place outside the Hong Kong Special Administrative region.

Hong Kong PEPs are individuals who are or have been entrusted with a prominent public function in a place within the Hong Kong Special Administrative Region, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

Former Hong Kong PEPs are individuals who were entrusted but are not currently entrusted with prominent public function in a place outside the Hong Kong Special Administrative region.

International organisation PEPs are persons who are or have been entrusted with a prominent function by an international organisation, such as members of senior management or individuals who have been entrusted with equivalent functions, i.e. directors, deputy directors and members of the board or equivalent functions.

Family members are individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership.

Close associates are individuals who are closely connected to a PEP, either socially or professionally.

The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories."

M. State-Owned Enterprises ("SOE")

Third-party databases may flag companies as state-owned by virtue of a minority shareholding by a nation state. Before deeming a company to be state-owned, employees should ascertain the level of ownership. A company less than 50% held by a nation state should not be classified as an SOE, therefore any individuals flagged as a PEP purely based on being employed by the company do not qualify as PEPs.

For companies which are majority-held by a nation state, the employee must consider the circumstances of the holdings. For example:

(a) Corporations listed on a stock market in an equivalent jurisdiction
(b) Corporations that were subject to government bail-outs due to financial crises (these are usually listed companies)
(c) Corporations whose shareholding is via government seed funds (this is generally limited in scope to well below 50%, however, economic climates are subject to change)

Classifying PEPs by Position, Influence, & Relevance

Unlike sanctions, PEP lists are run by third-party provider and are not official lists. Third-party databases do not generally distinguish between the level of exposure a PEP may have, although they usually provide the person's position.

A PEP flag is a signal to check the status and position of the individual. A risk-based approach is always necessary. As guidance, PEPs can be divided into two tiers. Family members and close associates align with the tier of the PEP in question (e.g. the spouse of a Member of Parliament would fall under Tier One).

Tier One – HIGH Risk

Tier One PEP's include:

(a) Heads of State (including Royal families) & Heads of Government
(b) Members of Government (ministers, deputies, state and under-state secretaries, permanent secretaries) at supranational, national, and sub-national levels in the case of federal states and provinces in China
(c) Members of parliament or national legislatures, senior members of the diplomatic corps e.g. ambassadors, chargés d'affaires, consuls-general, or members of boards of central banks
(d) Members of the European Parliament; President of the European Commission; Heads of other European Union bodies (e.g. Court of Auditors)
(e) Mayors of capital cities and other major cities (e.g. Barcelona, Chicago, Mumbai, Munich, New York, St. Petersburg, Sydney, Vancouver, etc.)
(f) Senior judicial officials who sit on bodies whose decisions are not subject to further appeal (including the International Criminal Court, European Court of Justice, European Court of Human Rights, Court of Arbitration for Sport)
(g) Heads and other high-ranking officers holding senior positions in the armed forces
(h) Heads, deputies, and board members of international / regional organisations (e.g. UN, EU, World Bank, EBRD, OAS, Arab League, ASEAN, CARICOM etc)
(i) Presidents/Chairs and board members of State-Owned Enterprises (SOEs), businesses and organisations with major political or economic significance
(j) Top ranking officials of mainstream political parties
(k) Heads and their deputies of minor political parties (without parliamentary representation).

Tier Two – HIGH or MEDIUM Risk

The risk level for Tier Two PEPs is subject to the jurisdiction of domicile of the PEP. For jurisdictions deemed HIGH risk, the PEP shall also be deemed HIGH risk.

(a) Members of subnational parliaments, i.e. the states within a federal system
(b) Members of legislative and executive bodies at regional or equivalent levels
(c) Judges, justices, magistrates in courts with jurisdiction at regional, provincial or equivalent level
(d) Mid-ranking officials of the military, judiciary, law enforcement agencies, central banks and other state agencies, authorities and state bodies
(e) Heads and senior members of mainstream religious groups
(f) Advisers to senior officials of the military, judiciary, law enforcement, central banks and other state agencies, authorities and state bodies

(g) Heads and board members / senior officials of Trade Unions. In the case of Chambers of Commerce and Charities a risk-based approach is followed
(h) Presidents, secretary generals, directors, deputy directors and members of the board or equivalent function of international NGOs (e.g. Oxfam, Amnesty, Transparency International etc)
(i) Middle ranking diplomats
(j) Mayors and members of local councils at municipal, town, village or equivalent levels (i.e. below regional, provincial, cantonal and similar levels)
(k) Civil servants at regional/provincial or equivalent levels; officials of administrative bodies at local levels

Material vs Non-Material PEPs

One key to determining the applicability of the PEP tag is to decide if the PEP is a material or non-material PEP. For this, the function of the PEP within the organisation should be considered before making a final determination as to the PEP status of the customer.

For example, non-executive directors would generally be considered as non-material PEPs, because:

a) They hold no executive power
b) They exert no control over the day to day running of the business

An Honorary Consul who is not the sole representative of that country in their place of domicile is unlikely to be a material PEP. Equally, Honorary Consuls who are sole representatives of that country in their place of domicile but carry out no consular services are unlikely to be material PEPs.

Current vs Former PEPs

Current PEPs are those who still hold the positions concomitant with their PEP status. When they no longer hold that position many databases change their status to “Former”. Within one year (12 months) of that “Former” date, the Company shall still consider the PEP to have an active status and re-evaluate that status at the next annual review.

The key considerations are relevance and timeliness. For example, a former junior health minister, who held the position for a year and left the role, and parliament, over 10 years prior might not be considered a current PEP and be deemed a former PEP. However, if that individual were to be an executive director of a major pharmacology corporation, it could be argued that that person’s experience, network and influence is being used, and therefore the individual could still be considered a current PEP.

Other PEPs whose PEP status would be deemed never to expire include:

(a) Heads of State
(b) Heads of Government

(c) Heads of International Organizations (e.g. UN, WHO, European Commission, etc.)
(d) Senior Cabinet Ministers having served multiple terms in office

N. Enhanced Due Diligence

All HIGH-risk customers and situation specified by the CCE in a notice in writing give to the Company are subject to enhanced due diligence ("EDD"). The aim of EDD is to provide further background information linking the customers to the transactions and providing further evidence that there is no cause for suspicion of money laundering. For natural persons this implies obtaining information on the source of the individual's wealth. In the case of high-profile individuals, independent public sources may be used to ascertain source of wealth, e.g. Forbes, Bloomberg, etc.

For legal persons, source of wealth should be ascertained for the entity and all beneficial owners in the case of corporations.

Further enhanced due diligence information for corporations can include:

(a) Size of the company, e.g. number of employees
(b) Annual turnover
(c) Assets & Liabilities

For Trusts, the source of wealth of the settlor should be established in addition to any other individual transferring assets to the Trust.

Furthermore, if a PEP is identified in the control or ownership of any legal person, the source of wealth for the PEP should also be verified. This can be taken from independent public sources.

Adverse media screening, whereby the customers and associated parties are either screened against a third-party database, or search engines are used alongside terms such as fraud, tax evasion, money laundering, financial crime, shall also be employed during EDD procedures.

Enhanced due diligence must be countersigned / signed-off by a member of Senior Management.

Examples of EDD include:

(a) business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic difference between the Company and the customer);
(b) legal persons or legal arrangements that involve a shell vehicle without a
(c) clear and legitimate commercial purpose;
(d) companies that have nominee shareholders and control through nominee or corporate directors or shares in bearer form;
(e) cash intensive business;
(f) the ownership structure of the legal person or legal arrangement appears unusual or excessively complex given the nature of the legal person's or legal arrangement's business;

(g) the customer or the beneficial owner of the customer is a foreign politically exposed person.
(h) anonymous transactions (which may involve cash);
(i) frequent payments received from unknown or un-associated third parties.
(j) countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as not having effective AML/CFT Systems;
(k) countries or jurisdictions identified by credible sources as having a significant level of corruption or other criminal activity;
(l) countries or jurisdictions subject to sanctions, embargoes or similar measures issued by, for example, the United Nations; or
(m) countries, jurisdictions or geographical areas identified by credible sources

O. Final Risk Rating & Sign-Off

Upon completion of CDD (including EDD where necessary), the Company shall document the final risk rating and the file shall be signed, either electronic or physically, by the person performing the CDD, a reviewer (if a four-eyes approach is taken) and by the relationship manager. In the event EDD was required, sign-off from a senior manager is also required.

The date upon which approval was granted shall serve as the deadline for the next review, e.g. a LOW-risk customer approved on the 30th April 2024, shall be due for approval no later than the 30th April 2029

V. Ongoing Monitoring & Periodic Review System

A. Ongoing Monitoring

Customer due diligence measures are most effective when the identification and verification of the customer's identity, controllers, and beneficial owners, is coupled with ongoing monitoring of their transactions and their details are regularly screened.

A.1 Ongoing Screening

The sanctions landscape is constantly shifting. As a result, it is necessary to regularly screen customers in between the regular review cycles.

The Company shall incorporate the names and associated parties of all customers in their ongoing database screening and review of any alerts trigger events.

Trigger events associated with screening include:

(a) Inclusion of a customer or an associated party on sanctions, or sector specific sanctions lists
(b) Newly acquired PEP or close associate status pertaining to the customer or an associated party
(c) Material adverse media, especially those related to predicate offences to money laundering such as tax evasion, fraud, embezzlement, drug trafficking, modern slavery, etc.

A.2 Transaction Monitoring

All raw data for incoming and outgoing transactions shall be stored and reviewed on a regular basis. Analysis is based on patterns over time and transactions deviating from the pattern must be examined closely. Any suspicious transactions must be flagged to the MLRO and all customer data provided to the MLRO for review.

Examples of unusual transactions include:

(a) Large or unusual settlements/transactions in bearer form
(b) Any transaction involving an unknown counterparty
(c) Unclear source of funds, or one inconsistent with the client's apparent standing
(d) Without reasonable explanation, the size or pattern of transactions is out of line with any previous pattern
(e) The client refuses to provide information requested without reasonable explanation including for the purpose of CDD and/or ongoing monitoring
(f) Wash trading (matching subscription and redemptions rather than switching) through multiple accounts including transfer of positions between accounts that do not appear to be commonly controlled

All suspicious transactions necessitate a trigger review; however, consideration should be given to the possibility of tipping off the customer. Senior Management,

together with the CO and MLRO, should be consulted as to if and how to commence the trigger event review.

A.3 Trigger Event Reviews

Trigger event reviews generally necessitate an elevation to HIGH risk and the performance of EDD. Senior management should be informed immediately of trigger events in respect of customers. Additionally, the CO/MRLO should be informed that a trigger event review is required and be informed as to the reason behind it.

Employees should be aware of the risks associated with tipping-off when it comes to trigger event reviews.

Material & Immaterial Changes

Circumstances for customers are always subject to change; however, not all changes require a full review of their file. Changes can be divided into material and immaterial changes.

Immaterial Changes

Immaterial changes are generally superficial changes that are unlikely to cause a change in risk rating. Examples of immaterial changes include:

(a) Addition / removal of authorised signatories
(b) Addition / removal of directors
(c) Change of address within the same jurisdiction
(d) Changes in ownership structure that do not give rise to the inclusion of additional shareholders holding greater than 25% nor affect the identities of beneficial owners

Review Procedures for Immaterial Changes

Only the aspect that has changed shall be reviewed, i.e. if there is a new signatory, the signatory must be identified and verified as per the procedures in Part IV, and screened against sanctions, PEP, and adverse media databases, or using search engines. Provided there are no true hits or material adverse media, the addition of the signatory can be approved by the person(s) performing the CDD and signed off by the relationship manager.

If the review triggers an upgrade in risk rating, i.e. from MEDIUM to HIGH, a full review must be performed.

Removal of Signatories & Resignations of Directors

Notices in respect of the removal of signatories and resignation of directors must be made in writing.

For removal of signatories a board resolution should be provided to that effect.

For resignations of directors, the associated filings to the relevant company registry should be obtained or provided in original or certified true copy form. The information should be kept on file but moved from the active section of the file.

Material Changes

Material changes are ones that are substantive in respect of the nature of the customer's business model, ownership, or income. Material changes necessitate a full review of the customer file. This would have the additional effect of resetting the next review date.

Examples of changes that shall be deemed material:

- Changes in the ownership structure that give rise to the inclusion of a shareholding entity, not previously identified as an associated party, holding greater than 25%
- Addition of a new beneficial owner
- Change in company form
- Change in nature of business
- Changes in address causing a change in jurisdiction
- Insolvency/bankruptcy of the customer or an individual or entity in its ownership structure holding greater than 25%
- One-off transactions exceeding the thresholds of HK$8,000 for wire transfers and HK$120,000 for other types of transaction
- Reactivation of dormant account

A.4 Periodic Review Procedures

Preparation for Periodic Reviews

The Company shall check the client database for upcoming review dates. If this is done on a quarterly basis this should encompass any reviews due within the next 6 months. For monthly reviews this can be reduced to those due within 3 months.

Collection of Documentation

Documentation which has expired or is deficient in some way (e.g. low-quality copies) shall be collected. The employee of the Company should request confirmation from the customer that any other existing data (which is still valid) is correct and up to date.

Conducting CDD

CDD shall be conducted in accordance with the procedures set out in Part IV.

A.5 Reviews not Meeting the Next Review Date Deadline

If it becomes known that a periodic review shall fail to meet the review deadline, senior management must be informed with the reasons for the delay. Should the delay be the result of actions or inaction on behalf of the customer senior management must give thought to filing a suspicious activity report and inform the MLRO immediately.

B. Dormant Accounts

Dormant accounts are not subject to the regular review process; however, the customer and associated parties should still be screened against sanctions lists. A

dormant account is defined as a continuing account that has no activity other than transaction initiated by the Company after a specified time period, especially 1 year.

VI. Reporting of Suspicious transaction

A. SAFE

The Company adopts “SAFE” approach which includes:

(a) **S**creening the account for suspicious indications;
(b) **A**sking the customers appropriate questions;
(c) **F**inding out the customer’s records; and
(d) **E**valuating all the above information

The Company and its employees shall notify the CO & MLRO of all suspicious activities and transactions as soon as is practicable. The MLRO shall have access to all information and investigate accordingly. The MLRO shall be the sole arbiter of whether an activity or transaction is suspicious or not and shall document the findings and submit a report to the Board of Directors. Where an activity or transaction has been deemed suspicious, the MLRO shall file a SAR to the JFIU.

A.1 Avoidance of Tipping-Off

It is an offence (“tipping off”) to reveal to any person any information which might prejudice an investigation; if a customer is told that a report has been made, this would prejudice the investigation and an offence would be committed. The tipping off provision includes circumstances where a suspicion has been raised internally within a TCSP, but has not yet been reported to the JFIU.

Once the Company has determined that a suspicious transaction has taken place, or that the activity of a customer is suspicious, CDD must be conducted immediately.

However, due to the potential of tipping off the customer by undertaking CDD, Senior Management, the CO, and MLRO must be contacted prior to contacting the customer in order to create a strategy for performing the required due diligence whilst minimising the risk of alerting suspicion to the cause of the request for CDD.

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

- making a review of transaction patterns and volumes through connected accounts, preferably adopting a relationship-based approach rather than on a transaction-by-transaction basis;
- making reference to any previous patterns of instructions, the length of the business relationship, and CDD and ongoing monitoring information and documentation; and

- appropriate questioning of the customer per the systematic approach to identifying suspicious transactions recommended by the JFIU.

The Company shall conduct an appropriate review of a business relationship upon the filling of an STR to the JFIU. The senior management shall determine how to handle the relationship concerned to mitigate any potential legal or reputational risks.

The Company shall establish and maintain a record of all internal and external STRs made to the MLRO. The record will include:

- details of the date the report was made;
- the staff member subsequently handling the report;
- the results of the assessment
- whether the internal report resulted in an STR to the JFIU; and
- information to allow relevant documents to the report to be located.

VII. Audit Function

.

Given the size of the Company, it does not have a dedicated audit function. The regular review will include, but not limited to, of the Company's AML/CFT systems, ML/TF risk assessment framework, application of RBA, effectiveness of suspicious transaction reporting systems, effectiveness of the compliance function and staff training will be undertaken on a periodic basis by a suitably qualified external party.

VIII. Staff Training

Staff training is an important element of an effective AML/CFT System. The effective implementation of Company's AML/CFT System can be compromised if staff using the system is not adequately trained.

Accordingly, the MLRO is responsible for development and carrying out of training sessions for the Company's employees in respect its AML/CFT Systems.

Staff training will be held for all new joiners and further refresher training will be held at least once a year, where staff will be made aware, among other things, of:-

(a) the Company's and their own personal statutory obligations and the possible consequences for failure to report suspicious transactions under the DTROP, the OSCO and the UNATMO;

(b) any other statutory and regulatory obligations that concern the Company's and themselves under the DTROP, the OSCO, the UNATMO, the UNSO and the AMLO, and the possible consequences of breaches of these obligations;

(c) the Company's policies and procedures relating to AML/CTF, including suspicious transaction identification and reporting; and

(d) Any new and emerging techniques, methods and trends in ML/TF to the extent that such information is needed by the staff to carry out their particular roles in the Company with respect to AML/CFT.

The Company may include following areas of training for front, middle and back staff:

(a) all new staff, irrespective of seniority:

- an introduction to the background to ML/TF and the importance placed on ML/TF by the Company; and
- the need for identifying and reporting of any suspicious transactions to the MLRO, and the offence of "tipping-off";

(b) members of staff who are dealing directly with the public (e.g. front-line personnel):

- the importance of their roles in the Company's ML/TF strategy, as the first point of contact with potential money launderers;
- the Company's policies and procedures in relation to CDD and record-keeping requirements that are relevant to their job responsibilities; and
- training in circumstances that may give rise to suspicion, and relevant policies and procedures, including, for example, lines of reporting and when extra vigilance might be required;

(c) back-office staff, depending on their roles:

- appropriate training on customer verification and relevant processing procedures; and
- how to recognise unusual activities including abnormal settlements, payments or delivery instructions;

(d) managerial staff including internal audit officers and COs:

- higher level training covering all aspects of the Company's AML/CFT regime; and
- specific training in relation to their responsibilities for supervising or managing staff, auditing the system and performing random checks as well as reporting of suspicious transactions to the JFIU; and

(e) MLROs:

- specific training in relation to their responsibilities for assessing suspicious transaction reports submitted to them and reporting of suspicious transactions to the JFIU; and
- (ii) training to keep abreast of AML/CFT requirements/developments generally.

The Company must monitor the effectiveness of the training. This may include:

(a) testing staff's understanding of the Company's policies and procedures to combat ML/TF, the understanding of their statutory and regulatory obligations, and also their ability to recognise suspicious transactions;
(b) monitoring the compliance of staff with the Company's AML/CFT Systems as well as the quality and quantity of internal reports so that further training needs may be identified and appropriate action can be taken; and
(c) monitoring attendance and following up with staff who miss such training without reasonable cause.

Records on training undertaken should be maintained for a minimum of 3 years.

IX. Record-Keeping

Record-Keeping

Record keeping forms an essential part of the Company's risk-based approach to AML/CFT as it provides an audit trail for the detection, investigation and confiscation of criminal or terrorist property or funds. Record keeping assists investigating authorities to establish a financial profile of a suspect; trace the criminal or terrorist property or funds; and allow the Court to examine all relevant past transactions to assess whether the property or funds are the proceeds of or relate to criminal or terrorist offences.

The Company shall keep all records pertaining to CDD, business correspondence, transaction data, analysis results, and any other pertinent information for at least five years following the termination of the business relationship or after the date of a one-off transaction. A more detailed breakdown of record keeping procedures can be found in Appendix B: Record-Keeping Policy.

The Company's records are held by the Company in electronic form* in Hong Kong.

This ensures that the Company can at all times demonstrate to the CR, among other things:

(a) how it assesses a customer's ML/TF risk; and
(b) the extent of CDD and ongoing monitoring is appropriate based on the customer's risk profile.

The Company will ensure that:-

(a) all records are stored in a manner that is reasonably practical to retrieve;
(b) a register is kept of any original documents which is required by law to be released;
(c) relevant competent authorities in Hong Kong and internal and external auditors of the Company are able to have access as required; and
(d) all relevant documents are retained for a period of at least 5 years after the business relationship with a customer ceases.

X. Cooperation with Regulator and Law Enforcement Agencies

The CR is the authority for regulating the TCSP with effect from November 2018. The Company will cooperate with the CR about their routine inspection or investigation. This company will also cooperate with other law enforcement agencies wherever required under the laws of Hong Kong.

The Company may receive requests like search warrants, production orders, restraint orders or confiscation orders from law enforcement agencies. The Company will handle these requests in an effective and timely manner, including allocation of sufficient resources and appointing a staff as the main point of contact with law enforcement agencies.

The Company will respond to any search warrant and production order within the stipulated time. Where the Company encounters difficulty in complying with the orders in stipulated time period, the Company will contact the officer-in-charge of the investigation for further guidance.

The Company will help the regulator and various law enforcement agencies in every possible manner.

VI. Appendices

A. Glossary of Abbreviations & Terms

Provided on request

B. Record Keeping

Provided on request

C. Guidance on Assigning Risk Ratings

Provided on request