



Growing Asia's Markets



ASIFMA Best Practices for AML/KYC

June 2018

Developed with support from an ASIFMA member working group led by:



HERBERT
SMITH
FREEHILLS

Contents

1.	Overview.....	3
2.	CDD Measures – Identification of Customer.....	4
3.	CDD Measures – Verification of Customer	7
4.	Beneficial Owners of Customers – Identification and Verification.....	9
5.	CDD – Establishing Business Relationship.....	10
6.	CDD – Person Purporting to Act on Behalf of Customer	10
7.	When CDD Measures Must be Carried Out.....	11
8.	Simplified Customer Due Diligence ("SDD")	11
9.	Duty to Continuously Monitor Business Relationships.....	11
10.	Risk Based Approach.....	12
11.	Carrying Out CDD Measures by Means of Intermediaries / Third Parties	12
12.	Documentation	13
13.	Conclusion.....	14

1. OVERVIEW

Many of the challenges of Know-Your-Client/Anti-Money Laundering (**KYC/AML**) implementation remain high on the global agenda. Differing guidelines and regulations among jurisdictions in Asia as well as divergent interpretation of these guidelines and regulations among financial institutions (**FIs**) have led to fragmentation, inconsistencies and varying practices amongst FIs. In this regard, FIs have started to adopt a forward looking, client-centric and digitised approach to reduce the resource challenges associated with meeting KYC/AML requirements.

Challenges in resourcing and dealing with regulatory change remain. According to a 2017 survey¹ conducted by Thomson Reuters, the largest FIs (USD10 billion+ turnover) saw an average spend on KYC-related procedures increase from USD142 million in 2016 to USD150 million in 2017. The number of employees working on KYC compliance in FIs rocketed from an average of 68 in 2016 to 307 in 2017. Despite the increase in headcount, approximately a third (34%) of FIs reported that resources remained the biggest challenge in conducting KYC and customer due diligence (**CDD**) processes, with another third (33%) considering the volume of regulatory change to be the key challenge in the KYC process.

To address the above challenges, this paper proposes a set of best practices to harmonise and standardise the application of certain key areas of AML/KYC requirements in Asia, based on input and industry feedback from a focused workgroup of ASIFMA members from both the buy side and sell side. The objective of this paper is to help industry participants gain an understanding of current best practices in the market and to drive harmonisation and standardisation in the area of AML/KYC in the Asia-Pacific region. In addition, these best practices can also help the adoption of and interoperability between the KYC utility providers.

This initiative follows an earlier survey conducted in 2017 by ASIFMA and PricewaterhouseCoopers whereby ASIFMA members and non-members were surveyed on the documents and data that they collected for four categories of institutional clients in the capital markets and trading business in 12 Asia-Pacific jurisdictions.² 55 firms – both buy side and sell side – responded to the survey.

The primary intent of this industry study was to obtain an overview of market practice to determine, based on the feedback from survey respondents, what constitutes good practice in relation to KYC practices and associated controls. The best practices here were drafted on the back of this survey and supplemented with specific input and industry feedback gathered in the course of several workgroup meetings with the industry.

These best practices have been drafted as generally as possible to be jurisdiction-neutral, although reference was largely drawn from industry consensus of best practices currently applied by members in Hong Kong and Singapore.

The working group identified the following key areas where it would be most useful to develop best practices:

- identification and verification of customers and their beneficial owners;
- obtaining information when looking to establish a business relationship;
- identification and verification of persons purporting to act on behalf of customers;
- the timing of due diligence measures;
- the application of simplified CDD measures;

¹ Thomson Reuters, KYC Compliance: The Rising Challenge for Financial Institutions 2017, available at this [link](#).

² Hong Kong, Singapore, Australia, Japan, China, India, Korea, Malaysia, Indonesia, Thailand, Taiwan, and the Philippines.

- the monitoring of business relationships;
- factors to consider in developing a risk-based approach;
- use of intermediaries or third parties to carry out CDD; and
- aspects of CDD documentation.

2. CDD MEASURES – IDENTIFICATION OF CUSTOMER

2.1 Determining who is the customer

2.1.1 General

Depending on the specific circumstances of each customer, the following overarching non-exhaustive approaches may be used to determine who the "customer" is:

- the party providing instructions to the FI; or
- the party that contracts with the FI.

2.1.2 Funds and fund managers

(A) Determining who is the customer

Party providing instructions to FI and/or exercising influence and control

Ordinarily, this will be the fund manager (in the context of funds) which has been delegated decision-making authority by the fund. If the party providing instructions is acting as an agent, then identity information of the underlying client would be required.

Party contracting with FI

This approach would mean that:

- if a fund manager contracts with a FI on behalf of an investment vehicle/fund, then simplified due diligence (**SDD**) can be performed on the fund manager provided that the fund manager has performed CDD on the fund. It may be possible to obtain limited KYC information on the fund; and
- if an investment vehicle or fund contracts with a FI, then CDD/SDD (as appropriate) should be applied to the investment vehicle or fund, depending on the legal form of the investment vehicle or fund. In this context, a fund manager should be regarded as a person purporting to act on behalf of a customer if it has the authority to place an order on behalf of an investment vehicle or fund.

(B) Equivalently regulated fund manager

Where an equivalently regulated fund manager provides instructions to a FI, CDD can be performed on the fund manager rather than the fund itself. For example, in Hong Kong, "equivalent jurisdiction" is defined in the Anti-Money Laundering Ordinance (**AMLO**) as meaning:

- a jurisdiction that is a member of the Financial Action Task Force (**FATF**), other than Hong Kong; or
- a jurisdiction that imposes requirements similar to those imposed under Schedule 2 of the AMLO.

Some information should still be collected in respect of the fund on a risk-based basis.

(C) **Fund manager which is not equivalently regulated**

Where a fund manager is not equivalently regulated, then full CDD should be performed on both the fund manager and the underlying fund unless:

- SDD can be performed in Hong Kong under Schedule 2, Part 2, para 4 of AMLO or in Singapore under the relevant SDD provisions; or
- the FI can place reliance on a third party that performs the CDD as specified in the Singapore and Hong Kong laws and regulations.

(D) **Where the fund is customer**

Where the fund is considered the customer for AML/CTF purposes, FIs should nonetheless identify the fund manager and verify the fund manager's identity due to the instructions issued and control exercised by the fund manager.

(E) **Capacity in which FI acts**

Where a FI is acting as:

- a prime broker, clearing broker, settlement agent or custodian, both the fund and the fund manager (due to instructions being provided by and control exercised by the fund manager) should be considered as customers; or
- an executing broker only, the fund manager (and not the investment vehicle/fund) should be considered as the customer.

2.1.3 **Trusts**

A similar approach should be adopted with respect to trusts. That is, the trustee should be considered the contracting party and thus the customer, although certain identification and verification information with respect to the trust should also be obtained.

2.1.4 **Third parties**

For third parties such as brokers, market infrastructures (such as clearing houses and exchanges), custodians and agent banks, KYC/CDD steps would still be required. Steps to be taken may include:

- perform SDD and check that the entity exists;
- confirm correct contact details;
- screen for negative news; and
- confirm the third party is equivalently regulated and not a sanctioned party.

For **third party brokers**:

- obtain licence proof to determine its regulated or licensed status from the relevant authorities. If the licensed status cannot be ascertained, escalate to Compliance for further review;
- for level 1 KYC:
 - obtain proof of existence – constitutional documents such as a certificate of incorporation or registration of a company search from the register. For equivalently regulated FIs or listed companies, obtain the latest printout from the regulator's or exchange's website which should evidence the full name and that it is currently regulated or listed and its stock code;

- a list of all controllers or directors – where a client has appointed corporate directors, it is required to identify the individuals of the corporate director who have been designated with the executive authority to perform directorate duties for the client;
- list of beneficial owners:
 - for low risk beneficial owners, FIs may decide not to identify beneficial owners if the entity is an equivalently regulated FI in an equivalent jurisdiction or a listed company with an approved exchange;
 - beneficial owner profile is required for a natural person including recent employment history (key roles or appointments), primary business activities, nationality and permanent residency and source of wealth (estimated net worth, assets and notable shareholdings); and
 - where there is a known nominee shareholder, it is required to identify the actual beneficial owner for whom the nominee shareholder is holding the shares on behalf of; and
- conduct Worldcheck screenings and adverse media checks via Google, LexisNexis, Factiva or any other relevant sources on all identified parties above;
- for level 2 KYC, to be applied where there are positive matches from screenings and adverse news:
 - further information to elaborate on issues or to corroborate the documentation received via level 1 KYC;
 - further documentation to verify the authenticity of the information gathered in level 1 KYC; and
 - engagement of a reputable external investigation agency to investigate into or review an entity or individual with a particular focus on financial crime or reputational risks.

For agent banks and custodian banks:

- obtain licence proof to determine its regulated or licensed status from the relevant authorities. If the licensed status cannot be ascertained, escalate to Compliance for further review;
- undertake red flag screenings which consist of basic checks on the entity to ensure the name is not subject to any sanctions or serious criminal-related issues, for example, by:
 - conducting sanction check using Worldcheck; and
 - conducting adverse media check using Google, LexisNexis, Factiva, Baidu or any other relevant sources.

For clearing houses and exchanges:

- for client counterparty, conduct full KYC of equivalently regulated FI or listed company. KYC requirements should be based on risk rating of the customer:
 - where a client counterparty is determined to be low risk, such as the customer is an approved exchange in an equivalent jurisdiction, to obtain:
 - proof of regulated status from the regulator website for regulated FIs and proof of listed status from the exchange's website;
 - phone number and address proof of the entity;
 - source of wealth where there are doubts as to the source of wealth;
 - list of all controllers; and

- board resolution authorising list of all authorised signatories / power of attorneys (**POA**);
- where a client counterparty is determined to be medium risk, to obtain:
 - proof of regulated status from the regulator website for regulated FIs and proof of listed status from the exchange's website;
 - phone number and address proof of the entity;
 - evidence of source of wealth, such as audited financials;
 - list of all controllers;
 - list of 25% or more beneficial owners and their IDs;
 - board resolution authorising list of all authorised signatories / POAs; and
 - Wolfsberg Questionnaire (for regulated FIs only);
- where a client counterparty is determined to be high risk, to obtain:
 - proof of regulated status from the regulator website for regulated FIs and proof of listed status from the exchange's website;
 - phone number and address proof of the entity;
 - evidence of source of wealth, such as audited financials;
 - list of Controllers and their IDs;
 - list of 10% or more Beneficial Owners and their IDs;
 - board resolution authorising list of all authorised signatories / POAs and their IDs; and
 - Wolfsberg Questionnaire (for regulated FIs only);
- for intermediary counterparties, where an account is not set up as a client counterparty and is set up for booking and settlement only, conduct Level 1 KYC and Level 2 KYC if applicable (refer to KYC requirements of Level 1 and 2 KYC under third party brokers section above).

2.2 **Determining whether a customer is a new customer**

2.2.1 **Historical customers**

Where a FI has previously off-boarded a customer and then subsequently seeks to onboard that customer again, the customer should be treated as a new client and new documents should generally be obtained as shareholders, directors, authorised signatories, etc., could have changed in the interim. However, it may be possible to refer to some documents previously obtained from the customer such as the certificate of incorporation.

2.3 **Recording names of all directors**

All directors should be identified. The best practice is to identify "controllers" of the customer. This would be required anyway in a Foreign Account Tax Compliance Act (**FATCA**)/Common Reporting Standard (**CRS**) context where FIs would require this information.

3. **CDD MEASURES – VERIFICATION OF CUSTOMER**

3.1 **Fund and fund manager context**

With regard to verification processes, where the investment vehicle/fund is considered the customer, verification should include obtaining the following information and documents to verify the following:

- in respect of **publicly traded funds**:
 - the entity's existence;
 - its publicly traded status, including identifying the name of the exchange it is listed on;
 - the names of controlling management and directors of the fund; and
 - written confirmation from the investment vehicle/fund/fund manager that there is no individual investor holding more than a 25% interest in the fund; and
 - if there are any individual investors who hold more than a 25% interest in the fund, identifying such investors and undertaking reasonable risk-based measures to verify their identity;
- in respect of **equivalently regulated funds**:
 - the entity's existence;
 - its regulated status, for example by obtaining a copy of the applicable regulators' register;
 - the names of controlling management and directors of the fund;
 - written confirmation from the investment vehicle/fund/fund manager that there is no individual investor holding more than a 25% interest in the fund; and
 - if there are any individual investors who hold more than a 25% interest in the fund, identifying such investors and undertaking reasonable risk-based measures to verify their identity;
- in respect of **pension funds** (generally considered to be low risk):
 - the entity's existence;
 - its pension fund status, for example by obtaining evidence that it is registered as a pension scheme; and
 - the name of the relevant employer entity, although this may be difficult in practice as there may be multiple employers associated with a single pension scheme;
- in respect of other funds such as **hedge funds which are not equivalently regulated**, unless reliance is placed on an equivalently regulated third party such as a fund manager or administrator:
 - the entity's existence;
 - the names of controlling management and directors of the fund;
 - determining whether there are any individual investors who hold 25% or more of the interest in the fund and taking reasonable risk based measures to verify their identity; and
 - taking steps to understand the degree and nature of CDD measures (including sanctions) applied to underlying investors.

3.2 Use of Hong Kong Company Search reports (ICRIS) to verify

For a Hong Kong incorporated company, a FI may verify information using ICRIS. Alternatively, a FI may obtain from the customer a certified true copy of a company search report certified by the company registry or a professional third party. Company search report should have been issued within last six months.

It is not sufficient for the report to be self-certified by the customer.

If a FI has obtained a company search report which contains information such as certificate of incorporation, company's memorandum and articles of association, etc., a FI is not required to obtain the same information again from customer.

3.3 **Verifying directors of corporate customer – Risk-based approach**

Where directors act as a person purporting to act on behalf of the customer (**PPTA**), then a FI should identify and verify the director according to the individual standard (e.g. name, date of birth, nationality and ID number). Board and/or shareholder resolutions should not be used to verify as they are internal documents and not considered independent.

3.3.1 **Low/medium risk FIs:**

For trading relationships (non-cash deposit accounts), trading in securities (DVP Bonds/FX), with equivalently regulated/listed entities, there should not be a requirement to verify a director's identity to the individual standard (name, date of birth, nationality and ID number).

Directors' names can be collected via company searches and annual reports or equivalent. FIs may verify only two directors on a risk-based approach and verification should be permitted by way of public searches, annual reports, etc.

3.3.2 **High risk customers:**

FIs should record the names of all directors and verify all directors and screen all names for negative news and sanctions.

4. **BENEFICIAL OWNERS OF CUSTOMERS – IDENTIFICATION AND VERIFICATION**

4.1 **Fund and fund manager context**

FIs may adopt a risk-based approach and consider if SDD can be applied or if they can rely on the CDD performed by a third party (such as the fund manager or administrator).

Where neither SDD nor reliance is available:

- if the fund manager or administrator confirms there is no single investor holding 25% or more of the issued capital or voting rights, then no further CDD on the underlying investors is necessary (although this will need to be subject to review in the ordinary course);
- if the fund manager or administrator confirms there is an investor holding 25% or more of the issued capital or voting rights, the FI may:
 - verify the investor's identity via written confirmation from the manager/administrator;
 - verify the investor's identity using public available sources; or
 - in high risk situations, the firm may seek to verify the investor through ordinary documentary evidence.

In addition to identifying and verifying beneficial owners, FIs should take reasonable measures to verify identity of any individual who exercises ultimate control over the management of a corporation.

4.2 **Identifying and verifying companies with complex ownership or control structures**

In view of the fact that there is no clear definition of what constitutes a "complex" ownership or control structure, the following non-exhaustive list has been suggested as examples of when a complex ownership or control structure might be found to exist:

- multiple levels of ownership for no apparent economic reason;
- owning/controlling structures that are formed in multiple jurisdictions (and in particular, in tax havens);
- differing ownership and controlling entity types (e.g. personal holding companies, trusts, insurance companies, nominee agents or directors);
- loop ownership structures;
- excessive use of trusts or unincorporated entities in the ownership structure for no apparent economic reason;
- use of nominee shareholders and/or directors; and
- multiple shareholders with shareholding percentage slightly lower than the relevant beneficial owner thresholds (e.g. 9.99%).

5. **CDD – ESTABLISHING BUSINESS RELATIONSHIP**

5.1 **Obtaining information as to intended purpose and reason – Fund context**

FIs should take reasonable measures to understand:

- the nature and purpose of the fund (e.g. pension fund, hedge fund, private equity fund, etc.);
- the fund's investment objectives and strategies; and
- the nature of the products and services being provided to the fund.

6. **CDD – PERSON PURPORTING TO ACT ON BEHALF OF CUSTOMER**

6.1 **Identifying and verifying identity of person acting on behalf of a customer**

Legal persons (e.g. corporates) are represented by their directors and/or authorised signatories. The FI should collect the passport of that person (e.g. a director) wanting to open the account to verify the person's identity.

6.2 **Verifying authority to act on behalf of customer**

A power of attorney and/or board resolution should be obtained to see that the person acting on behalf of the legal person has authority to do so. That power of attorney or board resolution should identify that the person is representing the customer.

6.3 **Fund and fund manager context**

A FI should take the following steps to satisfy itself on the authority of a fund manager to act on behalf of a fund:

- for execution only activity, such authority may be confirmed through standard terms of business issued to the fund manager and/or the investment management agreement, as well as establishment of a fund sub-account by the fund manager;
- for other trading activity/products, understanding authority to act may be confirmed through:
 - legal contractual agreements in place, such as International Swaps and Derivatives Association (**ISDA**) Master Agreement;
 - if the fund manager is equivalently regulated, by written confirmation from the fund manager itself;

- independent and reliable sources available in public domain such as regulatory filings or prospectus documentation; and/or
- documentary evidence such as copy of investment management agreement.

7. WHEN CDD MEASURES MUST BE CARRIED OUT

7.1 Fund and fund manager context

Where a fund manager is not equivalently regulated and therefore CDD is required to be performed on both the fund manager and the fund, it may be difficult to perform full CDD measures on the fund in a securities trading context before business relations are established. This is because FIs may not necessarily know in advance which underlying funds the trade will be allocated to at the time of accepting trade instructions and/or it would be difficult to perform full CDD before trade settlement.

Block trades by fund managers also frequently involve allocations that are made after the trade is booked. It may be possible to perform 'light KYC' at the fund level (e.g. name of fund, domicile and link to the fund manager).

In the above circumstances, members can perform CDD on the fund manager and complete CDD on the fund within 30 days of trade execution on an exceptional and case-by-case basis.

8. SIMPLIFIED CUSTOMER DUE DILIGENCE (SDD)

8.1 Investment vehicle – When SDD may not be applied

For funds that are not regulated in an equivalent jurisdiction, unless reliance is placed on an equivalently regulated third party such as a fund manager or administrator, the following CDD should be performed:

- confirming the entity's existence;
- determining the names of controlling management and directors of the fund;
- determining whether there are any individual investors who hold 25% or more of the interest in the fund and taking reasonable risk-based measures to verify their identity; and
- taking steps to understand the degree and nature of CDD measures (including sanctions) applied to underlying investors.

The approach above is only suitable if the investment/fund is the contracting party (i.e. deemed as FI's client). The investment vehicle can be in different legal forms (e.g. corporation, partnership, trust, etc.)

9. DUTY TO CONTINUOUSLY MONITOR BUSINESS RELATIONSHIPS

9.1 When to review information

In the situation where information is still outstanding at the time of review, the nature of the outstanding information needs to be considered. If it is a material piece of information such as information relating to the ownership structure of the customer or an ultimate beneficial owner, then the FI should consult compliance as to whether it can continue relationship with the customer. Alternatively, if the outstanding information is less significant, such as a missing certification, consider whether an extension can be granted.

9.2 Reviewing information – High risk customers

At a minimum, FIs should review all client documents every year for high-risk clients.

10. RISK BASED APPROACH

10.1 Customer risk – Funds and fund managers

The following list is a list of non-exhaustive factors that FIs may take into consideration when assessing the risk of a fund manager which is not equivalently regulated:

- history of operations and reputation of the fund manager, including its key controlling personnel;
- whether the fund manager has any relevant history of regulatory enforcement action for AML/CTF obligations;
- the money laundering/terrorist financing risks associated with the products/services provided;
- the nature of the type of funds managed by the fund manager;
- the risk profile of the underlying investor base;
- whether there have been any transactions associated with the fund manager that have given rise to a suspicious activity report (**SAR**);
- geographic risks applicable to the fund(s) and underlying investor base;
- escalation to Business or Compliance for review and acceptance of the risks; and
- ongoing assessment of the risk throughout the life of the relationship.

If a fund manager is not equivalently regulated, then full CDD should be performed on both the fund manager and the underlying fund unless:

- SDD can be performed under Hong Kong or Singapore laws (as applicable);
- if the fund or fund manager is not equivalently regulated, then it would be hard to argue that there was low risk; or
- the FI can place reliance on a third party (e.g. other regulated persons) as specified in local laws and regulations.

Nevertheless, a number of factors will need to be taken into account to apply such a risk-based approach. For example, depending on the risk profile of the jurisdiction where the fund manager is regulated, the general nature of the funds managed by the fund manager and whether there are any suspicious indicators that ML/TF activities may be involved, enhanced due diligence may be required.

11. CARRYING OUT CDD MEASURES BY MEANS OF INTERMEDIARIES/THIRD PARTIES

11.1 Use of intermediaries for CDD

Unless an intermediary is from a FATF member country, FIs have to evaluate and determine which jurisdictions impose requirements "similar" to those imposed in the local jurisdiction.

11.2 Reliance on specified domestic intermediaries/third parties – FIs

To determine if a domestic intermediary satisfies the criteria for reliance, FIs should:

- make enquiries concerning domestic intermediary's stature or the extent to which any group AML/CFT standards are applied and audited; or
- review the AML/CFT policies and procedures of the domestic intermediary.

Examples of steps FIs can take to justify that they can place reliance on other equivalently regulated FIs performing due diligence:

- obtaining a satisfactorily completed Wolfsberg Questionnaire;

- a more formal review of AML policies and procedures; and
- obtaining satisfactory information about the intermediary's AML policies and procedures.

11.3 **Suitability and reliability of intermediary**

11.3.1 **How to determine and document comparability with local laws**

Non-exhaustive examples of data and information which may be used to determine that the particular jurisdiction where the intermediary is carrying on business or practising is equivalent include:

- Transparency International's Corruption Perceptions Index;
- whether the jurisdiction is on a tax 'black' or 'grey' list;
- FIs equivalently regulated by "category A" parents;
- oversight by a body which demands compliance with AML standards (e.g. Office of the Comptroller of the Currency (**OCC**));
- reports issued by international organisations such as Asia/Pacific Group on Money Laundering (**APG**), Caribbean Financial Action Task Force (**CFATF**);
- assessments performed by/professional advice received from external counsel; and
- basic comparison of KYC/AML laws and regulations.

12. **DOCUMENTATION**

12.1 **Documents in foreign language**

12.1.1 **Persons suitably qualified to perform translations**

Persons considered by members to be 'suitably qualified' to perform translations may include (the below list is non-exhaustive):

- persons who work in the FIs' own group;
- equivalently regulated intermediaries;
- lawyers and accountants;
- translation company;
- a banker independent to the customer relationship; and
- a local office of the FI.

12.1.2 **Translation of non-Latin names for screening**

There are sophisticated screening tools that can screen in local non-Latin characters.

12.2 **Independent suitable certifiers**

Where certified copies of documents which are not identification documents cannot or will not be provided by customers, provided the sanctions and politically exposed parties screening is clear, FIs may fall back to trying to obtain information from a public source (e.g. from Bloomberg, Dow Jones, LexisNexis or from Thomson Reuters).

13. **CONCLUSION**

- 13.1 Effective AML measures in the banking sector are essential to ensure that FIs can perform their gatekeeper role and are able to conduct robust, risk-based KYC to manage ML/TF risks. We hope that these best practices serve as a guide to FIs to benchmark their existing practices against best practices standards in the industry, to drive harmonisation in the industry and in the region and to ensure that international standards and obligations for AML/KYC are met.
- 13.2 It is important to note that these best practices have been prepared to suit the current regulatory requirements as at June 2018 and should be reviewed and revised regularly in accordance with amended laws, regulations and regulatory guidance as appropriate.