Briefing Seminar on the New Guidelines on Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT)

February 2012

Intermediaries Supervision Department
Securities and Futures Commission

Disclaimer

This presentation is intended to provide the audience with a broad overview of certain aspects of the Anti-Money Laundering and Counter-Terrorist

diligence (CDD) and record-keeping requirements and the new guidelines on AML/CFT published by the SFC. It provides information of a general nature that is not based on a consideration of specific circumstances. It is not intended to cover all requirements that are applicable to you and your firm. Accordingly, it should not be regarded as a substitute for seeking detailed advice on any specific case from your own professional adviser.

Outline

A. Introduction

B. AML/CFT systems

CDD and ongoing monitoring:

C. Risk-based approach

D. Highlights of major differences in CDD requirements between the new guidelines and the Prevention of Money Laundering and Terrorist Financing Guidance Note (AMLGN)

E. Ongoing monitoring

F. Suspicious transaction reports

G. Record-keeping

H. Financial sanctions and terrorist financing

I. Wire transfers

A. Introduction

Background

The AMLO, among others, codifies requirements relating to CDD and record-keeping for specified financial institutions (FIs)

Comes into effect on 1 April 2012

New guidelines on AML/CFT

Guideline on Anti-Money Laundering and Counter-Terrorist Financing (the Guideline) published under section 7 of the AMLO and section 399 of the SFO

To provide guidance to assist licensed corporations (LCs) and their officers and staff to comply with the AMLO ***(see next slides for criminal liability for non-compliance with the AMLO)*** and other applicable AML/CFT legislation and regulatory requirements

Associated entities (AEs) are expected to have regard to the Guideline as if they were themselves LCs *

To supersede the existing AMLGN

Gazetted on 27 January 2012 (http://www.gld.gov.hk/cgi-bin/gld/egazette/index.cgi?lang=e)

* *Reference should be made to the Prevention of Money Laundering and Terrorist Financing Guideline issued by the SFC for Associated Entities*

Criminal liability for non-compliance with the AMLO

Paragraph 1.16

The AMLO makes it a criminal offence if an FI (1) knowingly; or (2) with the intent to defraud any RA, contravenes a specified provision of the AMLO. The "specified provisions" are listed in section 5(11) of the AMLO. If the FI knowingly contravenes a specified provision, it is liable to a maximum term of imprisonment of 2 years and a fine of $1 million. If the FI contravenes a specified provision with the intent to defraud any RA, it is liable to a maximum term of imprisonment of 7 years and a fine of $1 million upon conviction.

(s.5, AMLO)

Criminal liability for non-compliance with the AMLO

Paragraph 1.17

The AMLO also makes it a criminal offence if a person who is an employee of an FI or is employed to work for an FI or is concerned in the management of an FI (1) knowingly; or (2) with the intent to defraud the FI or any RA, causes or permits the FI to contravene a specified provision in the AMLO. If the person who is an employee of an FI or is employed to work for an FI or is concerned in the management of an FI knowingly contravenes a specified provision he is liable to a maximum term of imprisonment of 2 years and a fine of $1 million upon conviction. If that person does so with the intent to defraud the FI or any RA he is liable to a maximum term of imprisonment of 7 years and a fine of $1 million upon conviction.

(s.5, AMLO)

Overview

Breach of the Guideline

Breach of the Guideline may result in disciplinary action by the SFC

(Paragraphs 1.1- 1.8c & 1.15 - 1.18)

Why are there *italic* texts?

The Guideline is in general not different from the one issued by the HKMA, OCI, and C&ED, except that supplementary guidance specific to the securities sector (i.e. sectoral guidance) is provided

Sectoral guidance is shown in *italics*

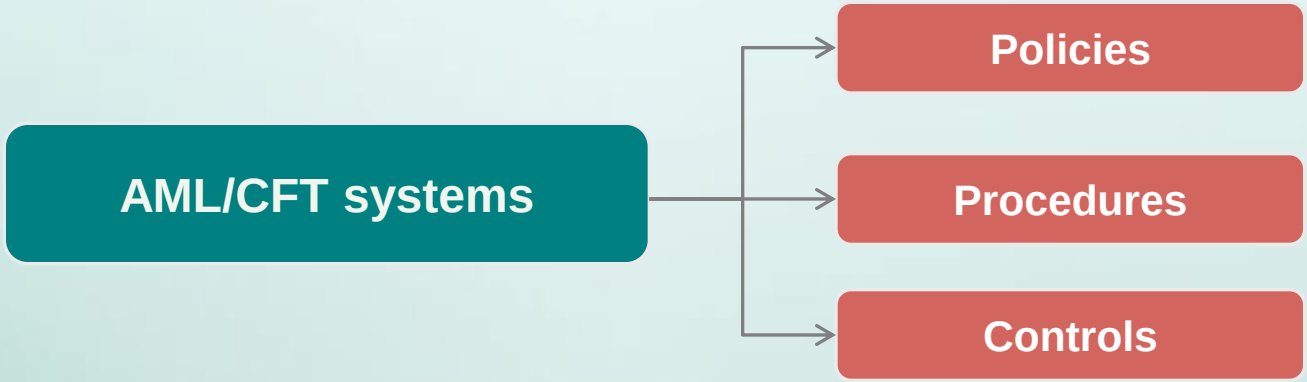
Overview

Paragraph 1.6

Given the significant differences that exist in the organisational and legal structures of different FIs as well as the nature and scope of the business activities conducted by them, there exists no single set of universally applicable implementation measures. It must also be emphasized that the contents of the Guideline is neither intended to, nor should be construed as, an exhaustive list of the means of meeting the statutory and regulatory requirements.

B. AML/CFT systems (Paragraphs 2.1 – 2.18)

Overview of AML/CFT systems



Senior management oversight

Paragraph 2.10

Senior management is responsible for oversight of the functions described below and should be satisfied that the FI's AML/CFT systems are capable of addressing the ML/TF risks identified.

Paragraph 2.12

Senior management should, as far as practicable, ensure sufficient seniority, authority, competence, resources, access to information and senior management, and independence of/for the CO and MLRO, in order that they can discharge their responsibilities effec>41ka4,7ld

Paragraphs 2.13 – 2.15

CO

Support senior management in adequately managing ML/TF risks and overseeing all activities relating to AML/CFT

Develop and/or continuously review and monitor the FI's AML/CFT

Paragraphs 2.16

Staff screening and training

Paragraph 2.18: Staff screening

Establish, maintain and operate appropriate procedures in order to be satisfied of the integrity of any new employees

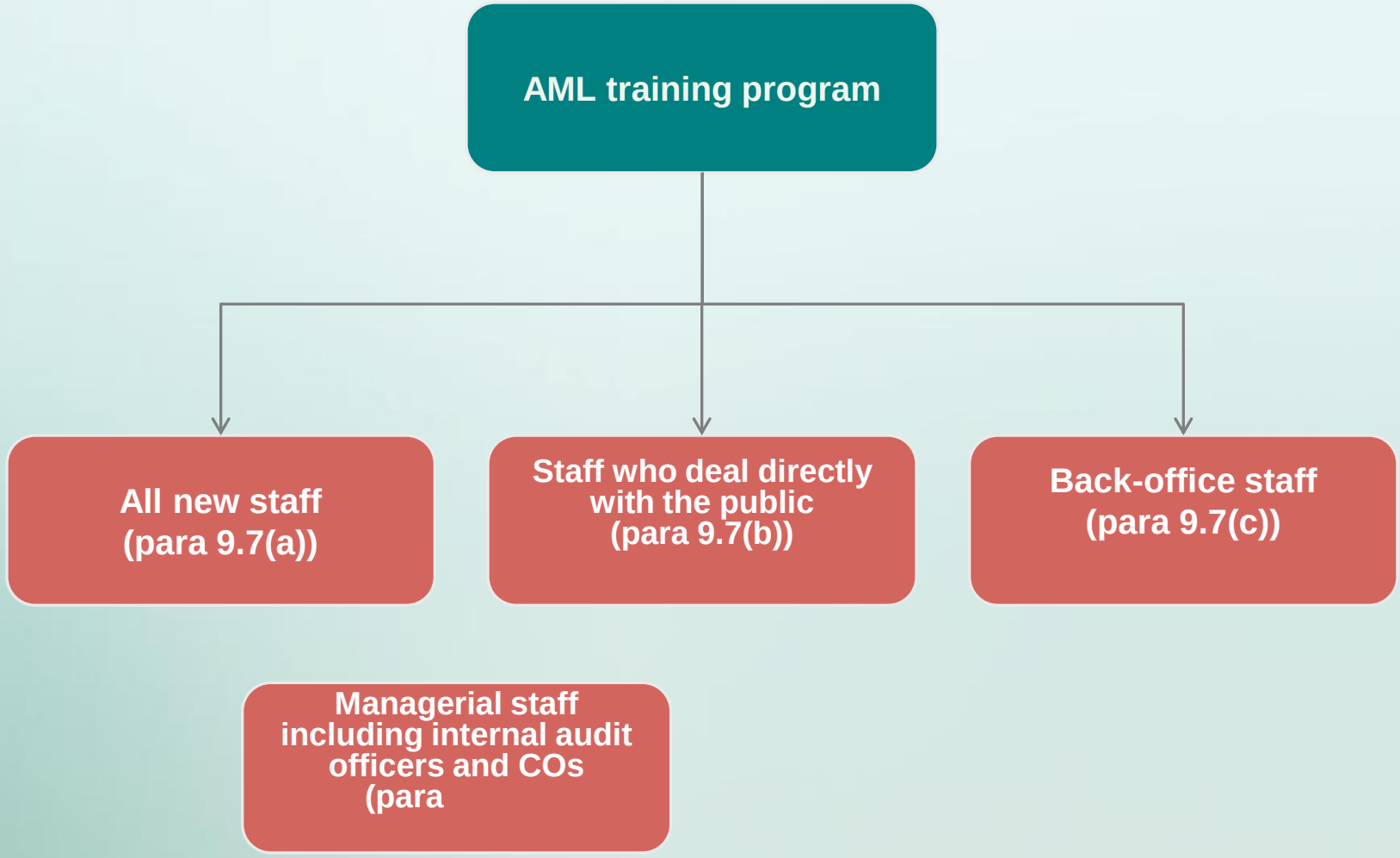
Paragraphs 9.1 – 9.10: Staff training

Staff should be trained in what they need to do to carry out their roles in the FI with respect to AML/CFT

AML training records* are to be kept for at least 3 years

* *This refers to records of staff who have been trained, when they received the training and the type of training provided*

AML training areas for different staff groups

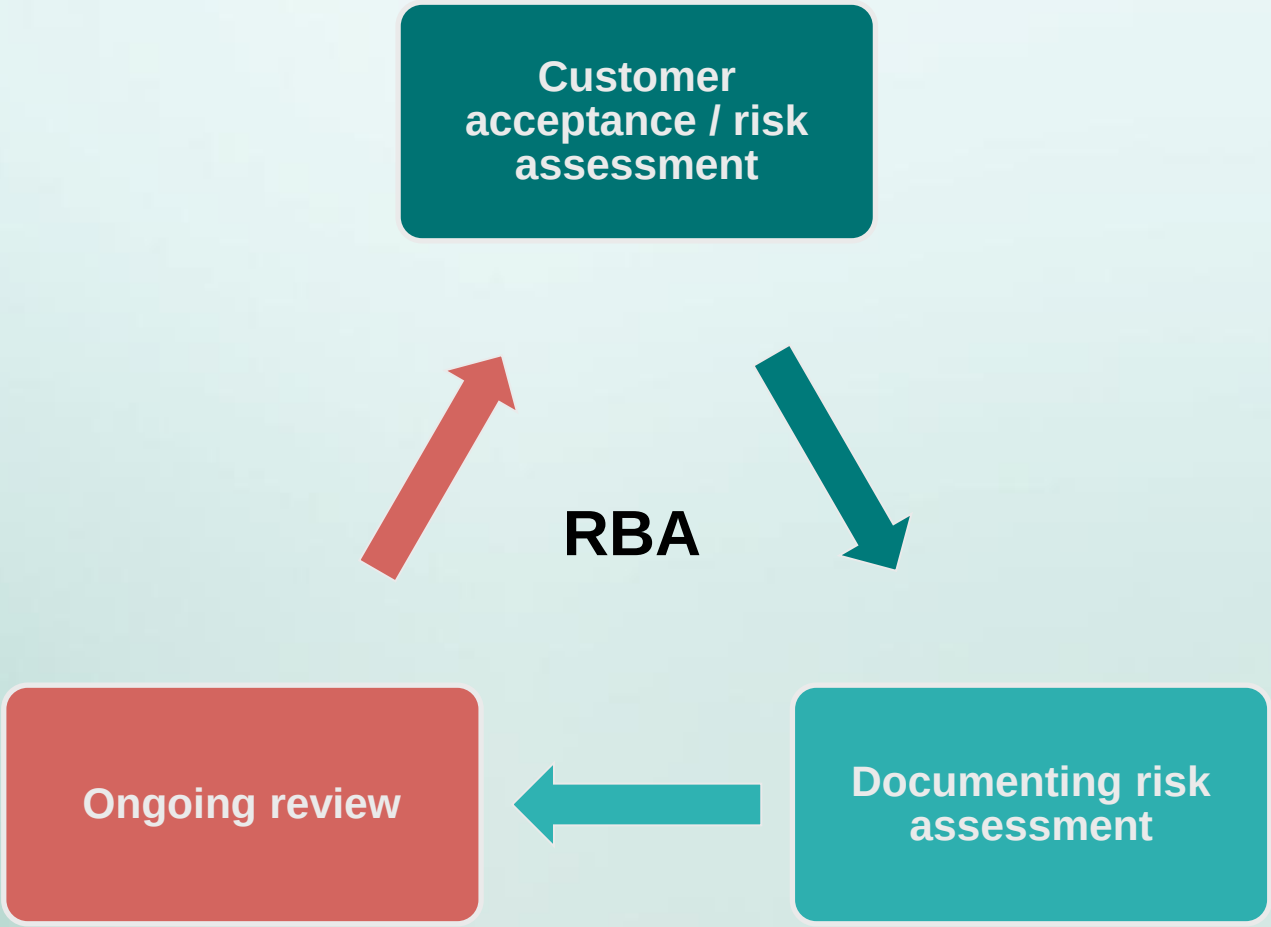


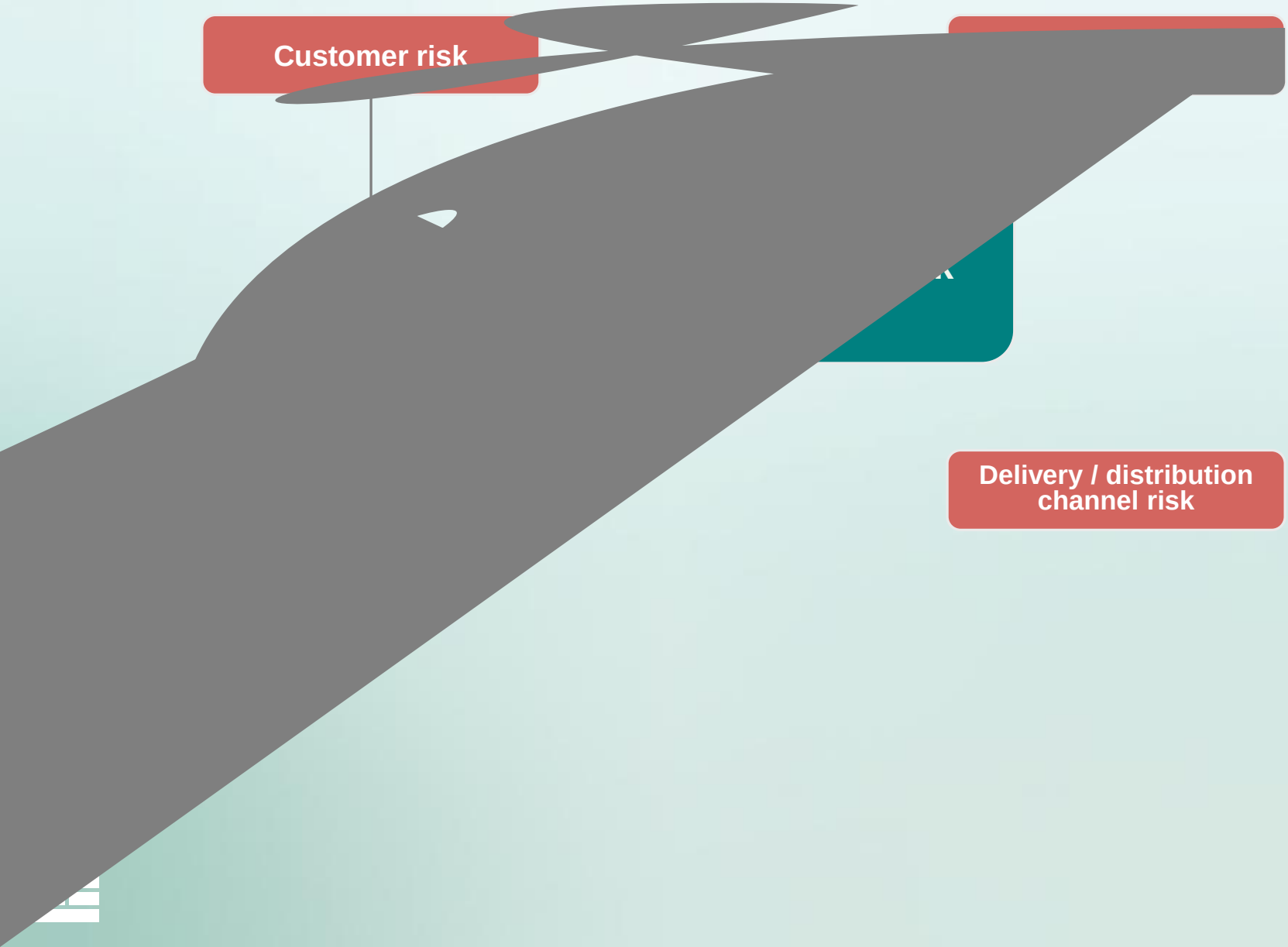
CDD and ongoing monitoring

Risk-

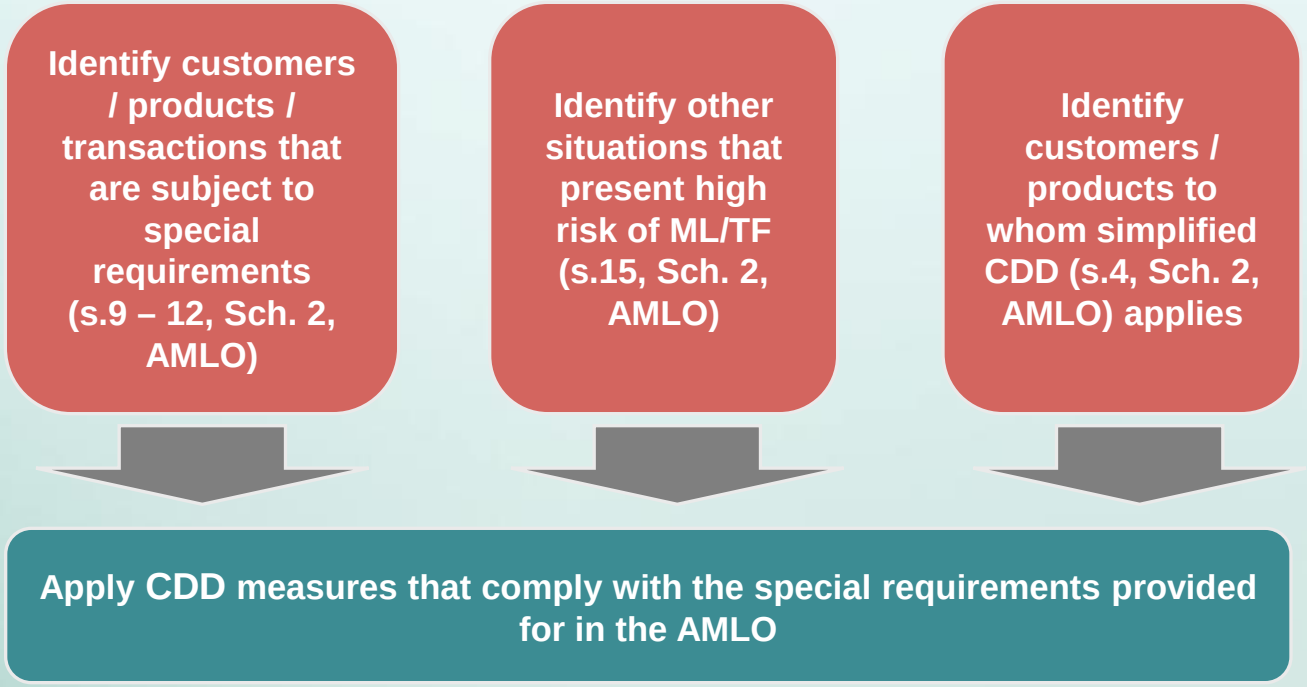
The extent of CDD and ongoing monitoring should be appropriate in view of the customer’s ML/TF risks

Customer acceptance / risk assessment




Customer risk
Delivery / distribution channel risk

CDD measures must comply with the AMLO



D. Highlights of major differences in CDD requirements between the new guidelines (Chapter 4) and the AMLGN

Identification and verification of beneficial owner (BO)

s.2(1)(b), Sch. 2, AMLO

If there is a BO in relation to the customer, FIs must identify the BO and, subject to subsection (2), take reasonable measures to verify the BO's identity so that the FI is satisfied that it knows who the BO is, including where the customer is a legal person or trust, measures to enable the FI to understand the ownership and control structure of the legal person or trust.

Simplified customer due diligence (SDD)

Meaning of SDD (s.4, Sch. 2, AMLO)

The AMLO defines what CDD measures are and also prescribes the circumstances in which an FI must carry out CDD. SDD means that application of full CDD measures is not required. In practice, this means that FIs are not required to identify and verify the beneficial owner. However, other aspects of CDD must be undertaken and it is still necessary to conduct ongoing monitoring of the business relationship. FIs must have reasonable grounds to support the use of SDD and may have to demonstrate these grounds to the relevant RA.

(Paragraph 4.10.1)

If a customer not falling within section 4(3) of Schedule 2 has in its ownership chain an entity that falls within that section, the FI is not required to identify or verify the beneficial owners of that entity in that chain when establishing a business relationship with or carrying out an occasional transaction for the customer. However, FIs should still identify and take reasonable measures to verify the identity of beneficial owners in the ownership chain that are not connected with that entity.

(Paragraph 4.10.4)

Identification and verification of a BO in relation to a legal person or trust

New guidelines	AMLGN
4.3.5 Identification requirement: 10% Verification requirement: • 25% (normal) • 10% (high risk) (s.2(2) , Sch. 2, AMLO)	**6.4.1** Identification requirement: 10% Verification requirement: 10%

BO – identification and verification requirement

Paragraph 4.3.2

Where an individual is identified as a BO, the FI should endeavour to obtain the same identification information as at paragraph 4.8.1 [for a personal customer].

Paragraph 4.3.3

The verification requirements under the AMLO are, however, different for a customer and a BO.

Paragraph 4.3.4

The obligation to verify the identity of a BO is for the FI to take reasonable measures, based on its assessment of the ML/TF risks, so that it is satisfied that it knows who the BO is.

Paragraph 4.3.6

For BOs, FIs should obtain the residential address (and permanent address if different) and may adopt a risk-based approach to determine the need to take reasonable measures to verify the address, taking account of the number of BOs, the nature and distribution of the interests in the entity and the nature and extent of any business, contractual or family relationship.

BO – multiple layer ownership structure

Paragraph 4.9.15

For companies with multiple layers in their ownership structures, an FI should ensure that it has an understanding of the ownership and control structure of the company. The intermediate layers of the company should be fully identified.

The manner in which this information is collected should be determined by the FI, for example by obtaining a director's declaration incorporating or

BO – multiple layer ownership structure

Paragraph 4.9.16

FIs need not, as a matter of routine, verify the details of the intermediate companies in the ownership structure of a company.

Complex ownership structures (e.g. structures involving multiple layers, different jurisdictions, trusts, etc.) without an obvious commercial purpose pose an increased risk and may require further steps to ensure that the FI is satisfied on reasonable grounds as to the identity of the BOs.

Paragraph 4.9.17

The need to verify the intermediate corporate layers of the ownership structure of a company will therefore depend upon

- the FI's overall understanding of the structure,
- its assessment of the risks, and
- whether the information available is adequate in the circumstances for the FI to consider if it has taken adequate measures to identify the BOs.

Identification and verification of a person purporting to act on behalf of the customer

s.2(1)(d), Sch. 2, AMLO

If a person purports to act on behalf of the customer, FIs must:

- identify the person and take reasonable measures to verify the person's identity; and
- verify the person's authority to act on behalf of the customer.

Identification and verification of a person purporting to act on behalf of the customer

New guidelines	AMLGN

4.4.1 to 4.4.4
• Requirement - Identify and verify the identity of any person purporting to act on behalf of the customer
• Where difficulty in identifying and verifying long lists of account signatories is encountered
  • Streamlined approach may be adopted based on RBA
• Other situations
  • Verify all
 	
(s.2(1)(d), Sch. 2, AMLO)
	6.4.1(e)
	Obtain:
	• copies of identification documents of at least 2 authorised persons

custom9d1 0 0 1 61.2 498.36 Tm0.19 0.51 0.s1 0 0 Tc.45

Timing of identification and verification of identity

When customer due diligence measures must be carried out (s.3, Sch. 2, AMLO)

Paragraph 4.7.1

An FI must complete the CDD process before establishing any business relationship or before carrying out a specified occasional transaction

New guidelines	AMLGN
4.7.8 Verification of identity should be concluded within a reasonable timeframe. Examples are: (a) Completing verification no later than 30 working days; (b) Suspending business relations if such verification remains uncompleted after 30 working days; (c) Terminating business relations if such verification remains uncompleted after 120 working days (s.3(2), (3) &(4)(b), Sch. 2 of AMLO)	**6.1.10**

Corporate customers

Paragraph 4.9.9

An FI should record the names of all directors and verify the identity of directors on a risk-based approach.

Paragraph 4.9.10

FIs should:

- confirm the company is still registered and has not been dissolved, wound up, suspended or struck off;
- independently identify and verify the names of the directors and shareholders recorded in the company registry in the place of incorporation; and
- verify the company's registered office address in the place of incorporation.

Corporate customers

Three verification methods for a company incorporated overseas:

- a similar company search enquiry of the registry in the place of incorporation and obtain a company report;
- a certificate of incumbency or equivalent issued by the company's registered agent in the place of incorporation; or

Local and foreign financial institutions

SDD – local and foreign FIs (s.4(3), Sch. 2, AMLO)

FIs may apply SDD to a customer that is an FI as defined in the AMLO, or an institution that carries on a business similar to that carried on by an FI and meets the criteria set out in section 4(3)(b) of Schedule 2. If the customer does not meet the criteria, the FI must carry out all the CDD measures set out in section 2 of Schedule 2

Provided that certain conditions are met, FIs may apply SDD to a customer that is an FI as defined in the AMLO that opens an account:

- in the name of a nominee company for holding fund units; or
- in the name of an investment vehicle in the capacity of a service provider.

(Paragraph 4.10.6)

Solicitor’s client accounts

SDD - oom[-3(r ol)-it)--2(o)-(r)7rm to1s,t6I i-

Local and foreign financial institutions / solicitor's client accounts

New guidelines	AMLGN
4.10.6 Not required to identify and verify the BOs including underlying customers of a customer that is an FI only if the customer is a specified local FI or an overseas FI customer who is: • from an equivalent jurisdiction; • has measures in place to ensure compliance with requirements similar to Sch. 2 to the AMLO; and • supervised for compliance with those requirements by an authority similar to any of the RAs (s.4(3)(a) & (b), Sch. 2, AMLO) **4.10. 17** Restrict the application of SDD to the client account of a customer that is a solicitor or a firm of solicitors in which moneys or securities of the customer's clients are mingled.	

Investment vehicles

SDD – investment vehicle (s.4(3)(d), Sch. 2, AMLO)

FIs may apply SDD to a customer that is an investment vehicle if the FI is able to ascertain that the person responsible for carrying out measures that are similar to the CDD measures in relation to all the investors of the investment vehicle falls within any of the categories of institution set out in section 4(3)(d) of Schedule 2.

(Paragraph 4.10.9)

Customers not physically present for identification purposes

Special requirements when customer is not physically present for identification purposes (s.9, Sch. 2, AMLO)

FIs are required to take additional measures to compensate for any risk associated with customers not physically present for identification purposes.

FIs must carry out at least one of the following measures:

- further verifying the customer's identity on the basis of documents, data or information not previously used for the purposes of verification of the customer's identity;
- taking supplementary measures to verify all the information provided by the customer;
- ensuring that the first payment made into the customer's account is received from an account in the customer's name with
  - an authorized institution or
  - a bank operating in an equivalent jurisdiction that has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2 and is supervised for compliance with those requirements by a banking regulator in that jurisdiction.

Consideration should be given on the basis of the ML/TF risk to obtaining copies of documents that have been certified by a suitable certifier.

(Paragraph 4.12.2)

Customers not physically present for identification purposes

Supplementary guidance specific to the securities sector

In taking additional measures to mitigate the risks posed by customers not physically present for identification purposes, reference should be made by LCs to the relevant provisions (presently paragraph 5.1) in the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission concerning account opening procedures for customers who are not physically present for identification purposes.

(Paragraph 4.12.2(a))

Other examples of suitable certifiers

Besides what is provided in the abovementioned Code of Conduct, other examples are:

a) an intermediary specified in s18(3) of Schedule 2;

b) a member of the judiciary in an equivalent jurisdiction;

c) an officer of an embassy, consulate or high commission of the country of issue of documentary verification of identity; and

Foreign Politically Exposed Persons (PEPs)

Special requirements when a customer is PEP (s.5(3)(b) &10, Sch. 2 , AMLO)

When FIs know that a particular customer or beneficial owner is a PEP*, it should, before (i) establishing a business relationship or (ii) continuing an existing business relationship where the customer or the beneficial owner is subsequently found to be a PEP, apply the following additional measures (referred to as enhanced customer due diligence (EDD) measures):

a) obtain approval from its senior management; and

b) take reasonable measures to establish the customer's or the beneficial owner's source of wealth and the source of the funds; and

c) apply enhanced monitoring to the relationship in accordance with the assessed risks.

(Paragraph 4.13.11)

** An individual who is or has been entrusted with a prominent public function in a*

a parent, a spouse or a partner of a child, or a close associate of the individual

Domestic Politically Exposed Persons (Domestic PEPs)

High risk situation (s.15, Sch. 2, AMLO)

While the statutory definition of PEPs in the AMLO only includes individuals entrusted with prominent public function in a place outside the People's Republic of China , domestic PEPs may also present, by virtue of the positions they hold, a high risk situation where EDD should be applied.

FIs should therefore adopt a risk-

PEPs

New guidelines	AMLGN
4.13 Separate requirements for foreign and domestic PEPs • PEPs outside the People's Republic of China EDD (Paragraphs 4.13.11) • Domestic PEPs EDD on RBA (Paragraphs 4.13.3)	**6.9.1** Both foreign and domestic PEPs EDD

Jurisdictional equivalence

Definition of equivalent jurisdiction (s.1, Sch. 2, AMLO)

Equivalent jurisdiction is defined in the AMLO as meaning:

a) a jurisdiction that is a member of the FATF, other than Hong Kong; or

b) a jurisdiction that imposes requirements similar to those imposed under Schedule 2.

(Paragraph 4.20.2)

Determination of jurisdictional equivalence

FIs should evaluate and determine for themselves which jurisdictions other than FATF members apply requirements similar to those imposed under Schedule 2 for jurisdictional equivalence purposes.

Factors that may be considered when conducting such evaluations are found in paragraph 4.20.3.

An FI should document such evaluations.

(Paragraph 4.20.3)

Jurisdictional equivalence

New guidelines	AMLGN
4.20.1 Jurisdictional equivalence -> any jurisdiction that imposes CDD requirements similar to those imposed in AMLO. (s.1, Sch. 2, AMLO)	**Glossary** Equivalent jurisdiction -> applies AML/CFT standards equivalent to those of the FATF

“Similarity test”

In assessing whether requirements are similar to those imposed under Schedule 2 to the AMLO, FIs should focus on the “substance” of the requirements, rather than the granular details, i.e. similar but no need to be identical

E. Ongoing monitoring (Chapter 5)

Duty to continuously monitor business relationships (s.5(1), Sch. 2, AMLO)

An FI must continuously monitor its business relationship with a customer by:

Risk-based approach to monitoring

FIs must take additional measures when monitoring business relationships that pose a higher risk. High-risk relationships, for example those involving PEPs, will require more frequent and intensive monitoring

Resources should be targeted towards business relationships presenting a higher risk of ML/TF

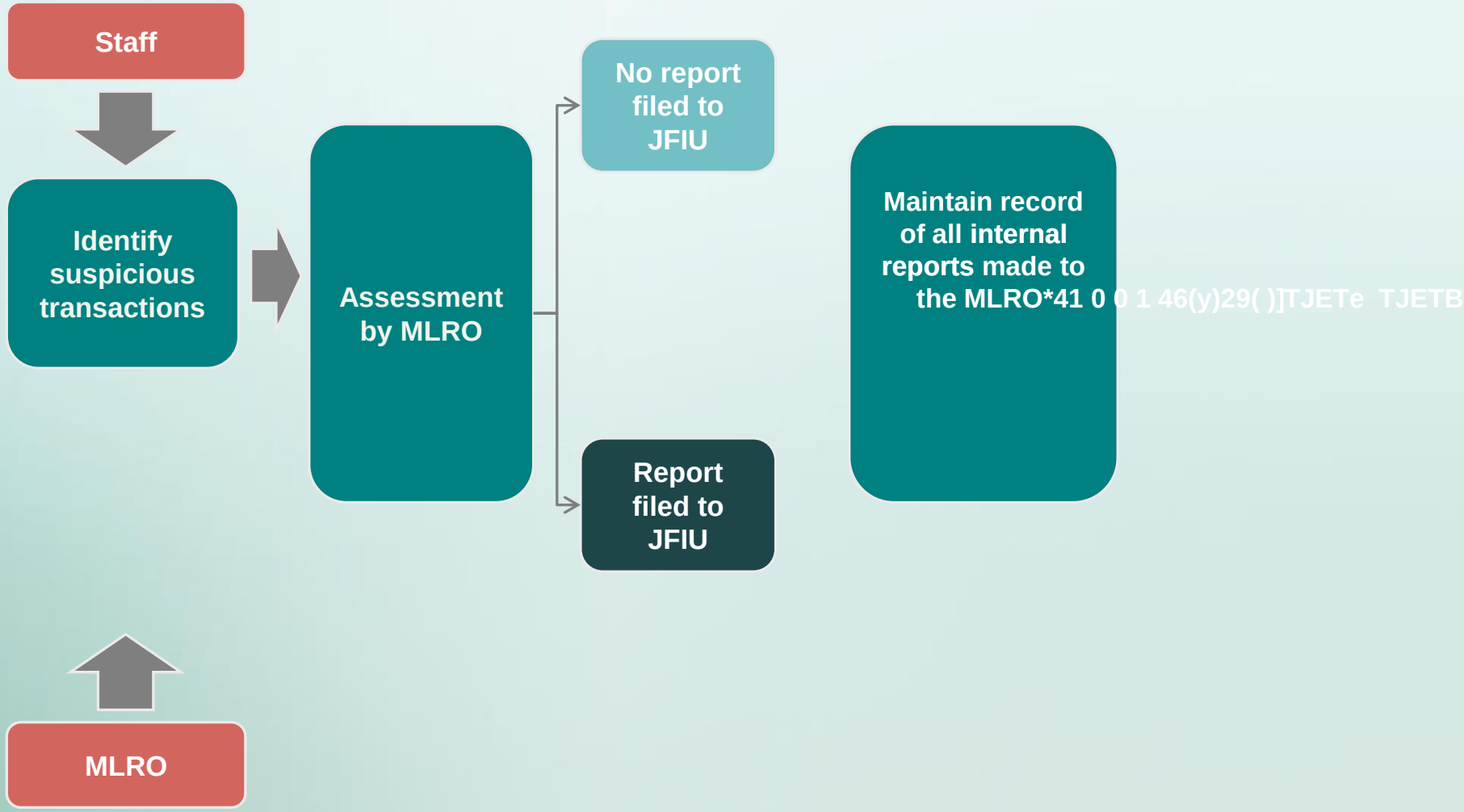
(Paragraphs 5.7 & 5.8)

Keeping customer information up-to-date

Duty to continuously monitor business relationships (s.5(1)(a), Sch. 2, AMLO)

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

Overview of suspicious transactions reporting (STR) process



susp.2340 c7 10 0 1 1.2340 1c[susp.2340 1c[susp.2340 c7 10 0 1 1.2340 lh541 09)1.2340 lh541 09)1.2340 lh43 c5

Examples of suspicious transactions

Paragraph 7.14 provides examples of suspicious transactions not different from those provided by HKMA, OCI, and C&ED under their guidelines.

Paragraphs 7.39 and 7.40 provide other examples that are specific to the securities sector and grouped into:

- Customer related
- Trading related
- Settlement/custody/transfers-related
- those involving employees of LCs

Not exhaustive and only provides examples of the most basic ways in which money may be laundered

G. Record-keeping (Chapter 8)

AMLO requirements

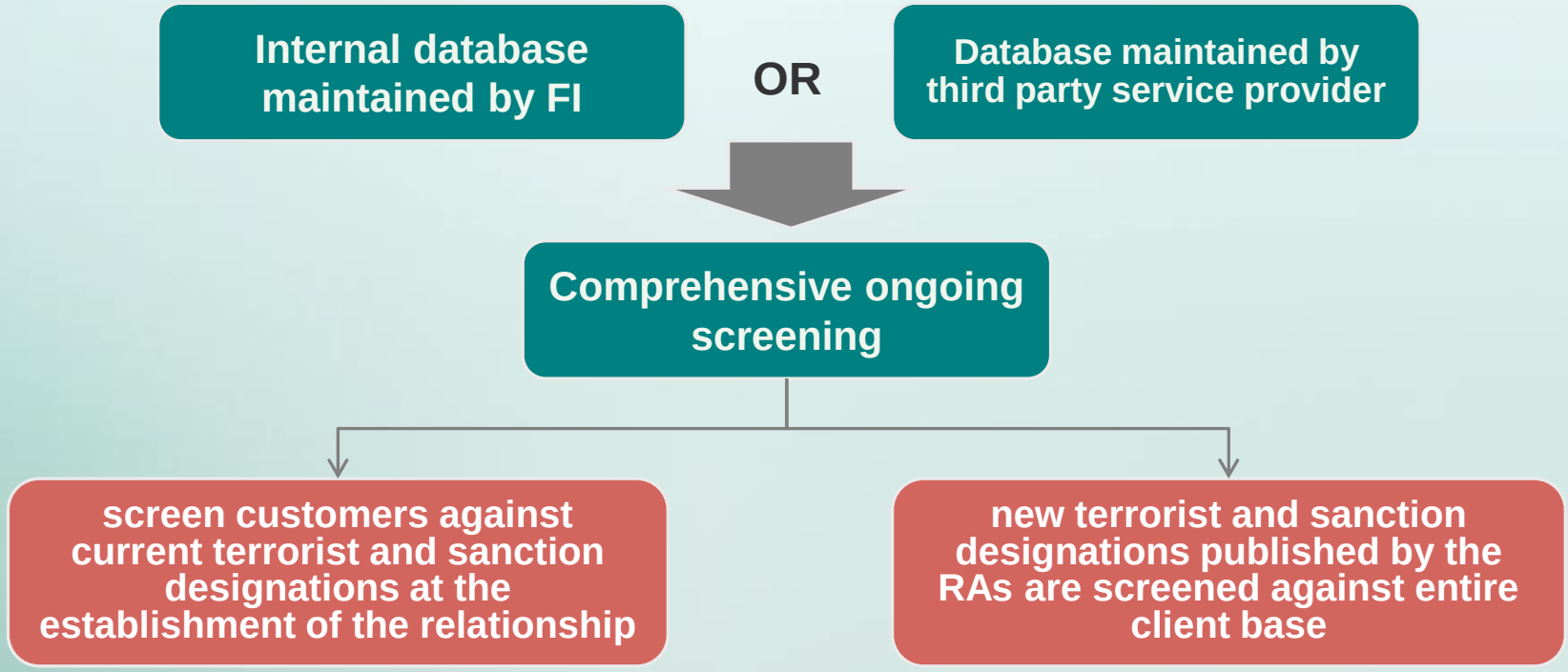
Record retention period

New guidelines	AMLGN
8.4 CDD documents and records mentioned on paragraph 8.3 are required to be kept for at least six years after the account is closed. (s.20(3), Sch. 2 of AMLO)	**8.1** The retention period for such documents and records is at least five years after the account is closed.
8.6 Documents and records on transactions are required to be kept for at least six years after the transaction is completed. (s.20(2), Sch. 2, AMLO)	**8.1** The retention period for such documents and records on transactions is at least seven years.

8(fina)-2(ncing[ ])]TJETBT1 0 0 491.44 298251 a)Tc[ ])]TJ

Financial sanctions and terrorist financing

FIs should be able to identify and report transactions with terrorist suspects and designated parties



I. Wire transfers (Chapter 10)

Wire transfers

Primarily applies to authorized institutions and money service