



SECURITIES AND
FUTURES COMMISSION
證券及期貨事務監察委員會

Key compliance issues on Anti-Money Laundering and Counter- Terrorist Financing (“AML/CFT”)

October 2012

Jeffrey Chan

Senior Manager, Intermediaries Supervision Department

Ivan Wan

Manager, Intermediaries Supervision Department

Disclaimer

This presentation is intended to provide the audience with a broad overview of certain aspects of the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance's (AMLO) customer due 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. Status update since 1 April 2012
- B. Common deficiencies and observations identified in the past inspections
- C. Monitoring and reporting of suspicious transactions



A. Status update since 1 April 2012



Status update since 1 April 2012

- The AMLO, among others, codifies requirements relating to CDD and record-keeping for specified financial institutions (“FIs”).
- Guideline on Anti-Money Laundering and Counter-Terrorist Financing (“the Guideline”) was published under section 7 of the AMLO and section 399 of the SFO.
- Frequently Asked Questions on the AMLO and the Guideline was issued.
- SFC Disciplinary Fining Guidelines under the AMLO was published on 29 June 2012 and comes to effect on 1 July 2012.
- On 13 July 2012, the Guideline was amended to reflect amendments made to United Nations (Anti-Terrorism Measures) Ordinance and the AMLO.

Status update since 1 April 2012

- SFC is updating the AML/CFT self-assessment questionnaire, which will be posted to our web-site in due course.
- SFC is reviewing the revised FATF Recommendations published in February 2012.

B. Common deficiencies and observations identified in the past inspections

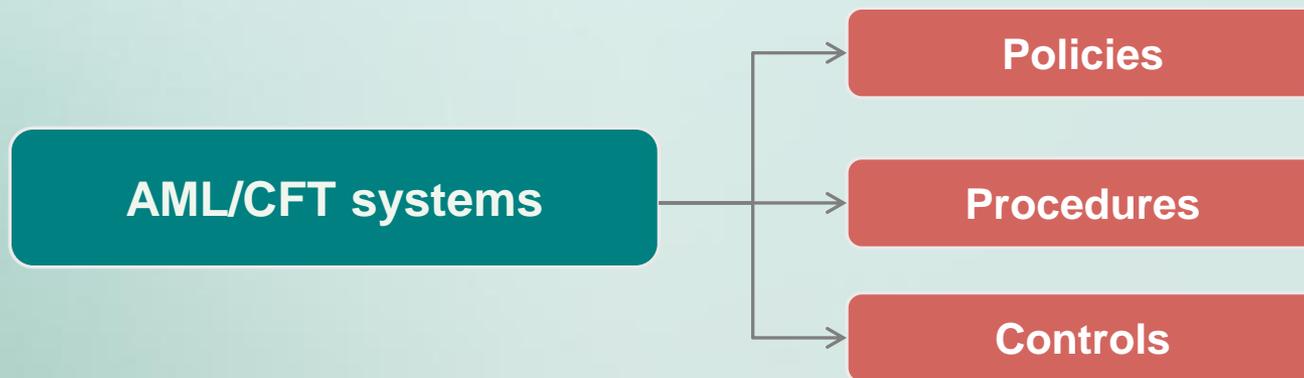


AML/CFT systems

AML/CFT policies and procedures

- Failure to tailor to firm's own circumstances and AML risk exposure
- Directly copy from the Guideline without outlining detailed procedures and controls
- Failure to incorporate key AML/CFT measures, e.g. conducting company search, PEPs screening, conducting additional measures to mitigate the risks in high risk situations, etc

Paragraph 2.1 of the Guideline

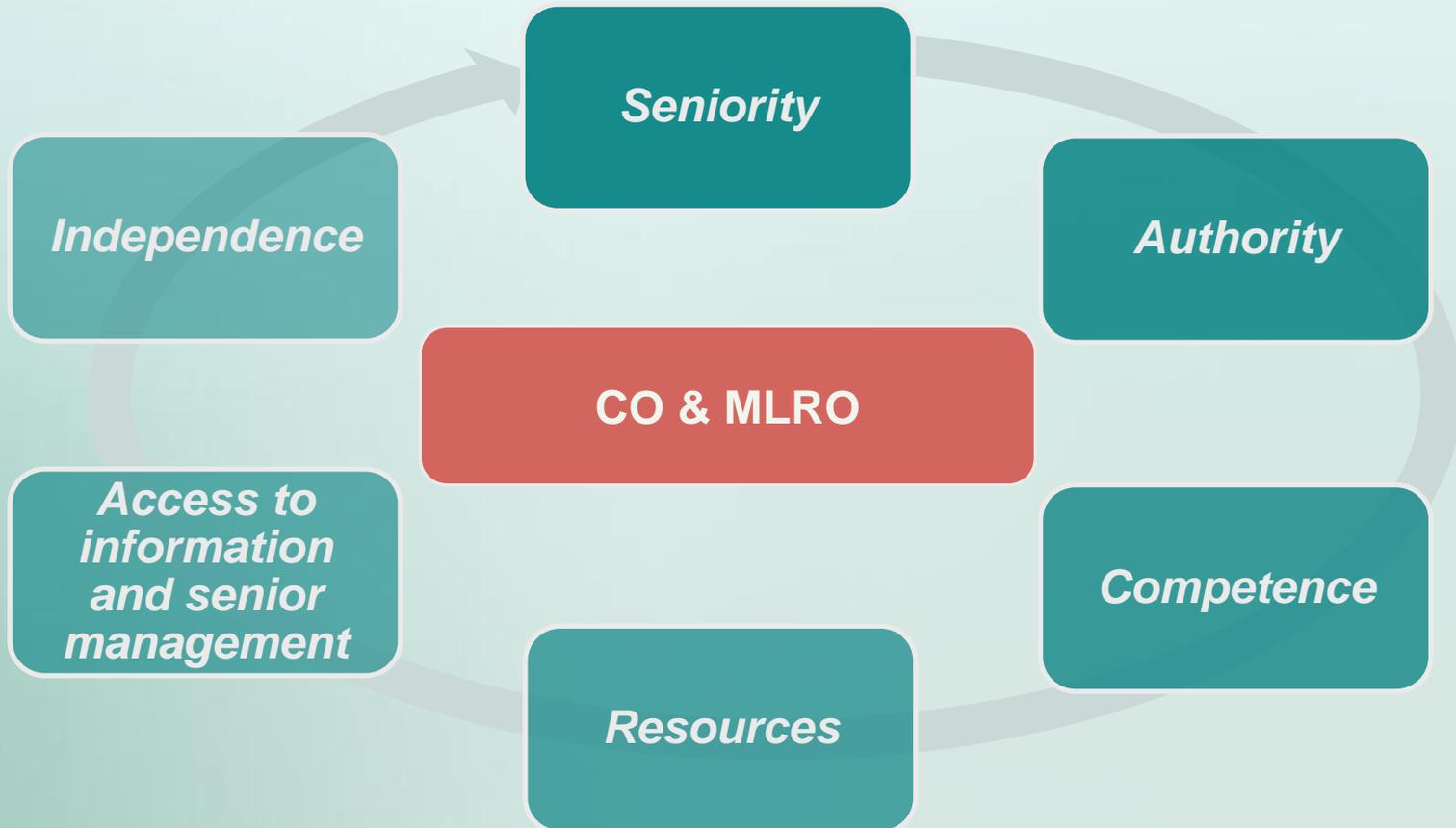


AML/CFT systems

Compliance Officer (“CO”) and Money Laundering Reporting Officer (“MLRO”)

- Appointment of an independent CO / MLRO

Paragraph 2.12 of the Guideline

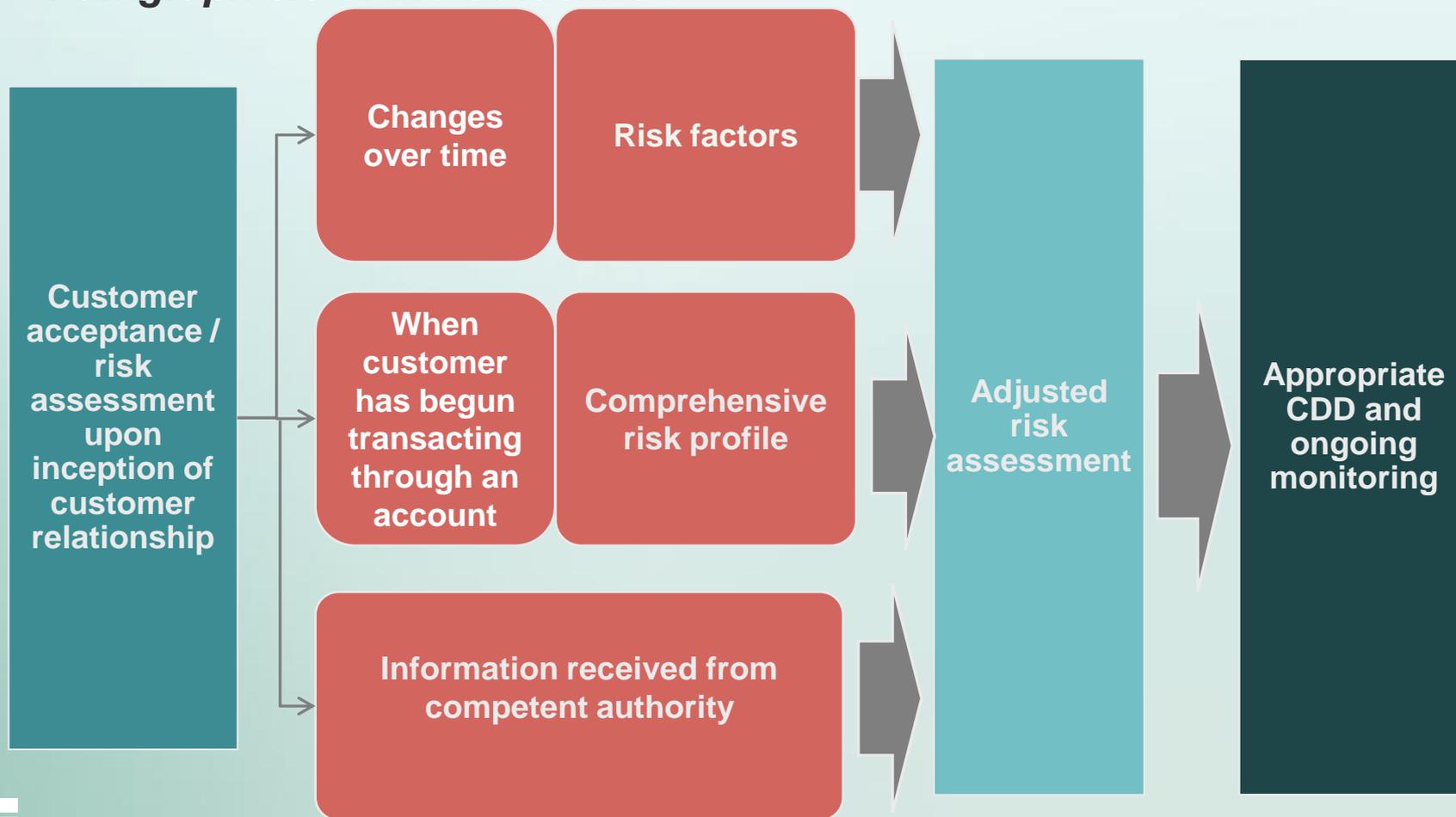


Risk based approach (“RBA”)

Risk assessment

- Failure to perform an on-going risk assessment on customers

Paragraph 3.6 of the Guideline

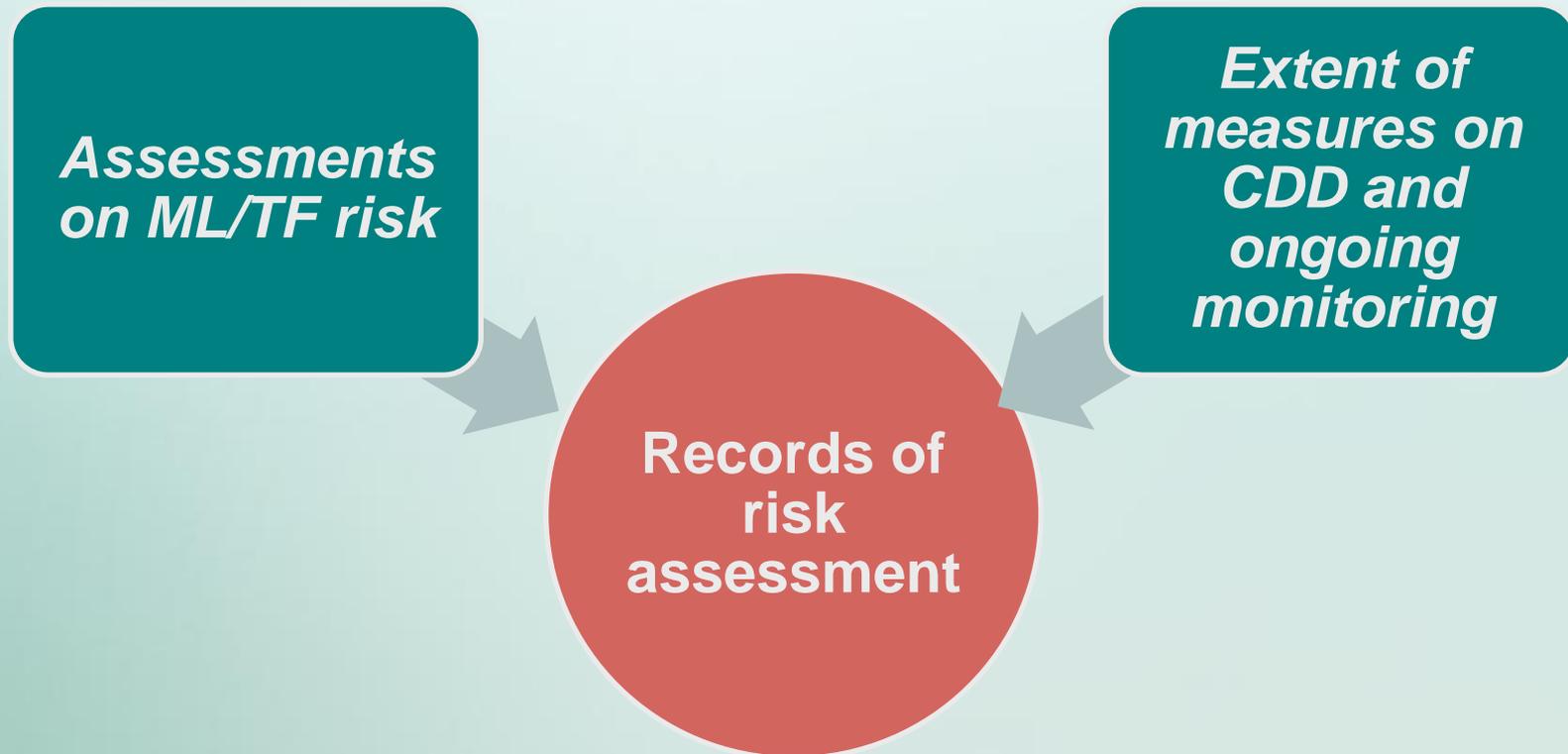


RBA

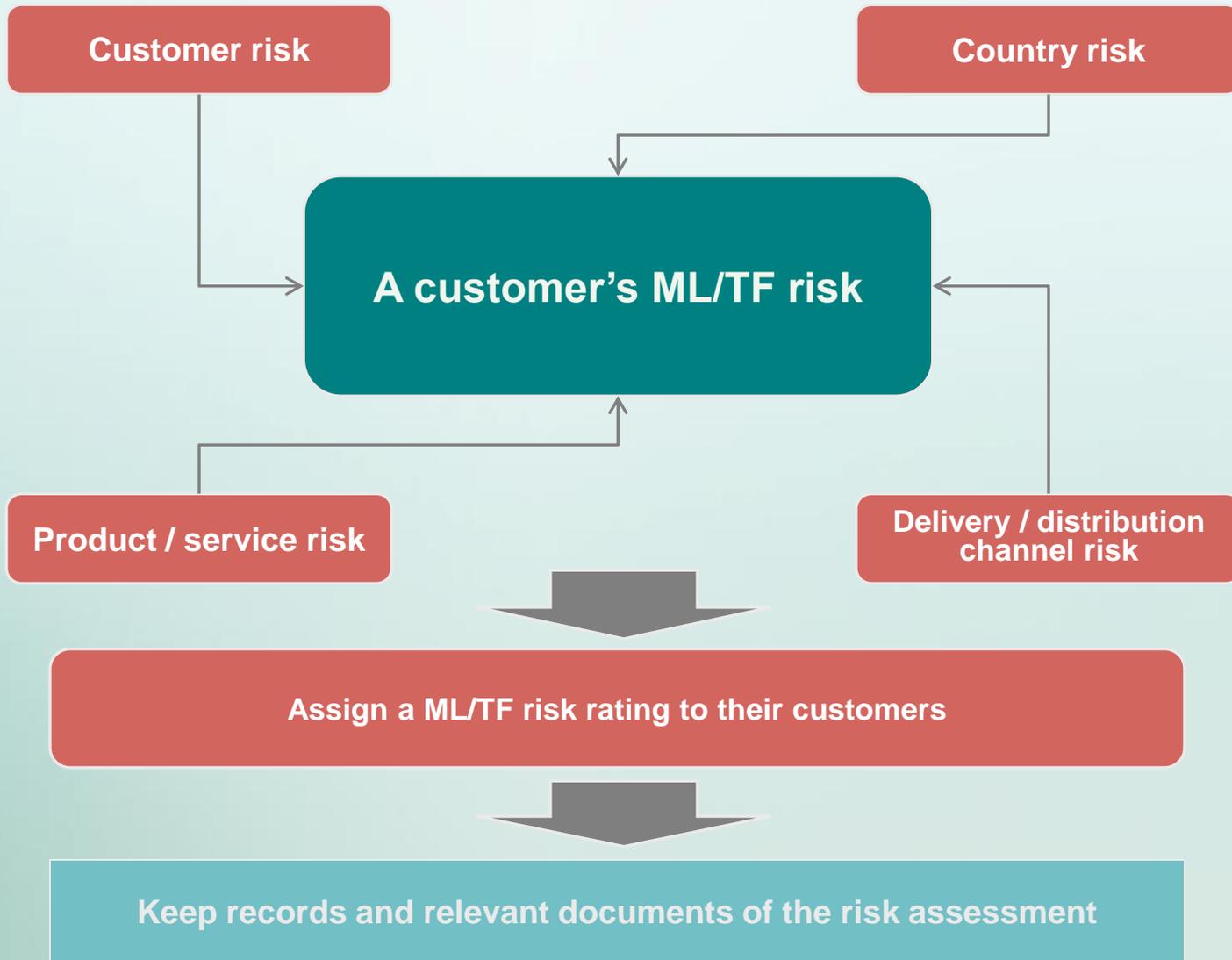
Documentation of risk assessment

- Failure to document the risk assessment

Paragraph 3.8 of the Guideline



RBA



CDD – Timing of identification and verification of identity

Common practice

- Account was not allowed to trade until all supporting documents have been obtained from customers.

Paragraphs 4.7.4 & 6 of the Guideline; s.3, Sch.2 of the AMLO

- 
- Where a customer is permitted to trade prior to verification

- 
- FIs should adopt appropriate risk management policies and procedures

CDD – Natural persons

Use of appropriate address proof

- List of examples of address proof is provided in paragraph 4.8.10.

Paragraph 4.8.10 of the Guideline

- The examples include:

a recent utility bill issued within the last 3 months

**recent correspondence from a Government department
or agency**

**a statement, issued by an authorized institution, a
licensed corporation or an authorized insurer within the
last 3 months**



CDD - Person purporting to act on behalf of the customer

Streamlined approach

- Application of streamlined approach

Paragraph 4.4.4 of the Guideline

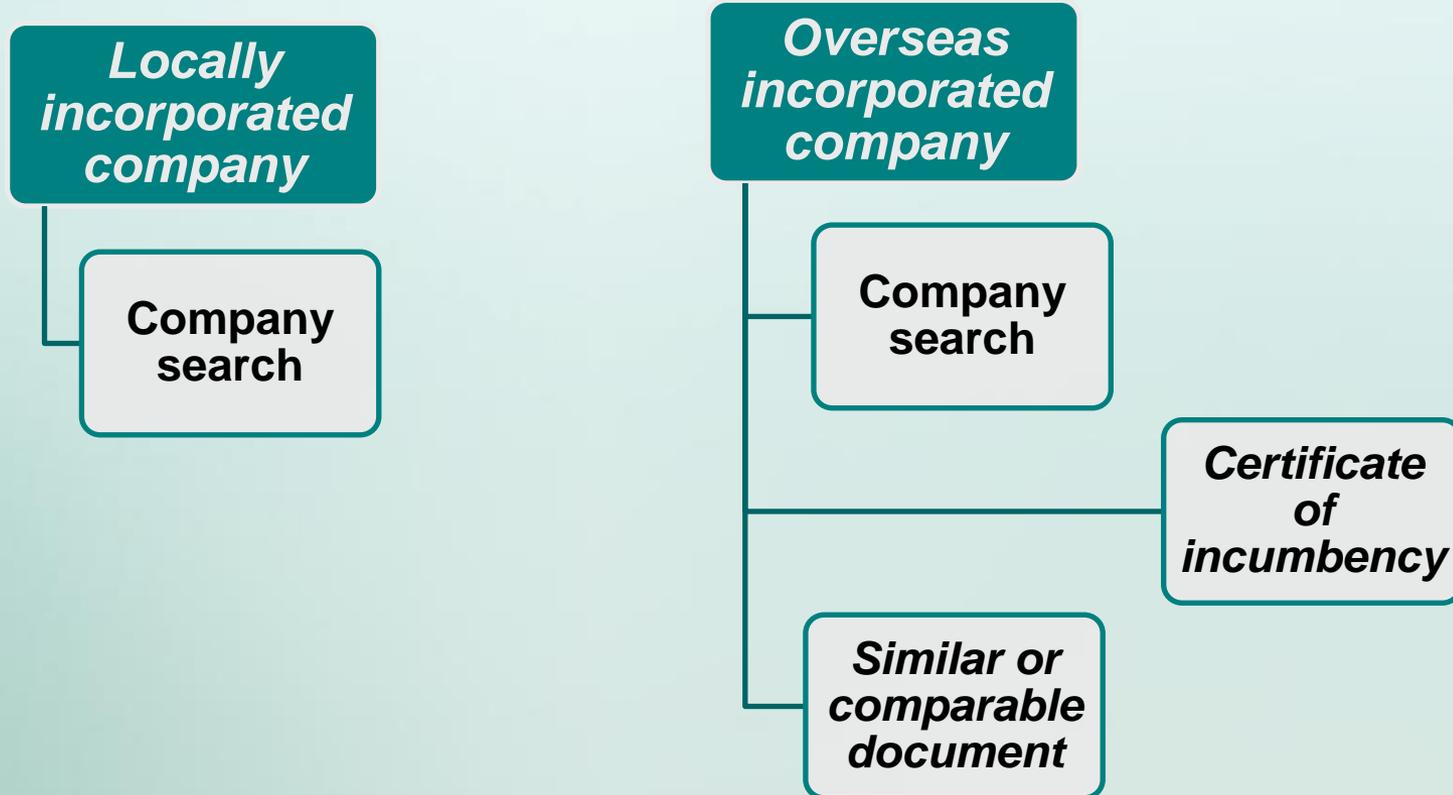


CDD – Legal persons

Conducting company search

- Failure to conduct company search for corporate customers

Paragraph 4.9.11 of the Guideline

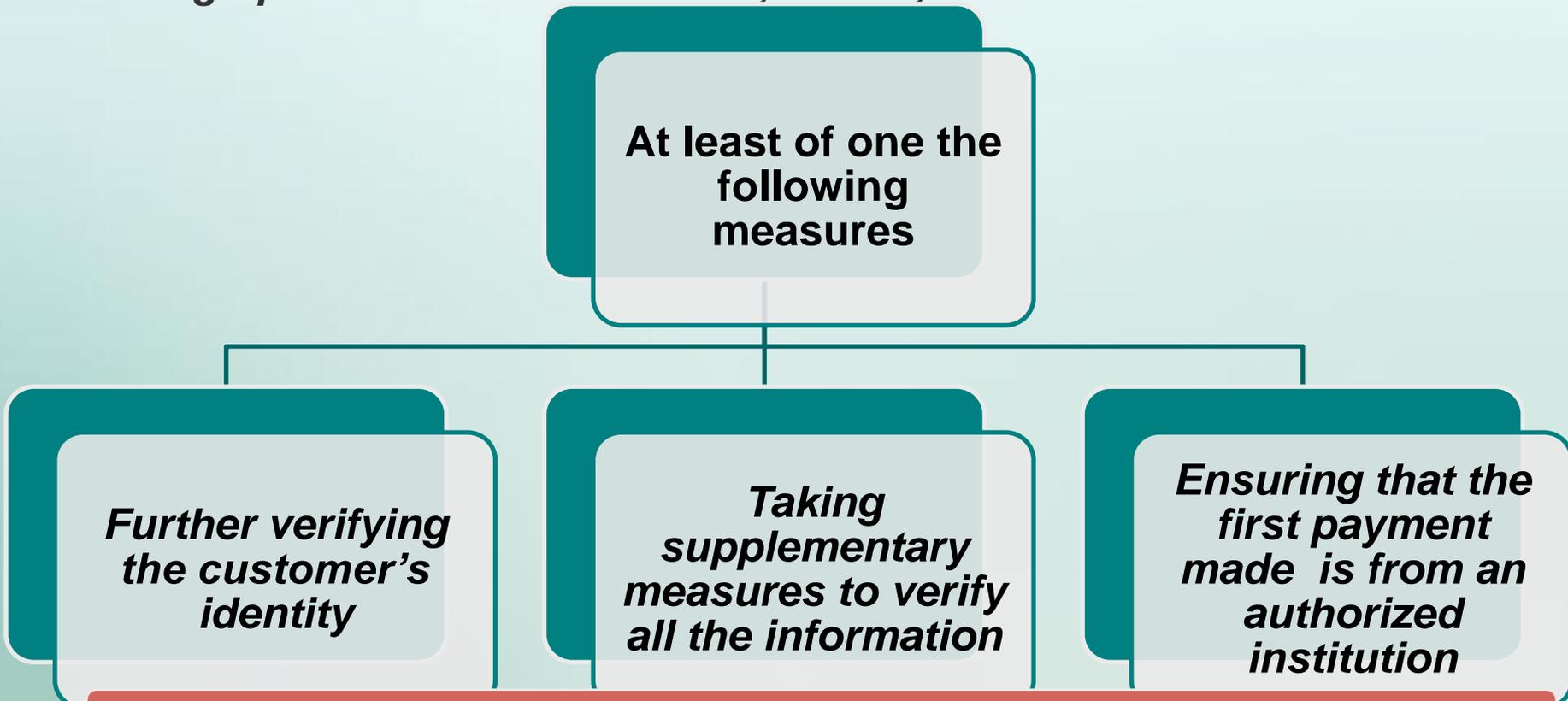


CDD - Customers not physically present for identification purposes

Additional measures

- Implementation of proper measures on customers not physically present for identification purposes

Paragraph 4.12.2 of the Guideline; s.5 & 9, Sch.2 of the AMLO



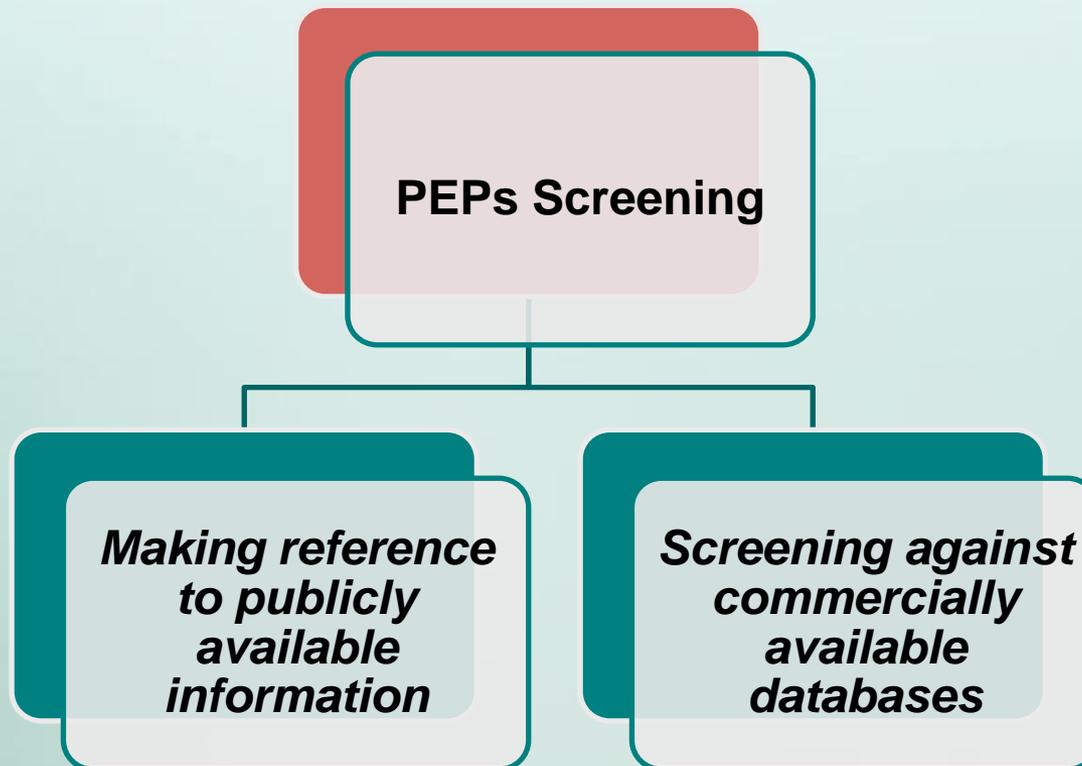
Reference should be made to the relevant provisions (presently paragraph 5.1) in the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission.

CDD - Politically exposed persons (“PEP”)

PEPs screening

- Insufficient controls on PEPs screening - solely relying on the background information provided by the customers

Paragraphs 4.13.9 of the Guideline; s.19, Sch.2 of the AMLO



CDD - Jurisdiction equivalence

Jurisdiction equivalence

- Failure to document the assessment of jurisdiction equivalence of non-FATF members

Paragraph 4.20.3 of the Guideline

FIs evaluate and determine which jurisdictions other than FATF members apply requirements similar to those imposed under Schedule 2 of the AMLO for jurisdictional equivalence purposes



Document the assessment

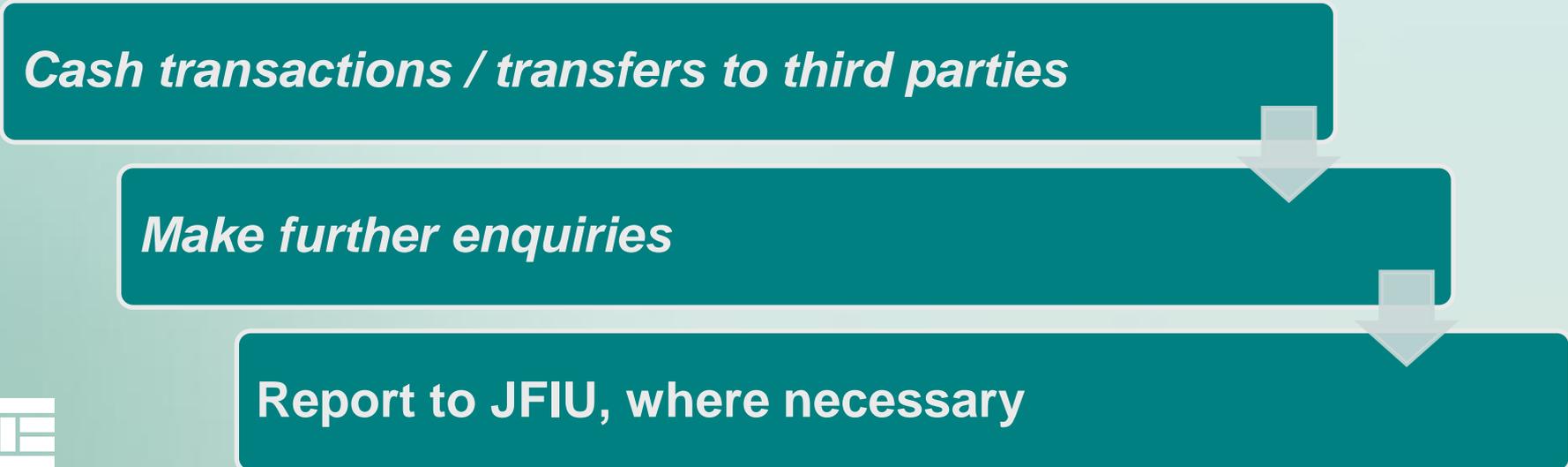
On-going monitoring

Common practices: examples on controls for third party transfer

- Obtaining cheque copy for deposit over a threshold
- Returning third party fund by transferring back to the third party
- Obtaining verbal declaration on whether the cheque deposit is made by third party
- For third party withdrawal, obtaining management approval, inquire about the reasons for the payment and the relationship between the customer and the third party

Paragraph 5.12 of the Guideline

Cash transactions / transfers to third parties



Make further enquiries

Report to JFIU, where necessary



On-going monitoring

Common practices: Examples on generation of exception reports

- Identify customers with changing transaction pattern through the comparison of monthly turnover of 2 consecutive months
- Identify customers with large fund deposit / withdrawal
- Identify cash receipt

Paragraph 5.9 of the Guideline

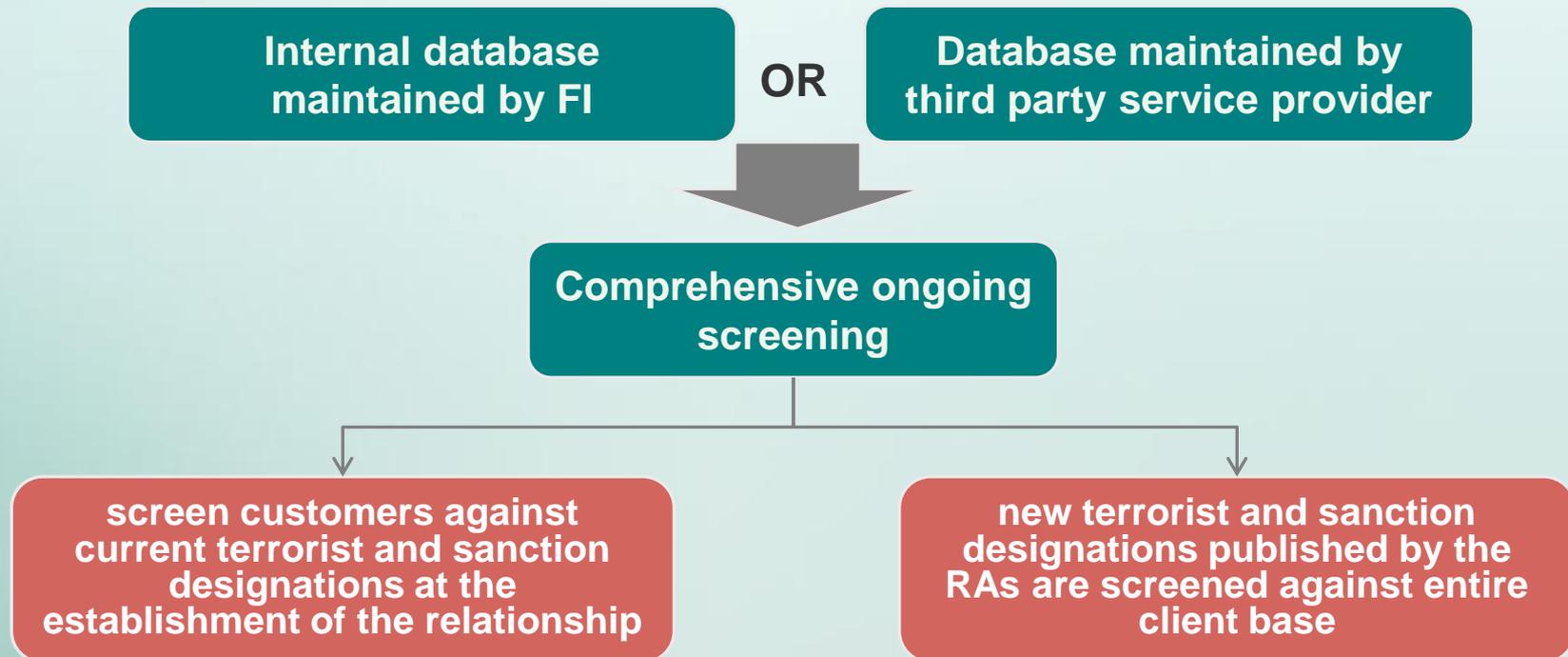
- ***Methods to monitor customer transactions and activities include exception reports (e.g. large transactions exception report) and transaction monitoring systems.***

Financial sanctions and terrorist financing

Monitoring of terrorist suspects and designated parties

- Implementation of an appropriate system in screening customers against terrorist suspects and designated parties

Paragraphs 6.20 & 6.22 of the Guideline

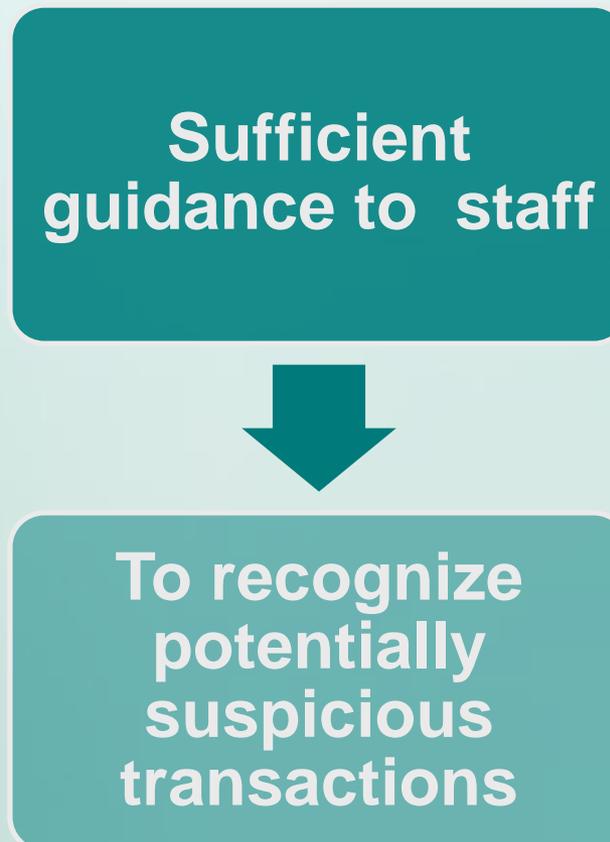


Suspicious transaction reports

Monitoring and reporting of suspicious transactions

- No sufficient guidance is given to staff

Paragraph 7.7 of the Guideline

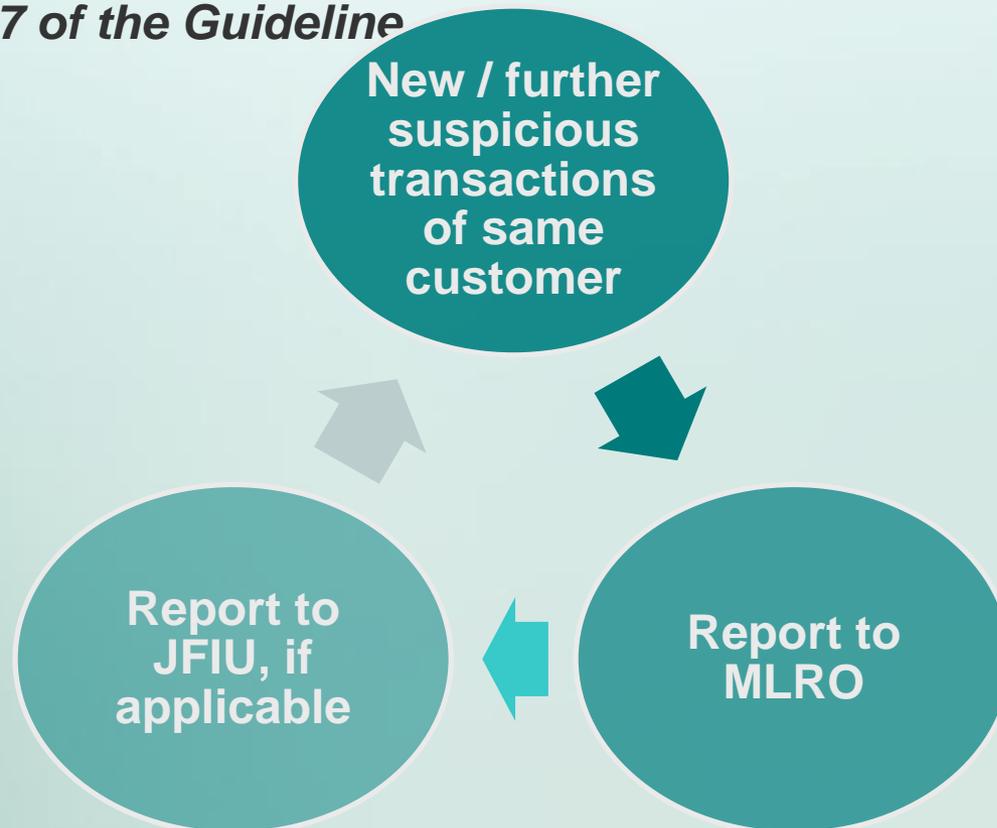


Suspicious transaction reports

Monitoring and reporting of suspicious transactions

- Failure to make report on further suspicious transactions of the same nature in relation to the previous suspicion to the Joint Financial Intelligence Unit (“JFIU”)

Paragraph 7.27 of the Guideline



Suspicious transaction reports

Monitoring and reporting of suspicious transactions

- Failure to establish and maintain records of all ML/TF reports made to MLRO

Paragraph 7.31 of the Guideline

```
graph TD; A[ML/TF reports made to MLRO] --> B[Documentation]
```

**ML/TF reports
made to MLRO**

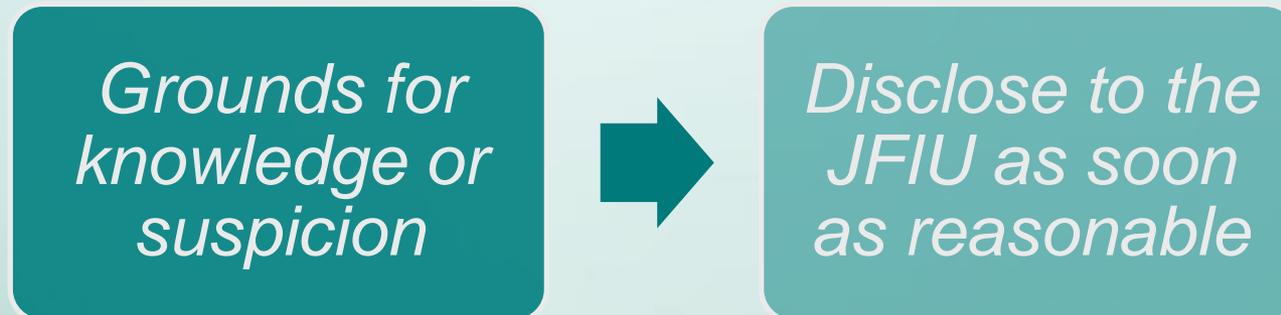
Documentation

Suspicious transaction reports

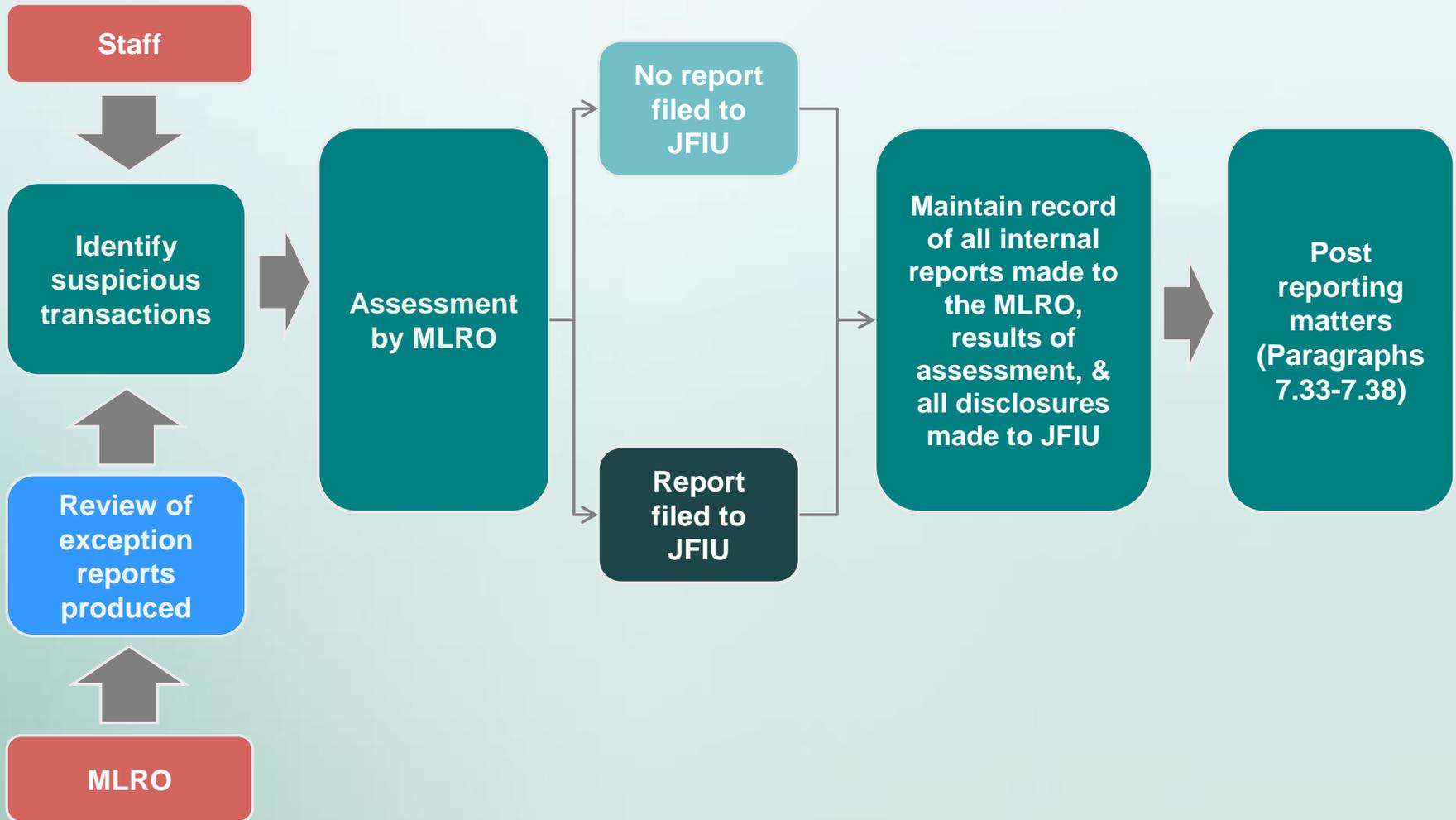
Monitoring and reporting of suspicious transactions

- Failure to timely report suspicious transactions to the JFIU

Paragraph 7.30 of the Guideline



Overview of suspicious transactions reporting (STR) process

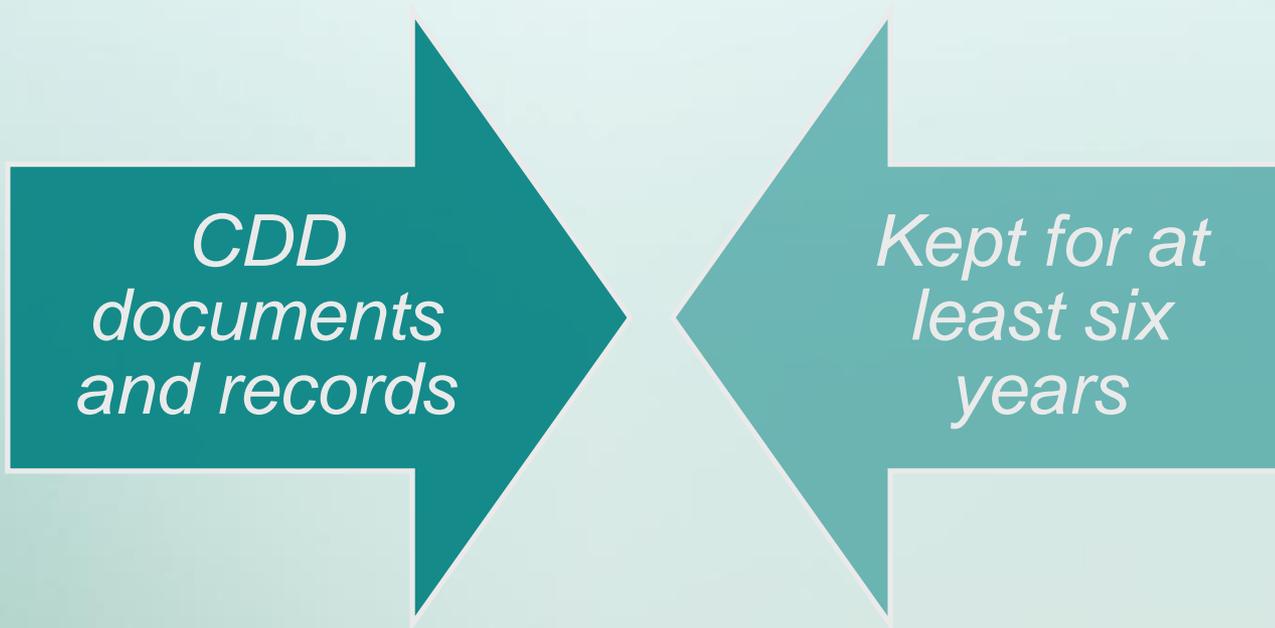


Record-keeping

Common practices

- Account opening files retained for an indefinite period

Paragraph 8.4 of the Guideline; s.20, Sch.2 of the AMLO

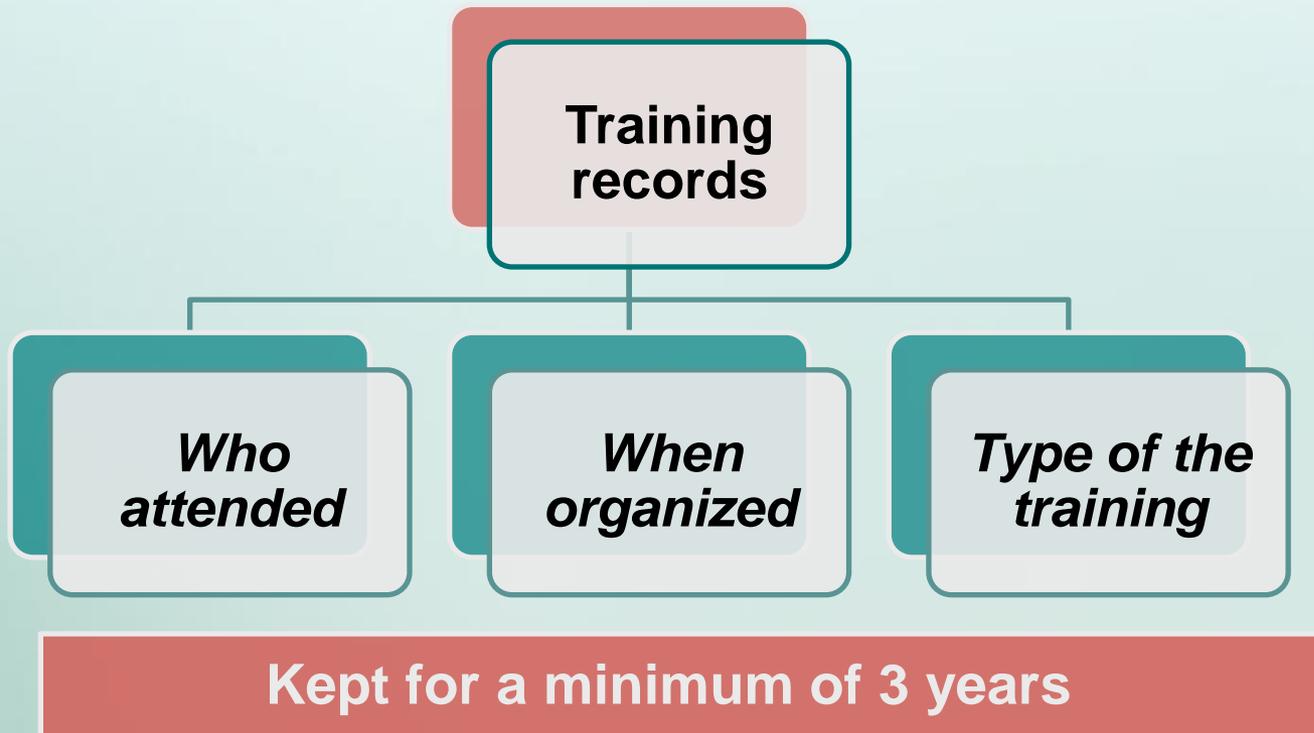


Staff training

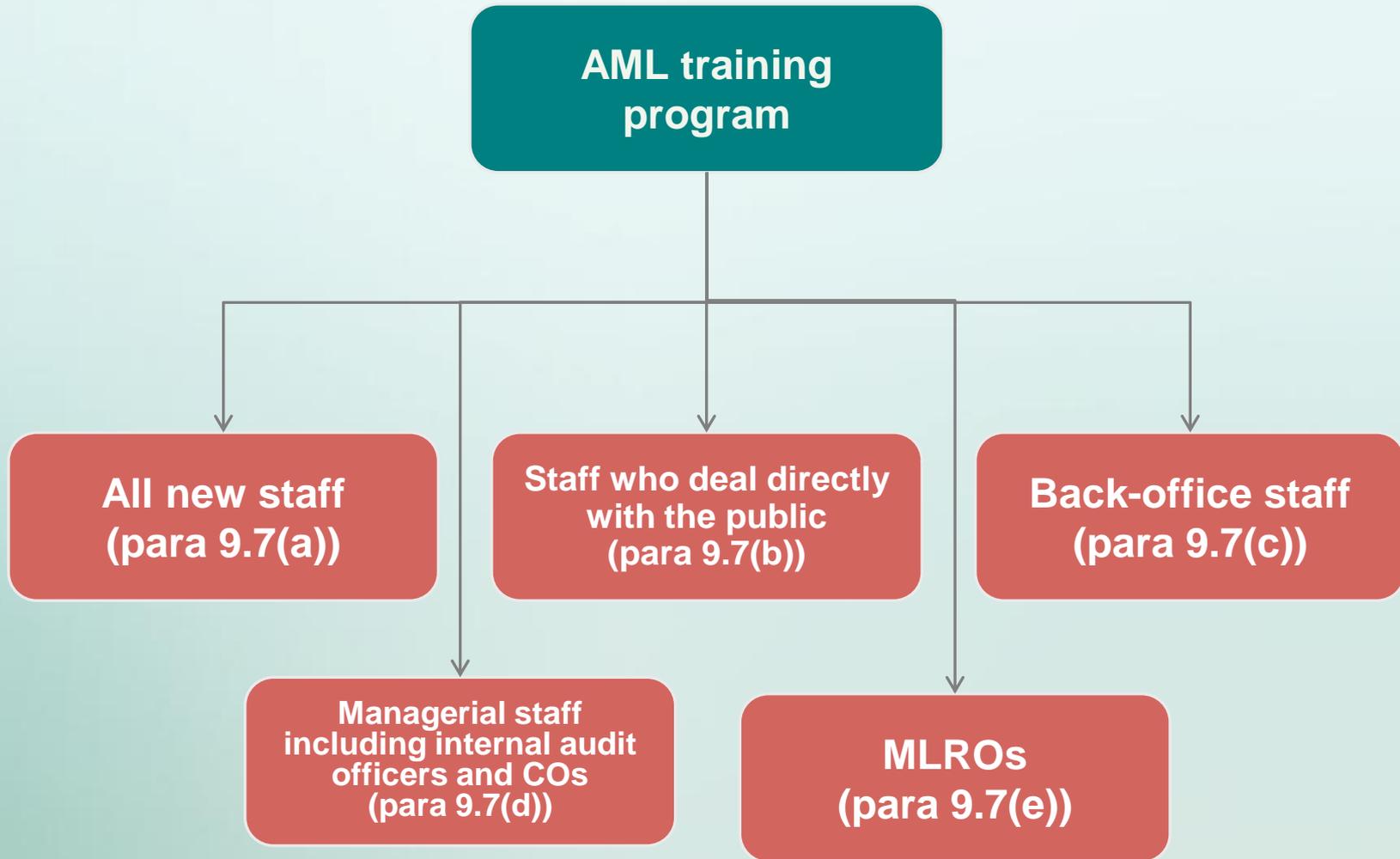
Staff training

- Failure to keep training record

Paragraph 9.9 of the Guideline



AML training areas for different staff groups



C. Monitoring and reporting of suspicious transactions



Suspicious transactions reports

- The obligation to report under the Drug Trafficking (Recovery of Proceeds) Ordinance, the Organized and Serious Crimes Ordinance or the United Nations (Anti-Terrorism Measures) Ordinance rests with the individual who becomes suspicious of a person, transaction or property
- Chapter 7 of the Guideline also outlines the requirements for monitoring and reporting suspicious transactions
- Appropriate measures should be taken to identify suspicious transactions in order to satisfy the legal obligations of reporting funds or property known or suspected to be proceeds of crime or terrorist property to the JFIU

Suspicious transactions reports

Identify suspicious transactions

- The most forgotten element of the CDD process
- Assess whether the transactions conducted are in line with your knowledge of the client's profile
- Put in place proper mechanisms to scrutinise transactions
- Focus should not just be on credit risk



Inadequate suspicious transaction reporting

Number of reports filed with the JFIU

	2007	2008	2009	2010	2011	As at 9/2012
Firms registered with the SFC	220	242	372	662	470	495

Inadequate suspicious transaction reporting

Number of reports filed with the JFIU

- Despite the increase in the number of reports filed, the number of reports from the securities sector is still low compared to the banking sector (2011: 17,194; 2010: 16,551; 2009: 12,602) and the money services provider sector (2011: 1,051; 2010: 1,667; 2009: 2,701)
- The reports were mainly made by a relatively small number of firms

Inadequate suspicious transaction reporting

The relatively low number of reports may be due to the followings:

- Failure to generate exception reports on large or irregular transactions
- Failure to design suitable exception reports by reference to the suspicious transaction indicators and the specific nature of its business
- Failure to perform timely reviews of existing customer records
- Failure to establish clear internal guidelines for assisting staff in identifying and reporting suspicious transactions