



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

Implementation of a Robust AML/CFT Regime

October 2014

Raymond Wong
Director, Intermediaries Supervision, Intermediaries

Disclaimer

Where this presentation refers to certain aspects of the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (AMLO) and the 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. Furthermore, 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.

The SFC is the owner of the copyright and any other rights in the PowerPoint materials of this presentation. These materials may be used for personal viewing purposes or for use within your firm. Such materials may not be reproduced for or distributed to third parties, or used for commercial purposes, without the SFC's prior written consent.



Why is it important?

- As a FATF member, Hong Kong is obliged to implement the AML/CFT requirements as promulgated by FATF standards.
- AML/CFT failures have serious consequences, including reputation risk, for both Hong Kong and LCs.
- Implementing an effective AML/CFT systems (policies, procedures and internal controls) are essential for the LCs to perform the role of gatekeeper.



Commitment to a Robust AML/CFT Regime

Senior management should:

- Develop strong AML/CFT governance and culture
- Understand the ML/TF risks and allocate adequate resources to meet the AML/CFT obligations
- Implement an effective AML/CFT system
- Enhance the awareness and competence building to enable the firm and their staff to meet the AML/CFT obligations



Key Questions

- What is the tone from the top?
- How well does the senior management understand the firm's ML/TF risks?
- How well does the LC implement AML/CFT systems as well as CDD and on-going monitoring measures commensurate with the risks?
- How well does the LC apply the CDD measures, especially on higher risk customers including politically exposed persons?
- To what extent does the LC meet the record-keeping requirements?
- To what extent does the LC meet the reporting obligations to Joint Financial Intelligence Unit?
- How well does the LC enhance awareness and build competence of its staff to ensure compliance with AML/CFT requirements?





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

Implementation and Monitoring of Effective Risk-Based AML/CFT Controls

October 2014

Ronald Mak
Senior Manager, Intermediaries Supervision, Intermediaries

Ivan Wan
Manager, Intermediaries Supervision, Intermediaries

Disclaimer

Where this presentation refers to certain aspects of the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (AMLO) and the 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. Furthermore, 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.

The SFC is the owner of the copyright and any other rights in the PowerPoint materials of this presentation. These materials may be used for personal viewing purposes or for use within your firm. Such materials may not be reproduced for or distributed to third parties, or used for commercial purposes, without the SFC's prior written consent.



Content

- I. Governance & Compliance Culture
- II. CDD on Politically Exposed Persons
- III. Screening, Monitoring and Reporting of Suspicious Transaction
- IV. Awareness and competence building



I. Governance & Compliance Culture



Governance & Compliance Culture

- “Tone from the top” is important.
- Senior management has responsibility to supervise the LC and take ownership in implementing effective AML/CFT systems.
- Senior management needs to adopt a proactive attitude to conduct, culture and behavioural issues.

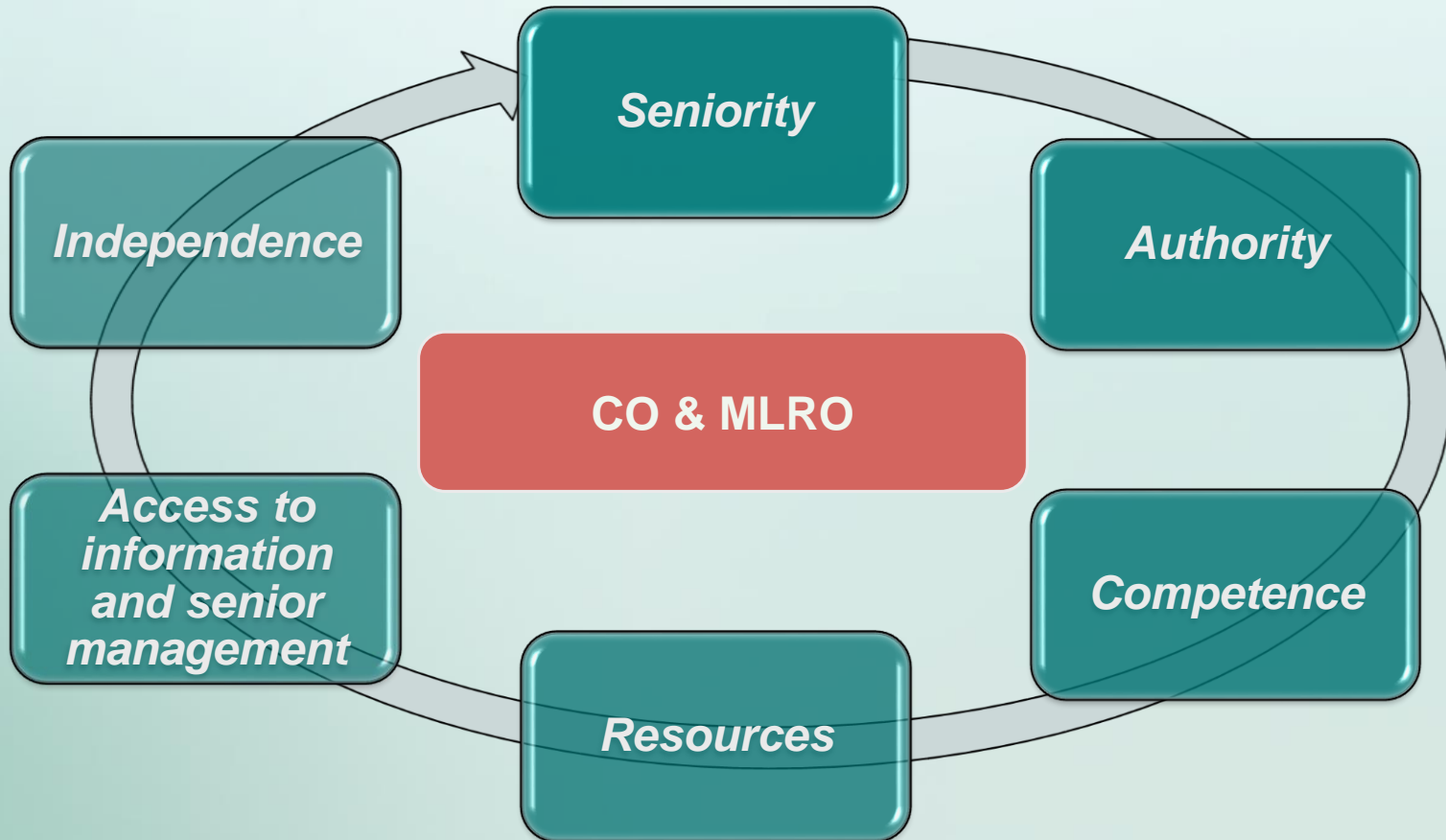


Governance & Compliance Culture

Regulatory Requirement

- Appointment of an independent CO / MLRO

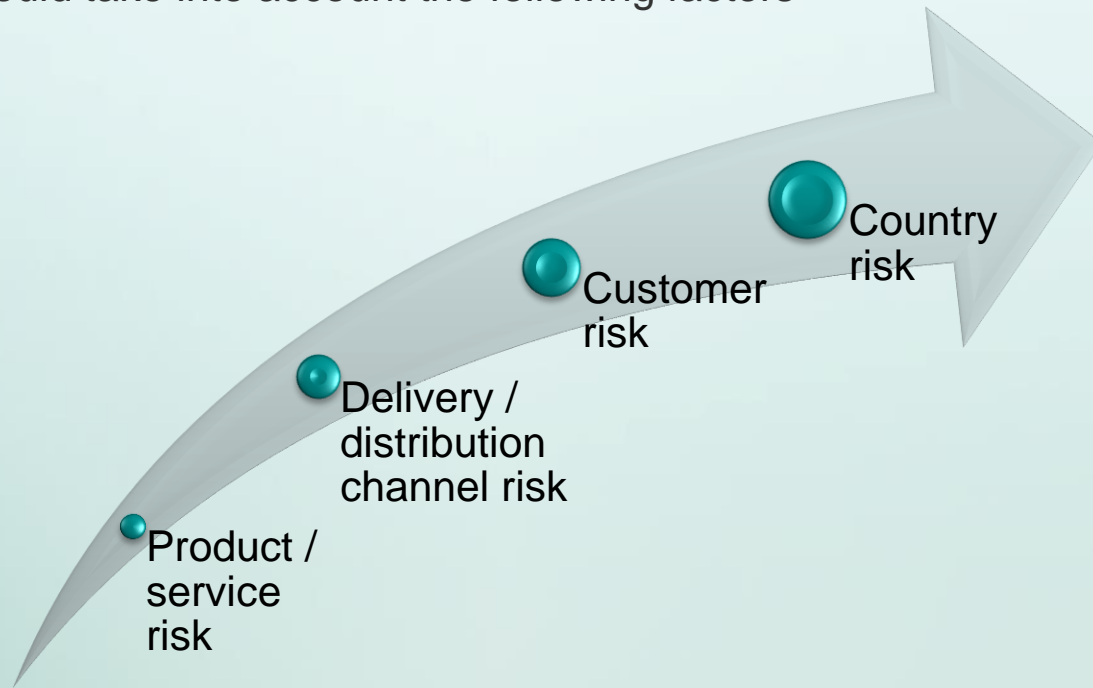
Paragraph 2.12 of the Guideline



ML/TF Risk Assessment

Regulatory Requirement

- FIs should take into account the following factors



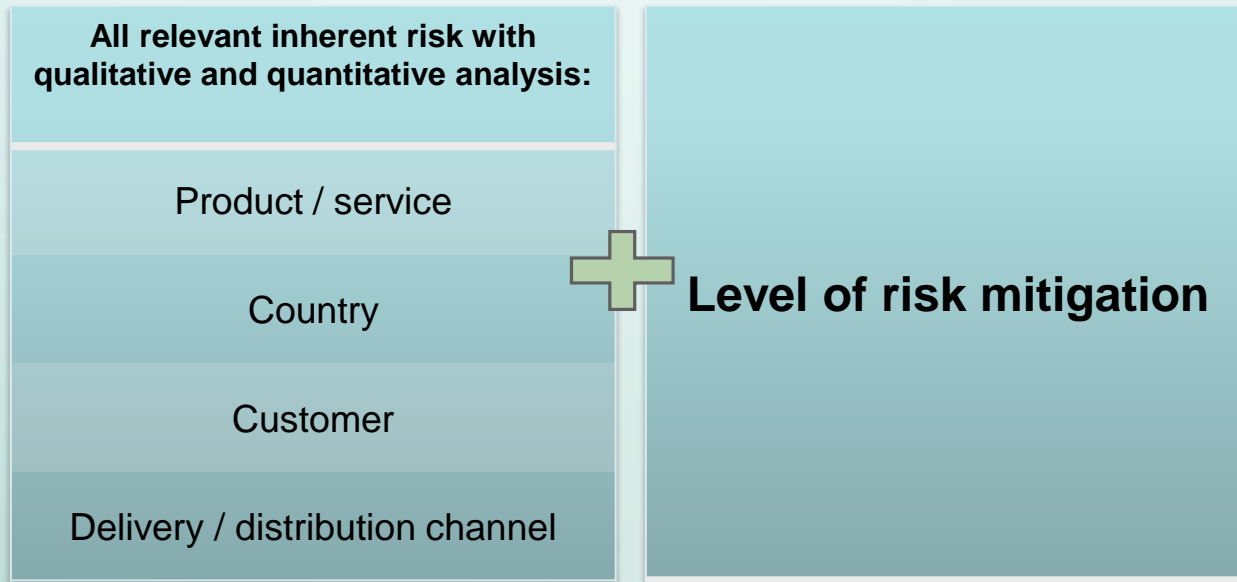
to establish and implement adequate and appropriate AML/CFT policies, procedures and controls.

Paragraph 2.2 of the Guideline



Process to Assess ML/TF risk

- A comprehensive risk assessment should consider:



- The risk assessment may be reviewed from time to time to reflect any changes in ML/TF risks.

Process to Assess ML/TF risk

- While there is not a prescriptive set of factors, LCs may consider the following:
 - diversity and complexity of business
 - target markets
 - type of customers
 - geographic locations / jurisdictions the LC is exposed to
 - distribution channels
 - new products or services
 - internal audit and regulatory findings
 - volume and size of transactions
- Sources of information may include:
 - Internal sources: Operational and transaction data
 - External sources: Mutual Evaluation Reports and follow-up reports by FATF or associated assessment bodies as well as typology reports, other reports issued by inter-governmental international organisations

Documentation of ML/TF Risk Assessment

- To enhance the effectiveness of communication and sharing with all business lines across the LC:
 - board of directors
 - management
 - appropriate staff
- the risk assessment should be appropriately documented.



II. CDD on Politically Exposed Persons (PEPs)

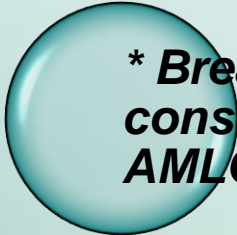


Identification of PEPs

Regulatory Requirement

- A financial institution must establish and maintain effective procedures for determining whether a customer or a beneficial owner of a customer is a politically exposed person.

Paragraph 4.13.9 of the Guideline, s.19(1), Sch. 2 of the AMLO*



**** Breach of s.19(1), Sch. 2 of the AMLO may constitute a criminal offence according to s.5 of the AMLO***

Identification of PEPs

Different sources of information:

Internet search engines	Utility:	Limitation:
Commercial databases	<ul style="list-style-type: none"> Use of internet search engines or free search tools through AML-specific websites to search for customers' information such as occupation or employment and the information of their family members Useful in retrieving general relevant information, e.g. which countries prohibit certain PEPs from maintaining bank accounts abroad 	<ul style="list-style-type: none"> Information may not be comprehensive and reliable May generate large number of 'hits' that are not related to customer in question or are not useful information for determining whether the customer is a PEP
Asset disclosure registers		
In-house databases		
Customer self-declarations		



Identification of PEPs

Different sources of information:

Free search engines	Utility: <ul style="list-style-type: none">Match the name and identity information of the customers against name list contained in the subscribed database	Limitation: <ul style="list-style-type: none">Different definition of PEPs may be adopted
Commercial databases		
Asset disclosure registers		
In-house databases		
Customer self-declarations		



Identification of PEPs

Different sources of information:

Free search engines	Utility: <ul style="list-style-type: none"> The names of filers and/or list of positions can help to determine if a client is a PEP Provide insight into the public functions that a country deems to be prominent 	Limitation: <ul style="list-style-type: none"> May not be available in some countries Criteria used may not correspond with the definition of a PEP.
Commercial databases		
Asset disclosure registers		
In-house databases		
Customer self-declarations		



Identification of PEPs

Different sources of information:

Free search engines	Utility: <ul style="list-style-type: none">• Match the name and identity information of the customers against name list contained in the in-house database	Limitation: <ul style="list-style-type: none">• Information may not be comprehensive
Commercial databases		
Asset disclosure registers		
In-house databases		
Customer self-declarations		



Identification of PEPs

Different sources of information:

Free search engines	Utility: <ul style="list-style-type: none">• A direct means of helping to determine whether that customer is a PEP• Obtaining information relating to present or former occupation or employment	Limitation: <ul style="list-style-type: none">• Customer may not know or understand the definition of PEP correctly• Self-declaration may be false
Commercial databases		
Asset disclosure registers		
In-house databases		
Customer self-declarations		

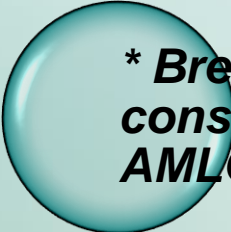


EDD Measures on PEPs

Regulatory Requirements

- When FIs know that a particular customer or beneficial owner is a PEP, it should apply EDD measures:
 - a) obtaining approval from its senior management;
 - b) taking reasonable measures to establish the customer's or the beneficial owner's source of wealth and the source of the funds; and
 - c) applying enhanced monitoring to the relationship in accordance with the assessed risks.

Paragraph 4.13.11 of the Guideline, s.5(3)(b) & s.10, Sch. 2 of the AMLO*



**** Breach of s.5(3)(b) & s.10, Sch. 2 of the AMLO may constitute a criminal offence according to s.5 of the AMLO***

EDD Measures on PEPs

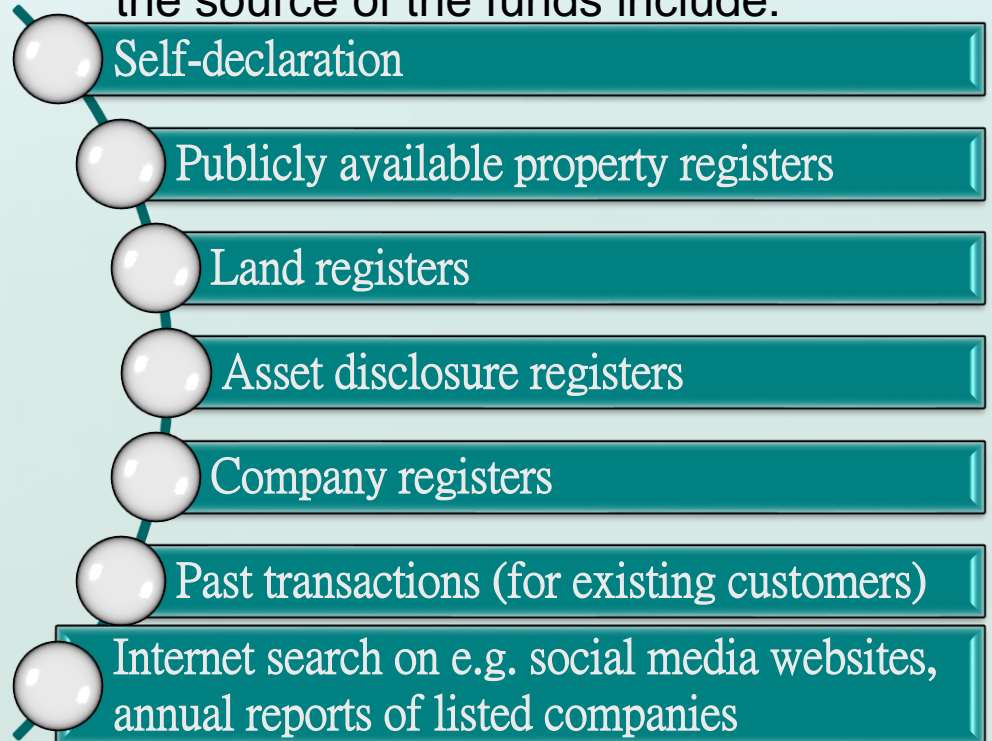
- (a) obtaining approval from its senior management;
 - (b) establishing source of wealth and the source of the funds; and
 - (c) applying enhanced monitoring in accordance with the assessed risks.
- To strengthen the effectiveness of the management oversight, senior management should, among others, have:



EDD Measures on PEPs

- (a) obtaining approval from its senior management;
 - (b) establishing source of wealth and the source of the funds; and
 - (c) applying enhanced monitoring in accordance with the assessed risks.
- Aim is to ensure that the level and type of transactions are commensurate with LCs' reasonable expectation

- Non-exhaustive examples of information sources to establish source of wealth and the source of the funds include:



EDD Measures on PEPs

- (a) obtaining approval from its senior management;
 - (b) establishing source of wealth and the source of the funds; and
 - (c) applying enhanced monitoring in accordance with the assessed risks.
- To develop appropriate red flags / indicators to identify potentially suspicious transactions. Non-exhaustive examples include:



Information provided is inconsistent with other publicly available information

Unable or reluctant to provide explanations for conducting transactions

Funds are repeatedly moved to and from countries to which the PEPs do not seem to have ties with

III. Screening, Monitoring and Reporting of Suspicious Transaction

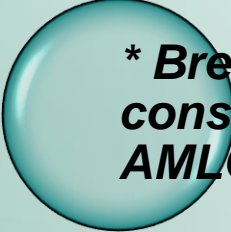


Screening and Monitoring of Suspicious Transaction

Regulatory Requirements

- An FI must continuously monitor its business relationship with a customer by:
 - monitoring the activities of the customer to ensure that they are consistent with the nature of business, the risk profile and source of funds; and
 - identifying transactions that are complex, large or unusual or patterns of transactions that have no apparent economic or lawful purpose and which may indicate ML/TF.
- Where the exceptions are noted, FIs should examine the background and purpose of the transactions. The findings and outcomes of these examinations should be properly documented in writing.

Paragraph 5.1 (b), (c) & 5.10 of the Guideline, s.5(1)(b), (c), Sch. 2 of the AMLO*



**** Breach of s.5(1)(b), (c), Sch. 2 of the AMLO may constitute a criminal offence according to s.5 of the AMLO***

Transaction Monitoring System

- Senior management should have oversight on the implementation of the system.
- MLRO should play an active role in identification and reporting of suspicious transactions, e.g. regular review of exception reports.
- Relevant staff should be aware of the operation of the transaction monitoring system and the rationale for setting certain parameters/thresholds.
- Relationships are monitored in a holistic manner, rather than on account/transaction basis, e.g. taking into account transactions conducted by all related accounts or trading pattern over a period of time.
- The parameters/thresholds in use are appropriate and justified for the nature and activities of its customers.
- LCs should take into account, among others, the size, nature and complexity (by referencing to para 5.9 of Guideline) to determine how best to monitor the transactions and activities



Handling Alerts

- Take into account relevant CDD information and transaction details (e.g. customer background, source of funds, transaction pattern) and other supporting documents (e.g. cheque copy) to determine whether transactions are suspicious
- Ensure that alerts are reviewed in a timely manner
 - Provide clear timeframes for an internal report to be completed or escalated
 - Monitor time taken to review alert
- Sufficient documentation to evidence the analysis and determination of whether the transaction highlighted in alert is suspicious or not
- Implement a clear reporting procedure to guide handling staff to make internal disclosures (e.g. how and whom he should report)

Suspicious Transaction Indicators

- To recognize suspicious activities effectively, LC should:
 - take into account of its own circumstances, among others, the nature of the transactions and instructions that staff is likely to encounter and the type of product or service
 - make reference to para 7.14, 7.39 & 7.40 of Guideline and other relevant guidance, e.g. FATF's Guidance for Financial Institutions in Detecting Terrorist Financing

in tailoring the appropriate suspicious transaction indicators.

Suspicious Transaction Indicators

- Some examples of situations that might give rise to suspicion noted in SFC's supervisory work:

Perform frequent fund transfer activities with unrelated third parties

Purchase and sell shares of these companies with no apparent reason, e.g. purchased securities at a high price and subsequently sells them at a considerable loss

Customer financial background, e.g. salary income, residential address, etc., not commensurate with large trading volume

- Example of situation that might give rise to suspicion regarding tax evasion:


Deliberate attempt to withhold information about dual citizenships



Reporting Suspicious Transaction

DTROP, OSCO and UNATMO make it

an offence, if a person



deals with any property knowing or having reasonable grounds to believe it to represent any person's proceeds of drug trafficking or of an indictable offence respectively; or

provides or collects property and makes any property or financial (or related) services available to terrorists or terrorist associates; or

fails to disclose his knowledge or suspicion of any property that represents the proceeds of drug trafficking or of an indictable offence or of terrorist property respectively.

- **Filing a report to the JFIU provides LCs with a statutory defence to the offence of ML/TF in respect of the acts disclosed in the report**

Reporting Suspicious Transaction

- Provide sufficient information relating to customers' background and transaction details, including:
 - Customer identity information
 - Occupation or employment
 - Summary of known financial situation
 - Amount, date and types of transactions
- Provide rationale for the suspicion identified
- Indication of termination of business
- Information provided should be well-structured and clear
- File the suspicious transaction reports as soon as reasonable to do it



IV. Awareness and Competence Building



Awareness and Competence Building

- Staff should be trained in what they need to know in order to carry out their particular role with respect to AML/CFT.
- Topics should, among others, cover:
 - How LC's products and services may be used for ML/TF
 - Relevant regulatory requirements
 - LC's policies and procedures for mitigating the risk (including circumstances that may give rise to suspicion)
- Testing staff's understanding of the firm's policies and procedures by providing quiz subsequent to the training provided to ensure the effectiveness of the training.



Awareness and Competence Building

- Training should be tailored to the particular function of the staff. Non-exhaustive examples include:
 - Front-office staff
 - the importance of their role in the LC's ML/TF strategy, as the first point of contact with potential money launderers
 - the LC's policies and procedures in relation to relevant requirements with respect to their job responsibilities
 - circumstances that may give rise to suspicion, e.g. where a customer frequently purchases securities at a high price and subsequently sells them at a considerable loss
 - Bank-office staff
 - appropriate training on customer verification and relevant processing procedures
 - recognition of unusual activities, e.g. frequent funds or other property transfers or cheque payments to or from third parties that are unrelated, unverified or difficult to verify, etc.



Awareness and Competence Building

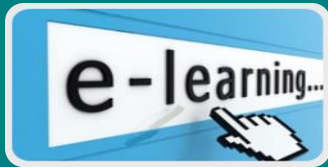
- Non-exhaustive examples of training modes include:



Classroom training



Regular meetings / briefing sessions



On-line learning systems



Relevant videos

Thank You

