

Key Aspects of an AML/CTF system

Dickson Chui
Manager (Enforcement) –
Anti-Money Laundering
14 September 2012



Office of the Commissioner of Insurance
The Government of the Hong Kong Special Administrative Region

Disclaimer

- *This part of presentation aims to raise the audience's awareness of key aspects of AML/CTF systems and controls. It does not cover all the statutory requirements applicable to insurance institutions. Insurance institution should seek its own professional legal advice in ensuring its compliance with the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance and Guideline on Anti-Money Laundering and Counter-Terrorist Financing.*
- *The PowerPoint materials of this presentation may be used for personal viewing purposes or for use within an insurance institution. These materials may not be reproduced for or distributed to third parties, or used for commercial purposes without the OCl's prior written consent.*



Chapter 1 – Overview

1.4: Purposes –

- a. General background on ML/TF and the applicable legislation
- b. Guidance in designing and implementing AML/CTF systems so as to meet statutory & regulatory requirements



Chapter 1 – Overview



1.6 – 1.7:

- **Not exhaustive** list of means
- But if departure from the Guideline, FIs will have to stand **prepared to justify** such to IA with documented rationale



Chapter 2 – AML/CFT systems

2.2: **establish & implement** AML/CFT systems,
taking into account risk factors (2.3-2.8)

2.1 & 2.9:

AML/CFT systems = internal P&P + Controls*

- * senior management oversight
- * appointing CO & MLRO
- * compliance & audit function
- * staff screening & training



Observation

- Some requirements under AMLO/Guideline are not incorporated in the AML/CTF policies and procedures without justification
- Reliance on insurer's AML/CTF policy

(Ref: Guideline paragraph 1.7)



Chapter 3 – Risk-Based Approach

RBA: **identify & categorize** ML/TF risks
and apply **corresponding measures**

3.2: - **determine** extent of CDD measures &
ongoing monitoring, using RBA
- measures **must** comply with the AMLO
requirements

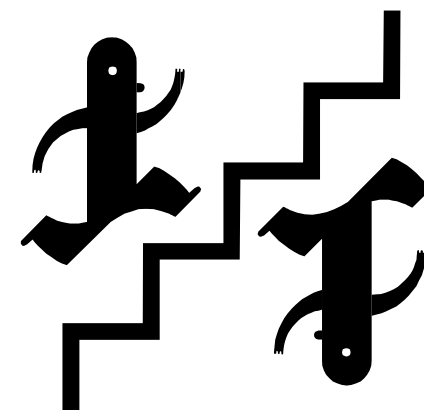


Chapter 3 – Risk rating on customer

3.4, 3.6: assess ML/TF risks of customers by assigning a **risk rating** to the customers; **adjust** risk assessment from time to time

3.5: consider risk factors:

- country
- customer
- product/service
- delivery/distribution channel



3.8: record keeping and **justification**



Observation

- Risk assessment methodology not laid down
- No documentary evidence that risk assessments were conducted on customers and that ratings were assigned.

(Ref: Guideline paragraph 3.4 & 3.8)



Chapter 4 – CDD measures

4.1.3: CDD measures

- a. customer
- b. beneficial owner (BO)
- c. purpose & intended nature of the business relationship (unless obvious)
- d. person purports to act on behalf of the customer
- e. beneficiary (4.4a.1)



Chapter 4 – Timing of identification & verification of identity

4.7.3: Complete CDD before establishing any business relationship, except:

- 4.7.4 & 4.7.5a – conditions *including* ML/TF risks are effectively managed etc.
- 4.7.8 – **complete verification** within the specified timeframe
 - » 30 working days
 - » 90 working days
 - » 120 working days



Chapter 4 – Keeping customer information up-to-date & relevant

4.7.12, 4.7.12a:

- on *triggering events*
- **Annual review** for all high risk customers



Chapter 4 – Simplified Customer Due Diligence (SDD)

4.10.1 SDD=**CDD** except not required to identify & verify BO; **but** ongoing monitoring is **still required**.

Applicable to specific customers (4.10.3) & specific products (4.10.15)

4.10.2: **No SDD when –**

- suspicion of ML/TF
- doubts the veracity & adequacy of information previously obtained



Chapter 4 – Enhanced Due Diligence (EDD)

4.11.1: Any **high** ML/TF risk situation, apply EDD –

- Additional customer info; regular profile updates
- Additional info on the intended nature of the business relationship, source of wealth and funds
- Senior management's approval
- Enhanced monitoring



Observation

- Missing copies of customers' identification documents
- Identity cards' images were not legible
- Utility bills used as address proof were issued beyond 3 months
- Address shown on address proof is not the same as the one stated in the application form

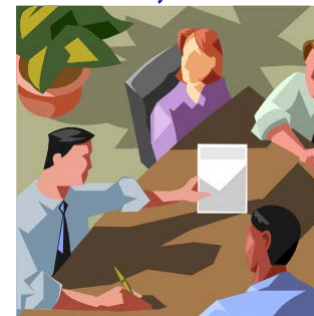
(Ref: Guideline paragraph 4.1.3 & 4.8.10)



Chapter 5 – Ongoing Monitoring

5.1: Continuously monitor business relationship with a customer by:

- Review from time to time CDD documents, data and information to ensure **up-to-date** and **relevant**
- **Scrutinize transactions** with customers to ensure they are consistent with the customer's risk profile
- **Identify transactions** that are complex, unusually large in amount or of an unusual pattern, or have no economic or lawful purpose



Chapter 6 – Screening



Prohibitions - UNSO(6.3), UNATMO(6.13,6.14),
WMDO(6.17)

6.4, 6.16: IA's circulars to FIs on designated persons
& entities

6.18: required "Screening" against up-to-date list

6.21: accessibility by staff

6.22: when to perform screening

6.25: screening results documented & recorded

6.26: file STR



Observation

- No evidence that PEP / terrorist checking (such as making reference to publicly available information and screening against current terrorist and sanctions designations) was performed against the customers.
- Use of third party vendor to conduct comprehensive screening

(Ref: Guideline paragraph 4.13.9, 6.20 & 6.22)



Chapter 7 – STR

7.7: Sufficient guidance for staff (including agents); ref annexes I & II for e.g. of suspicious transactions

7.19: MLRO; its roles (7.19-7.30, 7.33, 7.36)

- Central reference point for reporting suspicious transactions
- Sufficient status & adequate resources
- Active role
- Take reasonable steps to consider all relevant information

7.25, 7.31, 7.32: reports made to MLRO and JFIU must be documented



Office of the Commissioner of Insurance
The Government of the Hong Kong Special Administrative Region

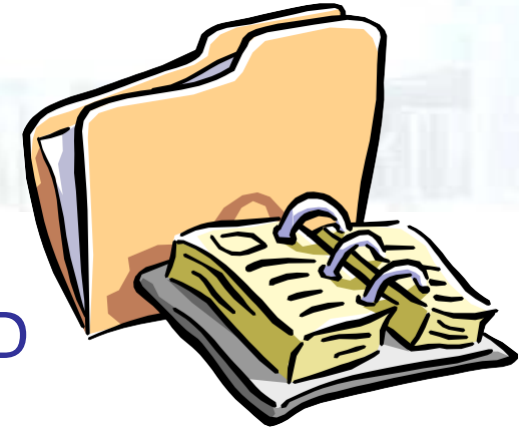
Observation

- Not all staff including agents are made aware of the identity of the MLRO

(Guideline paragraph 7.23)



Chapter 8 – Record Keeping



Documents/information obtained during CDD

- 8.3a: **Original/copy of the documents**, and a record of data and information, obtained in the course of identifying and verifying the identity of customer/beneficial owner/beneficiary/persons who purport to act on behalf of the customer/connected parties
- 8.3b: For the purposes of EDD or ongoing monitoring
- 8.3c: On the purpose and intended nature of the business relationship
- 8.3d: In relation to the **customer's account** and **business correspondence** (e.g. insurance application form, risk assessment form)



Chapter 8 – Record Keeping

8.5: Transaction records which should be sufficient to

- **permit reconstruction** of individual transactions
- **establish a financial profile** of any suspect account or customer



Observation

- Misconceptions by insurance agencies and brokers that copies of identification documents were not required to be kept if they had already been sent to the insurer

(Ref: Guideline paragraph 8.3 & 8.4)



Chapter 9 – Staff training

9.7: training packages tailored to different groups of staff
(including agents)

9.9: training records

9.10: monitoring the training effectiveness



Observation

- Inadequate training to staff to maintain their AML/CFT knowledge and competence
- Training records showing who have been trained, when the staff received training and the type of the training provided were not kept

(Ref: Guideline paragraph 9.3 & 9.9)



Observation

- Some outdated and incorrect information was noted in the training materials.

(Ref: Guideline paragraph 9.2)

- Customized training for different groups of staff

(Ref: Guideline paragraph 9.7)





Thank You



For further enquiries,
please send to iamail@oci.gov.hk



Office of the Commissioner of Insurance
The Government of the Hong Kong Special Administrative Region