Implementation of an effective AML/CFT system

Dickson Chui

Manager (Enforcement) –

Anti-Money Laundering

17 October 2013

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 how to implement an effective AML/CFT system. 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 OCI'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/CFT 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

Chapter 3 – Risk-Based Approach

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**

Chapter 3 – Risk-Based Approach

DON'Ts

- No risk assessment conducted on customers with ratings assigned (3.4)

- Risk assessments conducted, but not recorded and documented (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

4.7.1: 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 trigger events*
- **annual review** for all high risk customers
- what constitutes a trigger event should be **clearly defined in FI's policies and procedures**

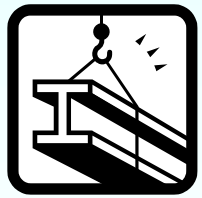
Chapter 4 – Legal Persons & Trusts

4.9.4: for a customer other than a natural person, FI should fully **understand its legal form, structure and ownership**

4.9.9: **record the name of directors** and verify the identity of directors on a risk-based approach

Chapter 4 – High risk situations

4.11.1: FI must, in any situation that by its nature presents a **higher risk of ML/TF**, take **additional measures** to mitigate the risk of ML/TF



4.13.9: effective procedures for determining whether a customer/BO of a customer is a PEP

Chapter 4 – Customer Due Diligence

DOs

- Keep clear copies of customer identification documents (4.1.3)
- Clear list of trigger events upon which CDD information should be reviewed (4.7.12)

DON'Ts

- Continue business relationship notwithstanding requisite CDD measures remained incomplete (4.7.1 & 4.7.8)
- Not trying to understand the legal form, structure and ownership of corporate customers (4.9.4)

Chapter 4 – Customer due diligence

DON'Ts

- Not record the names of all directors (4.9.9)
- Information not obtained/action not carried out as required under Company's AML/CFT policy, e.g. EDD for high risk customers (4.11.1)
- Threshold applied on PEP screening (4.13.9)
- Accuracy of database of screening programme was questionable (4.13.9)
- Loose standard in accepting supporting documents of income proof / occupation proof

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, large or unusual or patterns of transactions with no apparent economic or lawful purpose

Chapter 5 – Ongoing monitoring

5.10: Examination of transactions that are complex, large or unusual, or patterns of transactions which have no apparent economic or lawful purpose

- Findings / outcomes properly documented in writing
- Proper records of decision made, by whom, and rationale

Chapter 5 – Ongoing monitoring

DOs

- Detailed analysis on the inclusion of recommended suspicious indicators to the existing exception reporting system (5.1 & 7.14)

- Proper record of the staff who review exception reports (5.10)

Chapter 5 – Ongoing monitoring

DON'Ts

- Inadequate control on change of policy ownership, e.g. not ascertain the reason, no ongoing monitoring in place to identify unusual transactions (5.1)
- Non-specific record of nationality of customers in the customer database (5.1)

Chapter 6 – Screening

6.22: when to perform screening of customers

6.23: ensure proposed payments to designated parties are not made

6.25: screening results documented & recorded

Chapter 6 – Screening

DOs

- Proper documentation of the screening result evidencing the performance (6.25)

DON'Ts

- Screening conducted after insurance policy was issued (6.22)
- Screening not conducted on beneficiaries at time of payout (6.23)

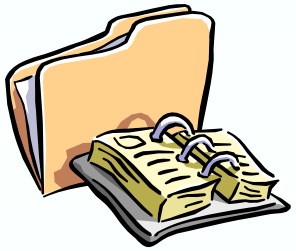
Chapter 7 – STR

7.16: disclosure to JFIU as soon as it is reasonable to do so

7.19: MLRO's roles (7.19-7.30, 7.33, 7.36)

- Central reference point for reporting suspicious transactions
- Sufficient status & adequate resources
- Active role; regular review of exception reports
- Keep proper records of deliberations and actions taken

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



Chapter 7 – STR

DOs

- Provide a reminder of the obligation regarding tipping off (7.26)
- Proper records of deliberation with supporting documents to substantiate the decision to / not to file an STR with JFIU (7.30)
- Respective departments keep their own logs of internal disclosure for proper audit trail (7.31)

Chapter 7 – STR

DON'Ts

- Unnecessary delay in reporting suspicious transactions (7.16)
- MLRO's duty of review of exception reports delegated to operations departments (7.21)
- Loose control on payment by third party, in particular where cash was involved

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

Chapter 9 – Staff training

9.3: clear and well articulated training policy

9.6: training coverage

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

9.9: training records

9.10: monitoring training effectiveness

Chapter 9 – Staff training

DOs

- Customerized training packages to staff of different departments (9.7)

DON'Ts

- Inadequate training to staff to maintain their AML/CFT knowledge and competence (9.3)
- Inadequate coverage of training materials (9.6)
- Assessment used was not comprehensive / ineffective to test understanding (9.10)

Thank You

For further enquiries,

please send to iamail@oci.gov.hk