Recent Regulatory Developments on AML/CFT

AML Seminars, Hong Kong Central Library

11th & 19th September 2014

Stewart McGlynn
Anti-Money Laundering and Financial Crime Risk Division
Banking Supervision Department
Hong Kong Monetary Authority

HONG KONG MONETARY AUTHORITY
香港金融管理局

Financial Services and the Treasury Bureau
The Government of the Hong Kong Special Administrative Region

Disclaimer

- This presentation provides guidance to authorized institutions ("AIs") on issues relating to the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance ("AMLO") and the AMLO Guideline. The presentation is provided for training purposes and does not form part of the formal legal and regulatory requirements of the HKMA. It should not be substituted for seeking detailed advice on any specific case from an AI's own professional adviser.

-

Challenges

HSBC to pay $1.9 billion U.S. fine in money-laundering case

BY ARUNA VISWANATHA AND BRETT WOLF
Tue Dec 11, 2012 6:15pm EST

HSBC 滙豐

(Source: REUTERS)

Standard Chartered fined $327 million for violating sanctions

By Chris Isidore @CNNMoneyInvest December 10, 2012: 1:17 PM ET

Recommend 40

Immediate Outcome 3, Para. 3.5 (FATF Methodology)

- **To what extent are supervisors able to demonstrate that their actions have an effect on compliance by FIs and DNFBPs.**

(Source: CNN)

payment by sending money overseas. The global banking giant will pay a total of $2.6 billion in penalties

The Swiss bank Credit Suisse pleaded guilty Monday to helping U.S. citizens commit tax evasion over the course of several

Fabrice Coffrini—AFP/Getty Images

(Source: TIME)

3年洗黑錢68億元 六旬公屋婦判囚十年

2013年03月13日

(Source: AM730)

Our Findings

- Governance and Oversight of ML/TF risk remain a key focus in our supervision
  - Historical perspective – Many reviews are ‘look backs’
  - Assurance activity should be performed by compliance function over the CDD or sanctions process – to detect control failures
  - Poor judgment or questionable decisions will be challenged
- Key post holders, MLRO etc., must be effective
  - Should help the AI to understand risk, dealing with that risk and recognizing where the AI needs to be better
- System or Program flaws, or risk events must be properly addressed by all AIs
  - Documented form, to the right level of Authority

Our Findings

- Risk assessment processes to identify higher risk customers
  - Important area for AIs – must be robust
  - Event driven reviews should be adequate
- Risk-based approach to CDD
  - AIs should be sure when EDD should be applied and what are the drivers
- Management of high risk customers
  - Source of wealth and funds – processes must be adequate

Our Findings

- Resource adequacy often drives effectiveness of implementation
  - Known weaknesses should be clearly articulated
- Correspondent Banks
  - Adequate Due Diligence vital
- AML/CFT IT systems
  - Some AIs need to consider automation
  - Calibration, validation and checking also important
- Effective alert clearance
  - Delays should be closely monitored, resource planning
  - Sufficient guidance to staff, audit trail etc.

Transaction Monitoring

Guidance Paper

3.6	AIs should take into account the size, nature and complexity of its business in an appropriate assessment, prior to the launch of the transaction monitoring system. To ensure adequate coverage of its business operations, the assessment should take into consideration the question of whether to implement, and if so the appropriate degree of, automation that is required for the transaction monitoring system. This assessment should be in writing as a record of the rationale for adopting the system, including how it meets the AI's needs and other material factors such as the appropriateness of the system vendor, the effectiveness of the interface between the new system and the AI's existing infrastructure, how updates will be undertaken and any resource implications.

National Risk Assessment ('NRA')

ML/TF Risk Assessment

- Cornerstone to Risk-Based Approach
- Applies to every level in the AML/CFT Regime
  - Jurisdictional level (NRA will commence soon)
  - Sectoral level
    - NRA includes risk assessment of banking sector
      - Gatekeeper Role
    - Private Sector Engagement Critical
      - AIs have to contribute in the process
  - Financial institution level
    - AIs must understand their own ML/TF risks
- Effective allocation of resources to manage and mitigate areas posed higher ML/TF risks

ML/TF Risk Assessment

- Banking encompasses a wide range of financial products and services, which are associated with different ML/TF risk
- Risk assessment enables the bank to understand how, and to what extent, it is vulnerable to ML/TF
- Often result in a stylized categorization of risk, which will help banks determine the level of AML/CFT resources necessary to mitigate that risk
- Overarching principle - no one-size-fit-all
  - not necessarily complex
  - should be commensurate with the nature and size of the bank's business

Recap of existing obligation

AMLO Guideline

2.1	AI must take all reasonable measures
2.2	Take into account risk factors
2.3	Product / Service risk
2.4	Delivery / Distribution channel risk
2.5-7	Customer risk
2.8	Country risk
3.3	An effective RBA does involve identifying and categorizing ML/TF risks at the customer level and establishing reasonable measures based on the risk identified

ML/TF Risk Assessment
- follow-up to last seminar

- AIs must recognize ML/TF risk assessment as their core part of risk management process
  - already developed or put in place action plans to develop ML/TF risk assessment
- Enhancement in terms of comprehensiveness required but some AIs are in a right direction in developing the framework
  - e.g. risk tolerance level, quantitative data analysis to support the risk assessment
- Variations in format along with the scale and complexity of business

ML/TF Risk Assessment
- follow-up to last seminar

- Policies and control procedures / risk monitoring reports / MIS *are not* risk assessments.
  - only reflect how a bank manages and controls its inherent ML/TF risks identified through its risk assessment.
- Comprehensive risk assessment should include:
  - identification and assessment of inherent risk which should be supported by quantitative and quantitative analysis
  - level of risk mitigation. The resulting risk profile reflects the bank's risk appetite.
- Risk assessment is a dynamic process and should be regularly updated

ML/TF Risk Assessment

- A bank should develop a thorough understanding of the inherent ML/FT risks present in its customer base, products, delivery channels and services offered and the jurisdictions within which it or its customers do business
- The Risk Assessment should be:
  - Properly documented, maintained and communicated to relevant personnel within the bank
  - Ready to provide it to the supervisor
  - Approved by senior management
  - Reviewed and updated on a regular basis
- It forms the basis for development of policies and procedures to mitigate ML/TF risk, reflecting the risk appetite of the bank and stating risk level deemed acceptable

ML/TF Risk Assessment

- Objective is to assess the AI's ML/TF risk profile and evaluate the adequacy of the its ML/TF risk assessment process
- We will obtain and review the AI's ML/TF risk assessment as part of the examination scoping exercise:
  - Is the process for periodically reviewing and updating the ML/TF risk assessment adequate?
  - Is the risk assessment in written form?
  - Has the risk assessment been shared and communicated with all business lines across the bank, board of directors, management, and appropriate staff? Do those staff understand the risk assessment?
- ML/TF risk profile will be discussed in the kick off meeting

ML/TF Risk Assessment

- Some factors we will consider:
  - nature, scale, diversity and complexity of business
  - target markets
  - number of customers already identified as high risk
  - geographic locations / jurisdictions the bank is exposed to
  - distribution channels
  - new products or services
  - volume and size of its transactions
- Complement this information with information obtained from relevant internal and external sources, e.g.
  - Internal sources: specific operational and transaction data
  - External sources: NRA, Mutual Evaluation Reports prepared by FATF or other FSRBs, other reports issued by inter-governmental international organisations

PEPs

- Challenges in identification and management remain
  - CDD is the key source of information for the purpose of identifying whether a customer is a PEP
  - Databases may assist but they are not mandatory and they may present misleading information – they are only part of the equation
- Ensure proper communication with customers / prospective customers
  - Bank must pay attention to QA issues in this area

Thank You