Feedback from recent AML/CFT examinations

AML Seminars, Hong Kong Central Library

3rd & 5th November 2015

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.

- The HKMA 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 an AI. Such materials may not be reproduced for or distributed to third parties, or used for commercial purposes, without the HKMA's prior written consent.

- The cases or examples provided in this presentation might be prepared on the basis of synthesis of multiple cases, and certain relevant details might have been omitted.

Governance

- Governance framework should be appropriate to nature, scale & complexity of AI
  - Variation expected, especially at smaller AIs
- Some AIs operate dedicated AML or FCC committees, others as part of more general risk committees
  - Examples of good and bad governance in both models
  - Formal structures, established terms of reference generally work better
- AIs’ responsibility to demonstrate effectiveness

Governance

Example

Bank A had a formal AML committee with terms of reference but:

- *Routine statistical information was being presented*
- *Some high risk / high impact issues, such as shortcomings in the screening tool had not been escalated*
- *Decisions taken by committee were not fully informed, either on basis of risk or materiality*
- *No institutional risk assessment. A good risk assessment would have helped to highlight the high risk / high impact issues (e.g. sanctions risk) and action on the screening tool should have been prioritised*

AI met technical requirement but implementation was not effective

Governance

Example

Bank B managed AML risk through a general risk committee [based on scale of operations] informed by an adequate risk assessment:

- *Key discussions were well documented*
  - *key decisions were consistently recorded, even those resulting from informal or telephone conversations*
- *Clear evidence that reporting was not routine, minutes indicated challenge and actions were followed up*
- *Interviews with committee members confirmed a good understanding of ML/TF risks at institution and customer level*
- *Because of some risk exposure, sanctions risk was closely monitored and results of screening / monitoring regularly reported*
- *No regulatory expectation for small AIs to have disproportionately more expensive or complex controls than larger AIs*

Institutional Risk Assessment

Example

Bank A is a small AI and provided a comparatively simplistic risk assessment which met technical requirement and was effective:

- *The report was well constructed with qualitative analysis*
- *Sufficiently wide range of information was considered, some statistical analysis in two higher risk areas*
- *Multiple key staff had provided input, including business who, when interviewed, displayed good understanding of the risks and the process of assessment*
- *Good records of internal discussions behind the analysis were kept – evidence process was robust*
- *The report had identified some shortcomings in data collection and action was implemented to update an IT system so that subsequent reports would be enhanced*

Institutional Risk Assessment

Example

Bank B provided a risk assessment:

- *Which was a description of the AI’s AML/CFT controls*
- *MLROs must be able to adequately describe what the AIs’ ML/TF risks are and understand the objective of a risk assessment*
- *Must be an understanding throughout the AI on the importance and use of risk information to target resources and review subsequent effectiveness of implementation*
- *Competency of relevant staff and accountability will always be supervisory considerations*

Institutional Risk Assessment

Example

Bank C provided a risk assessment:

- *Which relied solely on individual customer risk assessments*
- *Bank C needed to enhance knowledge of the risks around its products and services*
- *Consideration of emerging risks is also an important consideration*
- *Para. 2.3 of AMLO Guideline specifically requires new products and services to be risk assessed before they are introduced*
- *Bank must be able to demonstrate measures and controls were appropriate*

Customer Risk Assessment

Example

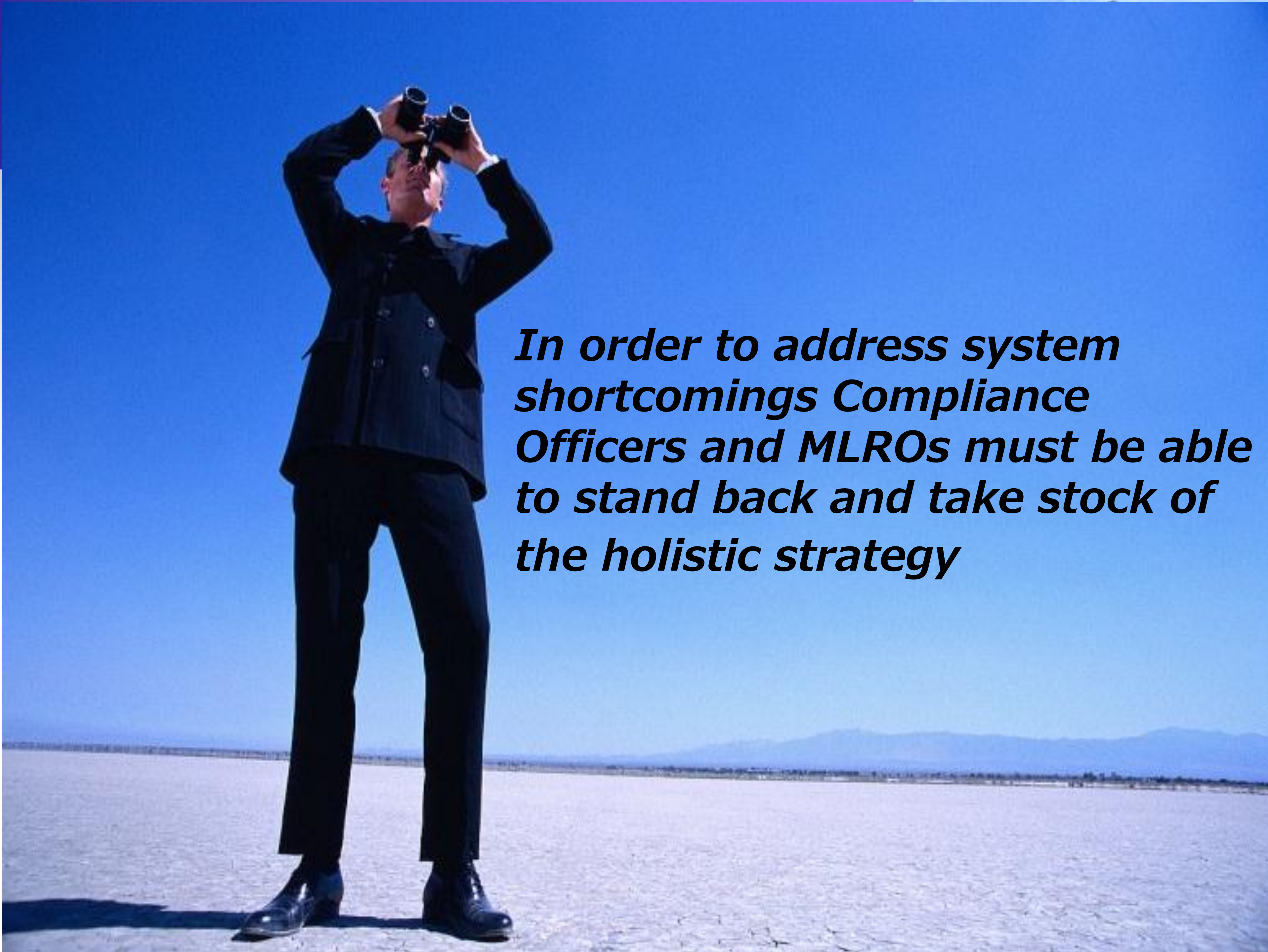
Bank A’s assessment of customer risk was effective:

- *Bank A considered a wide range of factors when assessing customer risk, including company structure [complex structure being clearly defined], country risk which looked at place of incorporation and operation, anticipated account activity, sector risk etc.*
- *There was a clear audit trail to determine the rationale behind a particular grading – in some AIs the audit trail is less clear*
- *Scores were appropriately weighted for certain risk factors*
- *Allocation of inappropriate low risk ratings for certain high risk factors will be queried; adequate explanation why or how the omission is compensated in other aspects of the assessment is expected*

Compliance Reviews

Observations

- Quality of reviews undertaken by Compliance varies tremendously
- We have seen some good practices in some small AIs which made good recommendations around IT system enhancement
- Compliance reviews require adequate sample testing and pre-defined criteria
- Reduction in sample sizes requires explanation
- Compliance reviews should take account of, and complement the work of IA



In order to address system shortcomings Compliance Officers and MLROs must be able to stand back and take stock of the holistic strategy

Sanctions / Screening

- Most AIs understand their obligations under Hong Kong’s financial sanctions regime, though implementation of effective control measures remains challenging for some
- AIs must ensure sufficient oversight of sanctions lists – up to date and accurate is the requirement
- Adequacy and accuracy of customer information in core banking system is an important aspect of effectiveness
- System development needs careful management
  - system migration can lead to inadvertent omissions
- Quality assurance work very important in this area

Sanctions / Screening

Example

Bank A’s customer screening was effective:

- *Policy and procedure were comprehensive and had clearly defined and realistic timeframes including escalation protocols*
- *Bank A ran regular checks on the system and when shortcomings were identified requested the vendor to assist*
- *Testing and validation were evident, both the MLRO and Head of Compliance had consistent and high level of knowledge and views on capabilities of system*
- *The system had been subject to frequent modifications*
  - *clear evidence of ‘ownership’ of the risk*
- *Management of alerts was efficient - staff resignations had been managed by the temporary reallocation of staff*

Sanctions / Screening

Example

Bank B's customer screening was effective:

- *Automated screening was conducted at time of on boarding and on a regular basis thereafter*
- *Both IA and Compliance reviews had been conducted, including sample testing*
- *Bank B recognised that failing to screen the whole customer base periodically, so that potential matches are missed, would expose the AI to unacceptable risks*
- *Bank B policy had clear time frame for alert clearance and backlogs, when they arose, were effectively managed*
- *Implications for both system development and resources had been escalated and acted upon*

Transaction Monitoring

- Hong Kong is a global payments hub
- Importance of effective screening and transaction monitoring systems stressed in all AML/CFT supervision
- Requirement is to monitor transactions to ensure consistency with AIs’ knowledge of the customer.
- Critical to identification & reporting of suspicious activities
- Alert clearance – quality of information
  - Whatever system used, rationale for clearance must be auditable
- Strong oversight expected on system development, testing and validation

Transaction Monitoring

Example

Bank A had recently strengthened effectiveness:

- *Large customer base but until recent review had activated only 3 basic scenario in automated system; some key risks not captured*
- *System upgrade to include a wider range of suitable scenario*
- *Threshold used for corporate and individual customers had been adjusted*
- *Stronger testing and validation of system introduced*
- *System no longer appeared as a “black box” to MLRO*
- *Better quality of alerts enhanced its ability to identity and mitigate higher ML/TF risk*

Transaction Monitoring

Example

Bank B customer screening was largely effective:

- *Automated system – self-initiated review and now incorporating further rules and scenarios based on recent risk assessment*
- *Validation on a regular basis, policy and procedures for regular review of thresholds, parameters and scenarios enacted*
- *Ownership of risk: local staff could explain internal workings of system and understood principle that system was only a tool to aid CDD process and understood shortcomings*
- *Strong oversight on exceptions in review process*
- *Front-line cleared alerts but centralised compliance team reviewed; again challenge noted: proactive role*
    - *The importance of good challenge*

Transaction Monitoring

Observations

Points to note from reviews:

- *Establish anticipated account activity at onboarding*
  - *Occupation: important consideration for risk and level of income*
  - *Corporates: details of expected turnover or counterparty information*
- *Important for AIs to collect information so as to establish what might be suspicious*
- *STRs based on 'large transactions' often linked to over reliance on one threshold based scenario*
- *Process for alert clearance is important; also record keeping to evidence the AI is adequately applying the risk-based approach*

Transaction Monitoring

Example

Bank D’s sophisticated automated transaction monitoring system produced meaningful alerts but could be strengthened:

- *Group-wide systems must take into account adequate local knowledge and risk*
- *Score deduction and suppression rules should be subject to adequate validation and scrutiny before adoption*
- *Alert backlogs need effective management ; resources allocated to the function strengthening*

Periodic Reviews

Examples - Good Practice

- *Some AIs carried out effective annual reviews on PEPs and other high risk customers*
  - *reassessed the ML/TF risk as a core part of the process*
  - *risk-based policies to guide staff in how such reviews should be conducted*
- *Some AIs undertook adverse media searches as part of the review and in light of what was found, reassessed risk*
- *Some AIs undertook review at relationship level rather than customer level*
- *Some AIs assessed whether the relationship was still within its risk appetite as part of the review*
- *Some AIs brought customer documentation up-to-date, especially where this was not up to AMLO standards*

Periodic Reviews

Examples - Good Practice

- *In determining review cycle customer risk should be a key factor*
- *AIs should maintain complete and accurate data on customers due for review so that no customers are omitted*
- *Periods in which reviews should be completed should not be excessive*
  - *There will be exceptions and these need to be managed and the grounds should be recorded*
- *Policy should be clear around what was a 'trigger event' for review*
  - *staff must be clear as to what was required; consistent application is important*

Risk based approach

Observation

- *We will continue to use a risk-based approach in our supervision*
- *This is not a ‘zero failure’ or ‘zero tolerance’ approach, no amount of action by the HKMA or AIs will prevent ML/TF completely*
- *Our objective is that AIs take a risk-based approach to implement AML/CFT measures*
- *Implementation by AIs should be aimed at managing risks*
- *We see some AIs that are successfully implement such an approach*
- *To implement such an approach effectively and successfully, sufficient consideration and resources must be given to execution and customer facing issues*

Q&A