



# Regulatory Update on AML/CFT

## Putting risk-based in AML – The Road Ahead

by Stewart McGlynn

Head of Anti-Money Laundering and Financial Crime Risk, Banking Supervision,  
Hong Kong Monetary Authority

The Hong Kong Institute of Bankers – Annual Banking Conference 2015

25th September 2015

Good afternoon. I would like to thank the Hong Kong Institute of Bankers for inviting me to talk at this conference.

I really welcome the opportunity to speak at this conference, set as it is, around such a significant topic – the "new normal" or, as been discussed in the morning session – 'innovation', 'vibrancy' and capturing 'new opportunities'. Now this is a very broad topic but there is, I believe, a very direct relevance to anti-money laundering (AML) and counter terrorist financing (CFT) systems and how banks approach money laundering (ML) and terrorist financing (TF) risks and developing that theme, I would like to share three things with you today.

*Firstly*, I will begin with a quick review of ML/TF threats we are facing. *Secondly*, I would like to provide a brief overview of a few issues which I believe will drive change in our AML/CFT regime in the foreseeable future. *But mostly*, I will seek to pivot the discussion towards solutions and banks' readiness for change, based on the expectation, discussed in this conference, that banks will adjust their business models to adapt to market developments and the pressures of new regulatory expectations.

### ***ML/TF Threats***

First of all I'd like to start with a few general observations about ML/TF for our debates today. It scarcely needs saying that AML/CFT continues to be a major concern for bank regulators around the world – and we are no different. We expect ML news involving Hong Kong will continue by virtue of the fact that Hong Kong is an IFC. The same applies to London, New York and other large financial centres. At stake for banks, regulators and policymakers are nothing less than protecting the legitimacy and stability of the global financial system, in which Hong Kong plays an important part:



- Hong Kong's banking sector processes hundreds of thousands of cross border payment transactions on a daily basis with great efficiency. *The vast majority of these transactions support perfectly legitimate economic activities.*
- Banks in Hong Kong establish huge numbers of new relationships every day. *The vast majority of these are companies or individuals who want to leverage Hong Kong's unique position and role in the region.*

But the efficiency and advantages that large IFCs offer are also attractive to those who would abuse their reputation as safe places to do business and bank, through illegal activities such as money laundering.

### ***Ongoing Supervisory Focus***

Given the existing ML/TF threats and taking into account Hong Kong's role as a hub in the global payment system, it is important for banks to have effective monitoring systems to identify high risk activities or suspicious transactions, and report these to the Joint Financial Intelligent Unit.

Recognizing this importance, the HKMA has over the past years taken steps to require banks to implement better systems and controls to deter ML/TF and detect suspicious transactions. This is best reflected in our actions: increasing our AML/CFT specialist resources threefold in 4 years and forming a dedicated Division to consolidate that experience. We have also ramped up our AML/CFT supervision and engagement with the banking sector, and provided more guidance, in particular around transaction monitoring and the reporting of suspicious transactions.

These investments have paid off; many banks have improved their understanding of ML/TF risks and their abilities to identify suspicious transactions. We have seen a significant increase in banks' capacity in this area. Taking last year as an example, 83% of all suspicious transaction reports ("STRs") filed to the Joint Financial Intelligence Unit was made by banks, with STRs by banks rising year on year, 19,202 in 2012, 27,328 in 2013 and 31,095 in 2014. This reflects increasingly mature and well developed AML/CFT systems and controls in banks.

However, as positive as some of the results are, it seems that there is always more which needs to be done. For example, although many banks have made great strides in being able to identify and monitor high-risk customers, this remains a challenge for some institutions. The scope of required controls can be underestimated, particularly in banks with significant exposures to riskier business and geographical locations, or that use a lot of outsourcing. Some smaller institutions also have concerns about the amount of time and effort they needed to invest and the resources required in strengthening their AML/CFT controls.

To summarize, the takeaways from all of the above:



- don't expect us to let up in the area of AML/CFT controls. We may refine our approach and focus based on our understanding of changing risks, but strong and effective AML/CFT controls will remain a key supervisory expectation;
- as a subset of the overall approach, we expect banks to place a continued emphasis on the ability to identify higher risk customers, manage the attendant risks and report suspicious transactions where they are identified;
- given Hong Kong's role as a payments hub, customer screening and transaction monitoring systems will continue to be focus areas in our supervision, together with the principle that these systems can only operate effectively if the CDD measures on which the effectiveness of these systems are based is sound and recognize that risk is dynamic and will change over time;
- our expectations are risk-based but higher for more complex institutions. We expect AML/CFT systems to be based on sound modeling, tested and validated as fit for purpose; and
- where we see banks that are not prepared to play by the rules, we will use every available part of our toolkit, including our powers to sanction and reprimand. There should be no doubt as to our resolve in this respect.

Now, let me turn to a few things that will drive change in this space.

### *What will drive changes to our AML/CFT regime?*

Firstly, the revised FATF Recommendations issued in 2012 have raised the bar on regulatory expectations in most jurisdictions. In Hong Kong, discussions have started about what changes will be required to our domestic legislation – the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance or the AMLO – and we are watching how other jurisdictions are implementing these changes. Some changes will require us to tighten certain requirements (e.g. wire transfers), while other changes may permit more flexibility where ML/TF risks are lower or where the risks are being well managed across the banking group.

Secondly, Hong Kong's preparations for the next mutual evaluation scheduled to take place in 2018, have already begun. The FATF evaluation process will include on-site dialogue by the assessors with the private sector, and no doubt some of the banks here today may have compliance staff invited to meet with the assessment team. It's likely the FATF will pay particular attention to how well banks implement their obligations.

Thirdly, the FATF now expects jurisdictions to analyze ML/TF threats and vulnerabilities and have measures in place to mitigate those threats effectively. As you know, a jurisdiction-wide ML/TF risk assessment is being performed for Hong



Kong, which I anticipate will be completed sometime next year and will feed into the process by which banks assess their own risks.

### *How Banks are preparing for Change*

What I would turn to now is how we can ensure banks are ready for those changes and others, and that AML/CFT systems are sufficiently flexible to adapt to market developments and pressures under new regulatory expectations.

We know increasing numbers of banks now understand the value in getting AML/CFT systems right or put another way they now fully understand the benefit of good compliance. These banks also understand that effective ML/TF risk management is not about preventing innovation or growth, to the contrary, they understand that it is essential to allow innovation and growth.

The ability of banks to meet basic AML/CFT requirements is more consistent than ever before. Customer due diligence is, by and large, getting much better. This is something banks are often given too little credit for and unfairly given the substantial efforts that have been made.

Speaking from a general industry perspective, these efforts now need to be taken to the next level, or put another way *greater optimization*. Now some banks are already well down the road on this journey, but some are much nearer the start than the end. Those further down the road are learning that the ability to optimize systems does not rest solely with the size of the budget, numbers of people or the latest IT systems. Even though these are sometimes a requirement, such an approach, driven solely by the desire to meet regulatory expectations rather than truly address the risk, is fundamentally flawed and will increase costs and compliance burden but may not necessarily enhance overall controls. System optimization requires those persons with the necessary skills, Heads of Compliance, Money Laundering Reporting Officers or others to stand back and take stock of the holistic strategy and the AML/CFT model being used by the Bank.

To execute this successfully, they will need many things but two which are fundamental and which I will talk about today are a sound assessment and understanding of the ML/TF risks faced by the institution and a strong ML/TF risk governance framework.

### *ML/TF risk assessment*

In January 2014, the Basel Committee on Banking Supervision issued a document, entitled “Sound Management of Risks related to Money Laundering and Financing of Terrorism” which included the following statement on the importance and conduct of ML/TF risk assessments:

*“Sound risk management requires the identification and analysis of ML/TF risks within the bank and the design and effective implementation of policies and*



*procedures that are commensurate with the identified risks. In conducting a comprehensive risk assessment to evaluate ML/TF risks, a bank should consider all the relevant inherent and residual risk factors at the country, sectoral, bank and business relationship level, among others, in order to determine its risk profile and the appropriate level of mitigation to be applied”.*

We fully endorse those principles; in fact we clarified our expectations through a circular and guidance issued in December 2014. Without a firm foundation in identifying the ML/TF risks inherent in your businesses, it will be hard to manage those risks, let alone show us and others that it is being managed. The risk assessment is critically important in the AML/CFT regime because it allows banks to focus their limited compliance resources where they are needed. Essentially, it operationalizes the risk-based approach we have been talking about for a long time.

However, if the ML/TF risk assessment is broadly unreliable or lacks specificity in the areas which count, the whole ML/TF risk management system may be undermined as resources and efforts will be targeted towards the wrong customers or transactions.

Undertaking an institution-wide ML/TF risk assessment may, for some banks, be challenging and require considerable resources but it is nonetheless essential in order to fully understand a bank's ML/TF risk environment. The results are essential in a number of different areas, including:

- identifying and remediating gaps in AML/CFT policies, procedures and controls
- having board-level decisions on the development and formulation of risk appetite and implementation of control efforts, allocation of resources etc.
- ensuring senior management are updated on what the key risks, control gaps and remediation efforts are
- assisting senior management with strategic decisions in relation to entering or exiting certain sectors or markets etc.
- ensuring regulators are made aware of the key risks, controls gaps and remediation efforts
- assisting senior management to ensure that resources and priorities are aligned with risks

In executing this requirement, some of the challenges that have arisen are as follows:

- Applying these broad institution-wide assessments in a meaningful way using significant volume of data, both customer and transactional, can be limited



by a lack of sensitivity or granularity to specific ML/TF risks. That is why the process by which banks perform the risk assessment is of great interest to us, as much as the report itself.

- Institutional risk assessments can produce tension between truth and cost, which can dilute their effectiveness. Put simply, the operational cost of having a large volume of customers warranting enhanced CDD is high and often not justified, although such an outcome is often the by-product of a poorly delivered assessment.
- We understand industry concerns that there is a lack of consistency in approach amongst regulators. There are varying requirements and levels of granularity and breadth, which can be confusing. We have been making efforts to ensure our requirements are clear, we will for example include the topic in this year's annual AML seminar and we also welcome more global initiatives such as the recent FAQs document published by the Wolfsberg Group or the FATF paper on the risk-based approach for the banking sector. These are informative documents which have added great value to the discussion and should be entirely familiar to you.
- The absence of real time risk assessments, or rather where risk assessments are not regularly updated particularly as the bank adjusts its business model to adapt to market developments, can lead to distortion.

Two final points: Firstly, not every bank has the resources to resolve the above challenges, so extra support or expertise may be a requirement. In this respect, we recommend banks to take a longer term view; the requirement is not to produce a static one-off risk assessment but to demonstrate ownership of the risk, today and tomorrow. Secondly, we do not expect smaller banks to have disproportionately more expensive or complex risk assessments than larger banks; but on the other hand we do want to see a reasonable risk assessment in place that adequately informs senior management.

### ***ML/TF Risk Governance***

We treat ML/TF risk like any other risks and you need to give us a very good reason why you are not taking proactive steps to manage it, which leads me to my last point: banks asking themselves the questions which matter. Please reflect on these questions after today as you consider what good ML/TF risk governance looks like, in the context of your own institution:

- How do you identify the ML/TF risks inherent within your bank and is the concept of risk appetite embedded within that approach? As with any other risk, you cannot hope to mitigate something you don't know the existence.
- Who is responsible for managing ML/TF risks in your institution? We expect banks to be asking themselves how they are encouraging their employees to



be and feel responsible for managing ML/TF risks in the course of daily business operation. Frontline staff plays a crucial role for effective ML/TF risk management; given that frontline staff have the best knowledge of the bank's business and operation, as well as the risks posed to the bank. If they are given the right incentives for good compliance culture, this will help the bank to develop long-term, sustainable business practices.

- The third question is about board and senior management oversight. How proactive is ownership of the AML/CFT agenda? Is a more integrated, strategic approach adopted in your institution to ensure compliance with regulatory expectation? This is about what management information the board and senior management will receive, and how they take this information into account in their decision-making.
- Fourthly, is your ML/TF risk governance forward looking enough? For example, banks should understand international trends and emerging risks; AML/CFT systems should be flexible enough to adapt to future changes.
- Lastly, how does your bank test and ensure control effectiveness, across all three lines of defence? It is imperative for both internal audit and compliance function to play proactive roles in testing banks' AML/CFT controls, and regularly review the AML/CFT system to identify any regulatory gaps and control deficiencies.

So to conclude, the cost of failing to implement strong AML/CFT systems is material. It makes good commercial sense to manage these risks as effectively as any other risk in your institution. To do that, and to make sure that effective measures are applied in the right places, assessment and understanding of ML/TF risks is critical. Responsibility starts at the top with the board taking account of the consequences of ML/TF risk in all its strategic decision-making.

The ongoing challenge, which is shared between the HKMA and the banking sector, is to ensure that banks effectively perform their gatekeeper role and are able to detect and report suspicious transactions on the basis of effective, risk-based AML/CFT controls that work towards our common interest in the long term sustainability of a respected and trusted banking sector.

I look forward to working with you all to do that.

*[Remarks: This is the text of the presentation as drafted and may differ slightly from the delivered version.]*