Nevis Financial Services
Regulation and Supervision Department

NEWSLETTER

AML/CFT Guidelines for Banks

Issue No. 41 April 2016

In this Issue

* *Key points from the Basel Committee Guidelines for the Sound Management of Risks Related to Money Laundering and Terrorist Financing.*
* *AML/CFT Guidelines as they relate to Banks.*

Overview

The inadequacy or absence of sound money laundering and financing of terrorism (ML/FT) risk management exposes banks to serious risks. Sound ML/FT risk management has particular relevance to the overall safety and soundness of banks and the entire banking system. Sound ML/FT risk management provides:

- the avenue to protect the reputation of both banks and national banking systems by preventing and deterring the use of banks to launder illicit proceeds or to raise or move funds in support of terrorism; and
- the preservation of the integrity of the international financial system as well as the work of governments in addressing corruption and in combating the financing of terrorism.

International Standards and Guidelines

Both the Basel Committee on Banking Supervision (Basel Committee) and the Financial Action Task Force (FATF) have a long-standing commitment to promoting the implementation of sound Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) policies and procedures that are critical in protecting the safety and soundness of banks and the integrity of the international financial system. Key Standards/Guidelines that relate to sound ML/FT risk management published by both bodies are :

- *The FATF (2012), International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation* (the FATF Recommendations);
- *The Basel Committee Core Principles for Effective Banking Supervision, revised in 2012; and*
- *The Basel Committee Guidelines for the Sound Management of Risks related to Money Laundering and Terrorist Financing, 2014.*

Essential elements of sound ML/FT risk management for Banks

In accordance with the updated Basel Committee's *Core Principles for Effective Banking Supervision* and the FATF standards (2012), all banks should have adequate policies and processes, including strict customer due diligence (CDD) rules to promote high ethical and professional standards in the banking sector. There are six (6) key elements that should form part of sound ML/FT risk management :

1. Assessment, understanding, management and mitigation of risks;
2. Customer acceptance policy;
3. Customer and beneficial owner identification, verification and risk profiling ;
4. Ongoing Monitoring ;
5. Management of Information; and
6. Reporting of suspicious transactions and asset freezing.

**These elements should be seen as a specific part of the banks' general obligation to have sound risk management. These elements should also be proportional and risk-based, informed by the banks' own risk assessment of ML/FT risks.*

Assessment, Understanding, Management and Mitigation of Risks

(a) Assessment and understanding of risks

In conjunction with FATF Recommendation 1, a comprehensive risk assessment should be undertaken to evaluate ML/FT risks. A bank should consider all the relevant inherent and residual risk factors in order to determine its risk profile and the appropriate level of mitigation to be applied. Policies and procedures for customer acceptance, due diligence and ongoing monitoring should be designed and implemented to adequately control those identified inherent risks. Any resulting residual risk should be managed in line with the bank's risk profile established through its risk assessment .

(b) Proper Governance Arrangements

Effective ML/FT risk management requires proper governance in particular, the requirement for the board of directors to approve and oversee the policies for risk, risk management and compliance. The board of directors should have a clear understanding of ML/FT risks. Information about ML/FT risk assessment should be communicated to the board in a timely and concise manner to assist in informed decision making to ensure that the bank's policies and procedures are managed effectively.

The board of directors and senior management should appoint an appropriately qualified chief Compliance Officer to have overall

responsibility for the AML/CFT function. The Compliance Officer should have the same stature and necessary authority within the bank such that issues raised by this senior officer receive the necessary attention from the board, senior management and business lines.

(c) The three Lines of Defense - Key to Risk Management

(d) **Adequate transaction monitoring system**

A bank should have a monitoring system in place that is adequate with respect to its size, its activities and complexity as well as the risks present in the bank. This system must enable the bank to undergo trend analysis of transaction activity for senior management relating to several key aspects, including changes in the transactional profile of customers.

Customer Acceptance Policy

A bank should develop and implement clear customer acceptance policies and procedures to identify the types of customer that are likely to pose a higher risk of ML and FT pursuant to the bank's risk assessment. When assessing risk, a bank should consider a customer's background, occupation, income and wealth, country of origin and residence , nature and purpose of accounts and business activities to determine the overall risk and the appropriate measures to be applied to manage those risks.

Policies and procedures should require basic due diligence for all customers and commensurate due diligence as the level of risk associated with the customer varies .Where the risks are higher, banks should perform enhanced due diligence to mitigate and manage those risks. The bank's customer acceptance policy should also define circumstances under which the bank would not accept a new business relationship or would terminate an existing one.

Customer and beneficial owner identification, verification and risk profiling

In accordance with the FATF Recommendation 10, a customer refers to any person who enters into a business relationship or carries out an occasional financial transaction with the bank. The customer due diligence should be applied not only to customers but also to persons acting on their behalf and beneficial owners. In accordance with the FATF standards, banks should identify customers and verify their identity. The identity of customers, beneficial owners, as well as persons acting on their behalf, should be verified by using reliable, independent source documents, data or information. Customer risk profiles will assist the bank in further determining if the customer or customer category is higher-risk and requires the application of enhanced CDD measures and controls.

When a bank is unable to complete CDD measures, it should not open the account, commence business relations or perform the transaction.

Ongoing monitoring

Ongoing monitoring is an essential aspect of effective and sound ML/FT risk management. A bank can only effectively manage its risks if it has an understanding of the normal and reasonable banking activity of its customers that enables the bank to identify attempted and unusual transactions which fall outside the regular pattern of the banking activity. Ongoing monitoring should be conducted in relation to all business relationships and transactions. Cross-sectional product/service monitoring should be performed in order to identify and mitigate emerging risk patterns.

Management of Information

A bank should ensure that all information obtained in the context of CDD is recorded . As per FATF Recommendation 11, records should remain accurate, up-to-date and relevant by undertaking regular reviews of existing records and updating the CDD information to add to its usefulness by regulatory bodies. In addition, keeping up-to-date information will enhance the bank's ability to effectively monitor the accounts for unusual or suspicious activities.

Reporting of suspicious transactions and asset freezing

The process for identifying, investigating and reporting suspicious transactions to the FIU should be clearly specified in the bank's policies and procedures and communicated to all personnel through regular training. FATF Recommendation 20 states that once suspicion has been raised in relation to an account or relationship, the bank should ensure that appropriate action is taken to adequately mitigate the risk of the bank being used for criminal activities. A bank should be able to identify and to enforce funds freezing decisions made by the competent authority and it should otherwise not deal with any designated entities or individuals (e.g. terrorists, terrorist organisations) consistent with relevant national legislation.

Sources

The Basel Committee Guidelines for the Sound Management of Risks related to Money Laundering and Terrorist Financing, 2014 and the FATF (2012) International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation.

NEVIS FINANCIAL SERVICES DEPARTMENT