Lecture

IAQS | INSTITUTE OF ACTUARIAL & QUANTITATIVE STUDIES

Class: TY BSc

Subject : Basel

Subject Code: PUSASQF 606B

Chapter: Unit 4 Chapter 2

Chapter Name: Money laundering and financial terrorism

Today's Agenda

1. Introduction
    1. Background

2. Best practices recommended by the committee
    1. Risk Assessment
    2. Risk Management
    3. Risk Mitigation
    4. Risk Monitoring
    5. Customer Acceptance
    6. Customer Verification
    7. Customer Identification

1 Introduction

- Many nations and international bodies have developed laws, regulations or guidelines focused on limiting the use of banking services to support criminal activities, particularly money laundering (ML) or financing of terrorism (FT).
- Though involvement with ML or FT is an operational risk, management of this risk has become a separate subfield due to the intensity of regulatory attention to the issue, the significant level of fines, and the creativity of criminals and terrorists.

1.1 Background

- Basel Committee made recommendations for identifying, assessing, and managing the risks associated with money laundering and the financing of terrorism (ML/FT) through banks.

- Criminals and terrorists use payment services to finance their activities, or to convert funds linked to criminal activity (including tax evasion) to an untainted or laundered form. Because banks are at the heart of the global payment system, they are uniquely vulnerable to being ensnared in such activities, which can expose them to reputational losses, fines, convictions, and restrictions on their ability to do business.

- The concept of customer due diligence (CDD) is important and focuses on the precautionary steps a bank must take to ensure it knows the true identities of the customers with which it is dealing.

2 Best practices recommended by the committee

- The Basel committee is committed to combating money laundering(ML) and the financing of terrorism(FT) as part of its mandate to enhance worldwide financial stability via a strengthening of regulation, supervision, and bank practices.

- The Committee has a long-standing commitment to sound Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) policies and procedures in banks. Banks without sound ML/FT risk management practices are exposed to serious risks including, but not limited to: reputational, operational, compliance, and concentration risks.

- Costs associated with these risks include fines and sanctions by regulators, the termination of wholesale funding and facilities, claims against the bank, loan losses, asset seizures, asset freezes, and investigative costs.

2.1 Risk Assessment

Banks should assess and understand the ML/FT risks inherent within their businesses and customer base:

- All relevant risk factors at the country, sector, bank and business relationship levels should be considered. Characteristics of the customer base, products and services offered, and delivery channels should be considered.
- For each customer or business relationship, a profile of normal activity should be built to support identification of abnormal activity.
- Risk assessments should be documented for potential inspection by authorities.
- International banks should be attentive to national risk assessments and country reports.

2.2 Risk Management

- Proper governance arrangements are necessary for the management of ML/FT risks.
- In particular, these publications require the board of directors to approve and oversee risk policies, risk management activities, and compliance. These functions are critical to the management and mitigation of ML/FT risks.
- ML/FT risk assessments must be communicated to the board of directors in a timely, complete, accurate, and understandable manner.
- The board of directors and senior management should appoint a qualified chief AML/CFT officer with the stature and authority to garner the attention of the board, senior management, and business lines when ML/FT issues arise.

2.3 Risk Mitigation

- The **business units** (e.g., the front office and customer facing activities) are the first line of defense in identifying, assessing, and controlling ML/FT risks. Policies and procedures should be specified in writing and communicated to bank personnel. There should be procedures in place for detecting and reporting suspicious transactions. The bank should carry out employee training on how to identify and report suspicious transactions.

- The **chief officer in charge of AML/CFT** is the second line of defense. The officer should engage in ongoing monitoring and the fulfillment of AML/CFT duties. The officer should be the contact person for AML/CFT issues both internally and externally. To avoid conflicts of interest, the officer should not have business line responsibilities or be responsible for data protection or internal audits. The officer may also be the chief risk officer and should have a direct reporting line to senior management and/or the board of directors.

- The third line of defense is **internal audits**. The bank should establish policies for conducting internal audits of the banks AML/CFT policies. External audits may also play a role in evaluating a banks policies and procedures with respect to the AML/CFT function.

2.4 Risk Monitoring

- The banks risk monitoring systems should be commensurate with the banks size, activities, and complexity. For most banks, and especially for banks that are internationally active, some of the monitoring activities will be automated.

- A bank must document its decision to forgo information technology (IT) monitoring and demonstrate an effective alternative.

- Monitoring systems should be able to provide accurate information to senior management on issues such as changes in the transactional profiles of bank customers.

- The IT system should also enable a bank to determine its own criteria for monitoring and filing suspicious transaction reports (STR) or taking other steps to minimize ML/FT risks.

- Internal audits should evaluate the effectiveness of IT monitoring systems.

2.5 Customer Acceptance

Banks must determine which customers pose a high risk of ML/FT. Factors the bank should consider include the customers:

- Background.
- Occupation including public and/or high profile figures.
- Business activities.
- Sources of income and wealth.
- Country of origin.
- Country of residence, if different from country of origin.
- Choice and use of bank products and services.
- Nature and purpose of the bank account.
- Linked accounts.

For lower-risk customers, simplified assessment procedures may be used (e.g., a customer with low balances who uses the account for routine banking needs). Also, the customer acceptance standards must not be so restrictive that they deny access to the general public, especially financially or socially disadvantaged persons.

2.5 Customer Acceptance

Enhanced due diligence may be required for:

- Accounts with large balances and regular cross-border wire transfers.
- A politically exposed person (PEP), especially foreign PEPs.

Banks must determine the risks they are willing to accept in order to do business with higher risk customers. The bank must also determine the circumstances under which it will not accept a new business relationship or will terminate an existing relationship.

2.6 Customer Verification

- The Financial Action Task Force (FATF) Recommendation 10 defines a customer as any person entering into a business relationship with a bank or carrying out an occasional financial transaction with a bank.

- Banks must, according to FATF standards, identify customers and verify their identity. Banks must establish a systematic procedure for identifying and verifying customers. In some cases, the bank must identify and verify a person acting on behalf of a beneficial owner(s).

- In terms of verification of a persons identity, the bank must be aware that the best documentation is that which is difficult to forge or to obtain illicitly.

- A bank may require a written declaration of the identity of a beneficial owner but should not rely solely on such a declaration. A bank must not forgo identification and verification simply because the customer cannot be present for an interview. The bank should pay particular attention to customers from jurisdictions that are known to have AML/CFT deficiencies.

- Enhanced due diligence is called for in these circumstances.

2.7 Customer Identification

In order to develop customer risk profiles (or categories of customers), the bank should collect data pertaining to the:

- Purpose of the relationship or of the occasional banking transaction.
- Level of assets.
- Size of the transactions of the customer.
- Regularity or duration of the banking relationship.
- Expected level of activity.
- Types of transactions.
- Sources of customer funds, income, or wealth (if necessary).

The bank should identify normal behavior for particular customers or categories of customers and activities that deviate from normal and might be labeled unusual or suspicious.

2.7 Customer Identification

Customer identification documentation may include:

- Passports.
- Identity cards.
- Driving licenses.
- Account files such as financial transaction records.
- Business correspondence.

If the bank cannot perform CDD, it should not open the account or perform a transaction. If the bank must, so as to not interrupt the normal conduct of business, engage in a business transaction prior to verification, and ultimately cannot verify the customers identity, then the bank should consider filing an STR.
The customer should not be informed that the STR has been or will be filed, either directly or indirectly. If the bank believes a customer has been refused banking services from another bank due to concerns about illicit activities, the bank should consider classifying the customer as high risk and engage in enhanced CDD or reject the customer altogether.
If the customer insists on anonymity (or gives an obviously fictitious name), the bank should refuse to accept the customer. Numbered accounts may provide a level of confidentiality for a customer, but the bank must still verify the identity of the account holder. Ongoing monitoring of customer accounts and vigilant record-keeping are necessary to ML/FT risk management.