

# **Money Laundering and Terrorist Financing Risk Assessment Guidelines for Banking Sector**



**Bangladesh Financial Intelligence Unit  
Bangladesh Bank**

## **Preface**

Recommendation 1 of Financial Action Task Force (FATF), the international standard setter on anti money laundering (AML) and combating terrorist financing (CFT) requires financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks. This requirement is reflected in the Money Laundering Prevention Rules (MLPR) 2013. Rule 21 of MLPR 2013 states that every Reporting Organization-Financial Institution (RO-FI) shall conduct periodic risk assessment and forward the same to the Bangladesh Financial Intelligence Unit (BFIU) for vetting. Rule 21 also states that RO-FI shall utilize this risk assessment report after having vetted by BFIU.

To perform the responsibilities and exercises the power bestowed in the Money Laundering Prevention Act (MLPA) 2012, Anti Terrorism Act (ATA) 2009 and Rules there under and to comply with the Recommendation 1 of FATF this guideline titled “Money Laundering and Terrorist Financing Risk Assessment Guidelines for Banking Sector” is prepared for banks working in Bangladesh and issued as per the provisions of Section 23 (1) (d) of MLPA 2012 and Section 15 (1) (d) of ATA 2009.

This guideline will provide the basic ideas of identifying, assessing and mitigating ML & TF risks that banks may encounter in doing their businesses. These risks may arise through/from customers, product and services, business practices or delivery methods and jurisdictions or geographical presence. Bank may also face risks regulatory risks, i.e., non compliant with the requirements of MLPA 2012, ATA 2009 and directives issued by BFIU. In order to treat those identified risks banks shall assess the level of risks by blending likelihood and impact of the risks.

This guideline shall be treated as minimum instructions and indications to identify and assess the risk of ML & TF in their businesses and take effective measures to mitigate the identified risk. It is important that all banks will prepare their own risk assessment and mitigation report in line with this guideline and get approval from their competent authorities before forwarding the same to the BFIU for vetting. After getting vetted by BFIU, the risk assessment and mitigation report shall be communicated to relevant personnel within the bank. Banks are allowed to use more stringent tools to identify and assess the risk of ML & TF in their banks but whatever the methods used the risk assessment and mitigation report should be updated or revised regularly.

It is to remember that the identified risks and measures taken into consideration by banks to mitigate those risks in line with this guideline will be used as an input of Guidance Notes on prevention of Money Laundering which was issued under Managing Core Risks in Banking by Bangladesh Bank (BB).

## Table of Contents

Preface	Page i
List of Abbreviation	iv
 Chapter 1: Overview of ML&TF Risk	 1-4
1. 1 Introduction	1
1.2 Obligation for ML&TF Risk Assessment and Management	1
1.3 Assessing risk	2
1.4 Risk management and mitigation	3
1.5 What is risk	3
1.6 What is risk management	3
1.7 Which risks do you need to manage	3
 Chapter 2: Risk Management Framework	 5-22
2.1 Introduction	5
2.2 Risk management framework	6
2.3 The risk management process	9
2.3.1 Risk identification	9
2.3.2 Risk assessment	13
2.3.3 Calculation of Risk Score	14
2.3.4 Risk treatment	19
2.3.5 Monitor and review	21
2.3.6 Additional tools to help risk assessment	21
2.3.6.1 Applying risk appetite to risk assessment	21
2.3.6.2 Risk tolerance	22
 Chapter 3: Risk management: some important issues	 23-29
3.1 Risk Management Strategies	23
3.2 Ongoing Risk Monitoring	24
3.3 Higher risk scenario	25
3.4 Lower risk Scenario	26
3.5 Risk variables	27
3.6 Counter Measures for Risk	28
3.6.1 Enhanced due diligence measures	28
3.6.2 Simplified CDD measures	28
3.7 Ongoing due diligence	29

## **List of Abbreviations**

<b>AML&amp;CFT</b>	<b>Anti-Money Laundering &amp; Combating the Financing of Terrorism</b>
<b>ATA</b>	<b>Anti Terrorism Act</b>
<b>BFIU</b>	<b>Bangladesh Financial Intelligence Unit</b>
<b>BB</b>	<b>Bangladesh Bank</b>
<b>CDD</b>	<b>Customer Due Diligence</b>
<b>DNFBPs</b>	<b>Designated non-financial businesses and professions</b>
<b>EDD</b>	<b>Enhanced Due Diligence</b>
<b>FATF</b>	<b>Financial Actions Task Force</b>
<b>IPs</b>	<b>Influential Persons</b>
<b>KYC</b>	<b>Know Your Customer</b>
<b>ML</b>	<b>Money Laundering</b>
<b>MLPA</b>	<b>Money Laundering Prevention Act</b>
<b>MLPR</b>	<b>Money Laundering Prevention Rules</b>
<b>PEPs</b>	<b>Politically Exposed Persons</b>
<b>RO-FI</b>	<b>Reporting Organizations-Financial Institutions</b>
<b>STR</b>	<b>Suspicious Transaction Report</b>
<b>SAR</b>	<b>Suspicious Activity Report</b>
<b>TF</b>	<b>Terrorist Financing</b>

## **Chapter: One**

### **Overview of ML&TF Risk**

#### **1. 1 Introduction**

As a lead agency for prevention of money laundering and combating financing of terrorism, Bangladesh Financial Intelligence Unit (BFIU) is very keen to achieve highest success in this regard. The success of AML&CFT program highly depends on efficient assessment of related threat/vulnerability/risk and placing necessary tools for combating ML&TF risks as per the result of assessed threat/vulnerability/risk.

The purpose of this guideline is to:

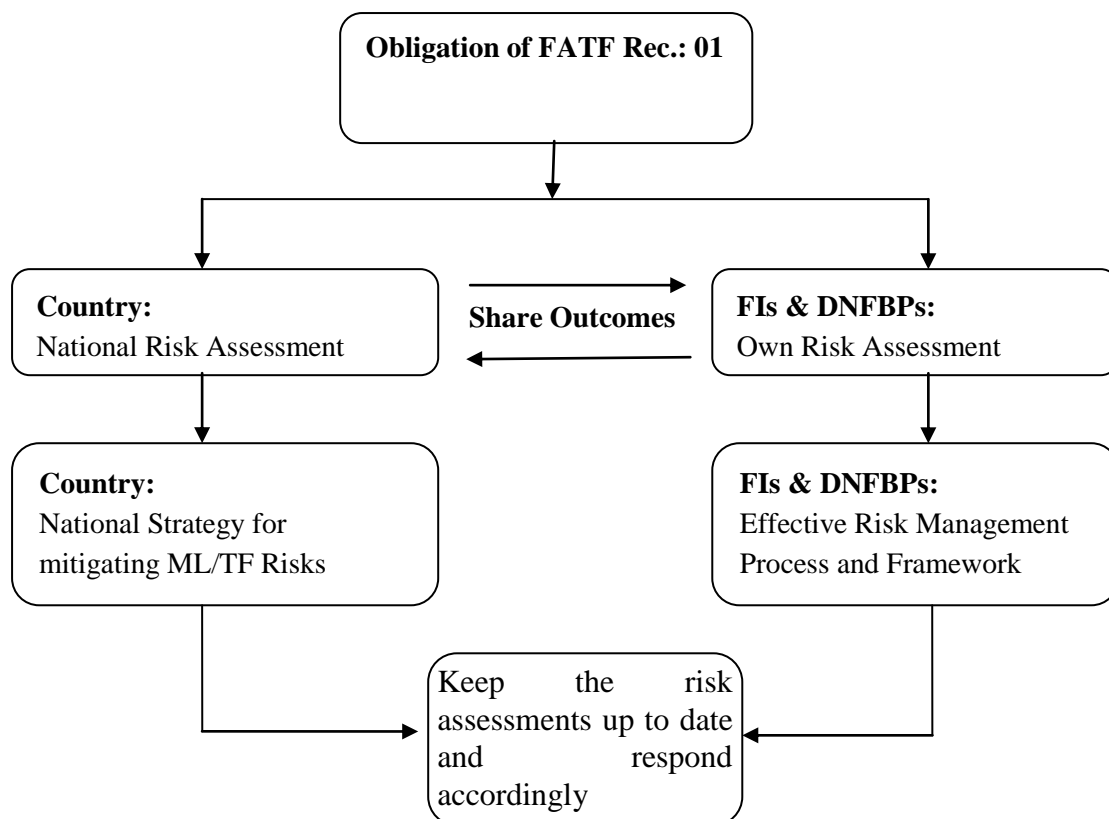
- provide general information about risks related with the products, services, delivery channels, and geographical locations;
- assist banks to assess their ML&TF risks efficiently;
- enable banks in implementing an AML&CFT program appropriate to their business having regard to the business size, nature and complexity; and
- provide a broad risk management framework based on high-level principles and procedures that a bank may wish to consider when developing and implementing a risk-based approach to identify, mitigate and manage ML&TF risks.

This guideline will enable the banks to understand how and to what extent, it is vulnerable to ML&TF risks. It will often result in stylized categorization of risks, which will help banks to determine the level of AML&CFT resources necessary to mitigate that risk.

#### **1.2 Obligation for ML&TF Risk Assessment and Management**

Recommendation 1 of Financial Action Task Force (FATF), the international standard setter on anti money laundering (AML) and combating terrorist financing (CTF) states that countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks. Rule 21 of MLPR 2013 states that every Reporting Organization-Financial Institution (RO-FI) shall conduct periodic risk assessment and forward the same to the Bangladesh Financial Intelligence Unit (BFIU) for vetting. Rule 21 also states that RO-FI shall utilize this risk assessment report after having vetted by BFIU.

The obligation of FATF Recommendation-1 may be shown as follows:



Money Laundering Prevention Act, 2012 empowers BFIU sufficiently to establish a sound and efficient AML&CFT regime. Every reporting agency has to comply with the instructions issued by BFIU under the power of Money Laundering Prevention Act (MLPA), 2012 and Anti Terrorism Act (ATA), 2009 (including all amendments). This Guideline has been issued through BFIU circular letter aiming to strengthen AML&CFT regime in Bangladesh. Therefore, it is obligatory for banks to comply with this Guideline.

### 1.3 Assessing risk

Banks should be required to take appropriate steps to identify and assess their money laundering and terrorist financing risks for customers, countries or geographic areas, products, services and transactions or delivery channels. They should document those assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities.

## **1.4 Risk management and mitigation**

Banks should be required to have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified. They should be required to monitor the implementation of those controls and to enhance them, if necessary. The policies, controls and procedures must be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with national requirements and with guidance from competent authorities.

## **1.5 What is risk**

Risk can be defined as the combination of the probability of an event and its consequences. In simple term, risks can be seen as a combination of the chance that something may happen and the degree of damage or loss that may result if it does occur.

## **1.6 What is risk management**

Risk management is a systematic process of recognizing risk and developing methods to both minimize and manage the risk. This requires the development of a method to identify, prioritize, treat (deal with), control and monitor risk exposures. In risk management, a process is followed where the risks are assessed against the likelihood (chance) of them occurring and the severity or amount of loss or damage (impact) which may result if they do happen.

## **1.7 Which risks do banks need to manage**

For the ML&TF aspects, BFIU expects a risk management practice to address two main risks: business risk and regulatory risk.

***Business risk*** is the risk that your business may be used for ML&TF. The banks must assess the following risks in particular:

- customer risks
- products or services risks
- business practices and/or delivery method risks
- country or jurisdictional risks.

***Regulatory risk*** is associated with not meeting all obligations of banks under the Money Laundering Prevention Act, 2012, Anti Terrorism Act, 2009 (including all amendments), the respective Rules issued under these two acts and instructions issued by BFIU. Examples of



regulatory obligations are failure to report STR/SAR, unable or inappropriately verification of customers and lacking of AML&CFT program (how a business identifies and manages the ML&TF risk it may face) etc.

It is unrealistic that a bank would operate in a completely ML&TF risk-free environment. Therefore, it is suggested that a bank shall identifies the ML&TF risk it faces, and then works out the best ways to reduce and manage that risk.

## **Chapter: Two**

### **Risk Management Framework**

#### **2.1 Introduction**

The banks will have flexibility to construct and tailor their risk management framework for the purpose of developing risk-based systems and controls and mitigation strategies in a manner that is most appropriate to their business structure (including financial resources and staff), their products and/or the services they provide. Such risk-based systems and controls should be proportionate to the ML&TF risk(s) a bank reasonably faces.

The risk management framework discussed in this guideline aims to assist banks to develop and implement their AML&CFT programs in compliance with the existing legal and regulatory requirements and international standards and best practices.

For effective risk management, the banks should at all levels follow the principles below:

- Risk management contributes to the demonstrable achievement of objectives and improvement of performance, governance and reputation.
- Risk management is not a stand-alone activity that is separate from the main activities and processes of the bank. Risk management is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning.
- Risk management helps decision makers making informed choices, prioritize actions and distinguish among alternative courses of action.
- Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.
- A systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results.
- Risk management is based on the best available information.
- Risk management is aligned with the bank's external and internal context and risk profile.
- Risk management is transparent and inclusive.
- Risk management is dynamic, iterative and responsive to change.

Following the above mentioned principles banks are expected to develop and maintain logical, comprehensive and systematic methods to address each of the components referred to in this Guideline and that such methods and the banks' approach to ML&TF risk are

understood, implemented and maintained, to some appropriate extent, within their organizations.

Banks would be expected to demonstrate to BFIU and Bangladesh Bank (BB) (for example, when a BFIU/BB inspection is being conducted) that their risk based systems and controls are suitable to their particular businesses and consistent with prudent and good practices.

In assessing and mitigating ML&TF risk, the banks should consider a wide range of financial products and services, which are associated with different ML/TF risks. These include, but are not limited to:

- Retail banking: where banks offer products and services directly to personal and business customers (including legal arrangements), such as current accounts, loans (including mortgages) and savings products;
- Corporate and investment banking: where banks provide corporate finance and corporate banking products and investment services to corporations, governments and institutions;
- Investment services: where banks provide products and services to manage their customers' wealth (sometimes referred to as privileged or priority banking); and
- Correspondent services: where banking services are provided by one bank (the "correspondent bank") to another bank (the "respondent bank").

Banks should be mindful of those differences when assessing and mitigating the ML/TF risk to which they are exposed.

## **2.2 Risk Management Framework**

A risk management framework would consist of:

- (a) establishing the internal and external context within which the designated service is, or is to be, provided. These may include:
  - the types of customers;
  - the nature, scale, diversity and complexity of their business;
  - their target markets;
  - the number of customers already identified as high risk;
  - the jurisdictions the bank is exposed to, either through its own activities or the activities of customers, especially jurisdictions with relatively higher levels of corruption or organized crime, and/or deficient AML/CFT controls and listed by FATF;

-the distribution channels, including the extent to which the bank deals directly with the customer or the extent to which it relies (or is allowed to rely on) third parties to conduct CDD and the use of technology;

-the internal audit and regulatory findings;

-the volume and size of its transactions, considering the usual activity of the bank and the profile of its customers.

(b) risk identification;

(c) risk assessment or evaluation; and

(d) risk treatment (mitigating, managing, control, monitoring and periodic reviews).

In identifying and assessing the ML/TF risk to which they are exposed, banks should consider a range of factors which may include:

**Figure 1: The risk management framework at a glance**

- **Risk identification:**

**Identify the main ML&TF risks:**

- customers
- products & services
- business practices/delivery methods or channels
- country/jurisdiction

**Identify the main regulatory risks:**

- failure to report STRs/SARs
- inappropriate customer verification
- inappropriate record keeping
- lack of AML/CFT program

- **Risk assessment/evaluation**

**Measure the size & importance of risk:**

- likelihood – chance of the risk happening
- impact – the amount of loss or damage if the risk happened
- likelihood X impact = level of risk (risk score)

- **Risk treatment**

**Manage the business risks:**

- minimize and manage the risks
- apply strategies, policies and procedures

**Manage the regulatory risks:**

- put in place systems and controls
- carry out the risk plan and AML&CFT program

- **Risk monitoring and review**

**Monitor and review the risk plan:**

- develop and carry out monitoring process
- keep necessary records
- review risk plan and AML&CFT program
- do internal audit or assessment
- do AML&CFT compliance report

## 2.3 The risk management process

### 2.3.1 Risk identification

**Identify the main ML&TF risks:**

- customers
- products & services
- business practices/delivery methods or channels
- country/jurisdiction

**Identify the main regulatory risks:**

- failure to report STRs/SARs
- inappropriate customer verification
- inappropriate record keeping
- lack of AML&CFT program

The first step is to identify what ML&TF risks exist in a bank when providing designated services. Some examples of ML&TF risk associated with different banking activities:

- *Retail banking*: provision of services to cash-intensive businesses, volume of transactions, high-value transactions, diversity of services.
- *Wealth management*: culture of confidentiality, difficulty to identify beneficial owners, concealment (use of offshore trusts), banking secrecy, complexity of financial services and products, PEPs, high value transactions, multiple jurisdictions.
- *Investment banking*: layering and integration, transfer of assets between parties in exchange for cash or other assets, global nature of markets.
- *Correspondent banking*: high value transactions, limited information about the remitter and source of funds especially when executing transactions with a bank located in a jurisdiction that does not comply or complies insufficiently with FATF Recommendations, the possibility that PEPs are involved regarding the ownership of a bank.

As previously discussed, there are two risk types: **business risk and regulatory risk.**

#### **Business risk**

A bank must consider the risk posed by any element or any combination of the elements listed below:

- Customers
- Products and services

- Business practices/delivery methods or channels
- Countries it does business in/with (jurisdictions).

Under these four groups, individual risks to a bank can be determined. While not an exhaustive list, some of these individual risks may include:

➤ **Customers:** followings are some indicators (but not limited to) to identify ML&TF risk arises from customers of a bank.

- a new customer
- a new customer who wants to carry out a large transaction
- a customer or a group of customers making lots of transactions to the same individual or group
- a customer who has a business which involves large amounts of cash
- a customer whose identification is difficult to check
- a customer who brings in large amounts of used notes and/or small denominations.
- customers conducting their business relationship or transactions in unusual circumstances, such as:
  - significant and unexplained geographic distance between the institution and the location of the customer
  - frequent and unexplained movement of accounts to different institutions
  - frequent and unexplained movement of funds between institutions in various geographic locations
- a non- resident customer
- a corporate customer whose ownership structure is unusual and excessively complex
- customers that are politically exposed persons (PEPs) or influential persons (IPs) or head of international organizations and their family members and close associates
- customers submits account documentation showing an unclear ownership structure

- customer opens account in the name of his/her family member who intends to credit large amount of deposits not consistent with the known sources of legitimate family income.

➤ **Products and services:**

- private banking i.e., prioritized or privileged banking
- credit card
- anonymous transaction
- non face to face business relationship or transaction
- payment received from unknown or unrelated third parties
- any new product & service developed
- service to walk-in customers
- mobile banking.

➤ **Business practice/delivery methods or channels:**

- direct to the customer
- online/internet
- phone
- fax
- email
- third-party agent or broker.

➤ **Country/jurisdiction:**

- any country which is unidentified by credible sources as having significant level of corruption and criminal activity
- any country subject to economic or trade sanctions
- any country known to be a tax haven and unidentified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organizations operating within their country
- any country unidentified by FATF or FSRBs as not having adequate AML&CFT system
- any country identified as destination of illicit financial flow



▪ **Regulatory risk**

This risk is associated with not meeting the requirements of the Money laundering Prevention Act, 2012, Anti Terrorism Act, 2009 (including all amendments) and instructions issued by BFIU. Examples of some of these risks are:

- customer/beneficial owner identification and verification not done properly
- failure to keep record properly
- failure to scrutinize staffs properly
- failure to train staff adequately
- not having an AML&CFT program
- failure to report suspicious transactions or activities
- not submitting required report to BFIU regularly
- not having an AML&CFT Compliance Officer
- failure of doing Enhanced Due Diligence (EDD) for high risk customers (i.e., PEPs, IPs)
- not complying with any order for freezing or suspension of transaction issued by BFIU or BB
- not submitting accurate information or statement requested by BFIU or BB.

### 2.3.2. Risk assessment:

For assessing risk, in this chapter we have used, the Table -1, which is a simple & generic table with Risk Score and Treatment. Risk Score can be found by blending likelihood and impact; the details will be explained later on. Table -1 is used, only the examples of customer risk assessment and developed phase by phase so that user can have a good idea of risk assessment.

**Table 1: Risk Management Worksheet – risk**

<b>Risk group:</b>	<b>Customers</b>			
<b>Risk</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk score</b>	<b>Treatment/Action</b>
New customer ( <i>example only</i> )				
Customer who brings in large amounts of used notes and/or small denominations ( <i>example only</i> )				
Customer whose business address and registered office are in different geographic locations ( <i>example only</i> )				

A table similar to *Table 1* shown above - *Risk management worksheet* - could be used for each risk group in preparation for assessing and managing those risks: customers, products and services, business practices/delivery methods, country/jurisdiction and the regulatory risks.

### 2.3.3. Calculation of Risk Score

#### Measure the size & importance of risk:

- likelihood – chance of the risk happening
- impact – the amount of loss or damage if the risk happened
- likelihood X impact = level of risk (risk score)

Having identified the risks involved, they need to be assessed or measured in terms of the chance (likelihood) they will occur and the severity or amount of loss or damage (impact) which may result if they do occur. The risk associated with an event is a combination of the chance (likelihood) that the event will occur and the seriousness of the damage (impact) it may do.

Therefore each risk element can be rated by:

- the chance of the risk happening – **‘likelihood’**
- the amount of loss or damage if the risk happened – **‘impact’ (consequence)**.

To help assess the risks identified in the first stage of this process, we can apply the risk rating scales for likelihood (*Table 2*) on page 15 and impact (*Table 3*) on page 16 and from these get a level of risk or risk score using the risk matrix (*Figure 2*) on page 16.

<b>LIKELIHOOD</b>	<b>X</b>	<b>IMPACT</b>	<b>=</b>	<b>RISK LEVEL/SCORE</b>
-------------------	----------	---------------	----------	-----------------------------

#### ▪ Likelihood scale

A likelihood scale refers to the potential of an ML&TF risk occurring in the business for the particular risk being assessed. Three levels of risk are shown in Table 2, but the entity can have as many as they believe are necessary.

**Table 2: Likelihood scale**

Frequency	Likelihood of an ML&TF risk
Very likely	Almost certain: it will probably occur several times a year
Likely	High probability it will happen once a year
Unlikely	Unlikely, but not impossible

▪ **Impact scale**

An impact scale refers to the seriousness of the damage (or otherwise) which could occur should the event (risk) happen.

In assessing the possible impact or consequences, the assessment can be made from several viewpoints. It does not cover everything and it is not prescriptive. Impact of an ML&TF risk could, depending on individual bank and its business circumstances, be rated or looked at from the point of view of:

- how it may affect the business (if through not dealing with risks properly the bank suffers a financial loss from either a crime or through fines from BFIU or regulator)
- the risk that a particular transaction may result in the loss of life or property through a terrorist act
- the risk that a particular transaction may result in funds being used for any of the following: corruption and bribery, counterfeiting currency, counterfeiting deeds and documents, smuggling of goods/workers/immigrants, banking offences, narcotics offences, psychotropic substance offences, illegal arms trading, kidnapping, terrorism, theft, embezzlement, or fraud, forgery, extortion, smuggling of domestic and foreign currency, black marketing
- the risk that a particular transaction may cause suffering due to the financing of illegal drugs
- reputational risk – how it may affect the bank if it is found to have (unknowingly) aided an illegal act, which may mean government sanctions and/or being shunned by the community of customers

- how it may affect the wider community of customers if it is found to have aided an illegal act; the community may get a bad reputation as well as the business.

Three levels of impact are shown in Table 3, but the bank can have as many as they believe are necessary.

**Table 3: Impact scale**



Consequence	Impact – of an ML/TF risk
Major	Huge consequences – major damage or effect. Serious terrorist act or large-scale money laundering.
Moderate	Moderate level of money laundering or terrorism financing impact.
Minor	Minor or negligible consequences or effects.

#### ▪ Risk matrix and risk score

Use the risk matrix to combine LIKELIHOOD and IMPACT to obtain a risk score. The risk score may be used to aid decision making and help in deciding what action to take in view of the overall risk. How the risk score is derived can be seen from the risk matrix (*Figure 2*) and risk score table (*Table 4*) shown below. Four levels of risk score are shown in Figure 2 and Table 4, but the bank can have as many as they believe are necessary.

**Figure 2: Risk matrix**

Threat level for ML/TF risk

<b>LIKELIHOOD</b>  <b>What is the chance it will happen?</b>	Very Likely	Medium 2	High 3	Extreme 4
	Likely	Low 1	Medium 2	High 3
	Unlikely	Low 1	Low 1	Medium 2
		Minor	Moderate	Major
		<b>How serious is the risk?</b> <b>IMPACT</b> 		

**Table 4: Risk score table**

Rating	Impact – of an ML&TF risk
<b>4 Extreme</b>	<b>Risk almost sure to happen and/or to have very serious consequences.</b> <b>Response:</b> <b>Do not allow transaction to occur or reduce the risk to acceptable level.</b>
<b>3 High</b>	<b>Risk likely to happen and/or to have serious consequences.</b> <b>Response:</b> <b>Do not allow transaction until risk reduced.</b>
<b>2 Medium</b>	<b>Possible this could happen and/or have moderate consequences.</b> <b>Response:</b> <b>May go ahead but preferably reduce risk.</b>
<b>1 Low</b>	<b>Unlikely to happen and/or have minor or negligible consequences.</b> <b>Response:</b> <b>Okay to go ahead.</b>

- **Risk Assessment and Management Exercise:**

From the above discussion, the banks will have an idea to calculate risk score by blending likelihood and impact, the risk matrix and risk score and can assess the risks of individual customer, product/service, delivery channel and risks related to geographic region by using the simplified risk management worksheet (Table-01). It can also fix up its necessary actions against the particulars outcomes of risks. All the exercises done by the banks would be called together "**Risk Registrar**".

Once threat levels and risk scores have been allocated banks can be entered in the risk management worksheet (*Table 5*) next to the risk.

**Table 5: Risk management worksheet – threat level and risk score**

<b>Risk group:</b>	<b>Customers</b>			
<b>Risk</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk score</b>	<b>Treatment/Action</b>
<b>New customer (example only)</b>	<b>Likely (example only)</b>	<b>Moderate (example only)</b>	<b>2 (example only)</b>	
<b>Customer who brings in large amounts of used notes and/or small denominations (example only)</b>	<b>Likely (example only)</b>	<b>Major (example only)</b>	<b>3 (example only)</b>	
<b>Customer whose business address and registered office are in the different geographic location (example only)</b>	<b>Very likely (example only)</b>	<b>Major (example only)</b>	<b>4 (example only)</b>	

### 2.3.4 Risk treatment

#### Manage the business risks:

- minimize and manage the risks
- apply strategies, policies and procedures

#### Manage the regulatory risks:

- put in place systems and controls
- carry out the risk plan and AML&CFT program

This stage is about identifying and testing methods to manage the risks the bank may have identified and assessed in the previous process. In doing this they will need to consider putting into place strategies, policies and procedures to help reduce (or treat) the risk. Examples of a risk reduction or treatment step are:

- setting transaction limits for high-risk products
- having a management approval process for higher-risk products
- process to place customers in different risk categories and apply different identification and verification methods
- not accepting customers who wish to transact with a high-risk country.

**Table 6: Risk management worksheet – risk treatment or action**

<b>Risk group:</b>	<b>Customers</b>			
<b>Risk</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk score</b>	<b>Treatment/Action</b>
New customer ( <i>example only</i> )	Likely ( <i>example only</i> )	Moderate ( <i>example only</i> )	2 ( <i>example only</i> )	<b>Standard ID check</b>
Customer who brings in large amounts of used notes and/or small denominations ( <i>example only</i> )	Likely ( <i>example only</i> )	Major ( <i>example only</i> )	3 ( <i>example only</i> )	<b>Standard + additional ID check</b>
Customer whose business address and registered office are in the different geographic location ( <i>example only</i> )	Very likely ( <i>example only</i> )	Major ( <i>example only</i> )	4 ( <i>example only</i> )	<b>Do not accept as customer</b>



Another way to reduce the risk is to use a combination of risk groups to modify the overall risk of a transaction. The bank may choose to use a combination of customer, product/service and country risk to modify an overall risk.

It is important to remember that identifying, for example, a customer, transaction or country as high risk does not necessarily mean that money laundering or terrorism financing is involved. The opposite is also true: just because a customer or transaction is seen as low risk does not mean the customer or transaction is not involved in money laundering or terrorism financing. Experience and common sense should be applied to the risk management process of an entity.

### 2.3.5 Monitor and review

#### **Monitor & review the risk plan:**

- develop and carry out monitoring process
- keep necessary records
- review risk plan and AML&CFT program
- do internal audit or assessment
- do AML&CFT compliance report

Keeping records and regular evaluation of the risk plan and AML&CFT program is essential. The risk management plan and AML&CFT program cannot remain static as risks change over time; for example, changes to customer base, products and services, business practices and the law.

Once documented, the entity should develop a method to check regularly on whether AML&CFT program is working correctly and well. If not, the entity needs to work out what needs to be improved and put changes in place. This will help keep the program effective and also meet the requirements of the AML&CFT Acts and respective Rules.

### 2.3.6 Additional tools to help risk assessment

The following tools or ideas can be useful in helping to manage risk. It can be included in the previous risk assessment process so that the decisions are to be better informed.

#### 2.3.6.1 Applying risk appetite to risk assessment

Risk appetite is the amount of risk a bank is prepared to accept in pursuit of its business goals. Risk appetite can be an extra guide to the risk management strategy and can also help deal with risks. It is usually expressed as an acceptable/unacceptable level of risk. Some questions to ask are:

- What risks will the bank accept?
- What risks will the bank not accept?
- What risks will the bank treat on a case by case basis?
- What risks will the bank send to a higher level for a decision?

The risk matrix can be used to show the risk appetite of the bank.

In a risk-based approach to AML&CFT the assessment of risk appetite is a judgment that must be made by the bank. It will be based on its business goals and strategies, and an assessment of the ML&TF risks it faces in providing the designated services to its chosen markets.

**Figure 3: Sample risk matrix showing risk appetite**

<b>LIKELIHOOD</b> ↑	Very Likely	Acceptable Risk Medium 2	Unacceptable Risk High 3	Unacceptable Risk Extreme 4
	Likely	Acceptable Risk Low 1	Acceptable Risk Medium 2	Unacceptable Risk High 3
	Unlikely	Acceptable Risk Low 1	Acceptable Risk Low 1	Acceptable Risk Medium 2
What is the chance it will happen?		Minor	Moderate	Major
		How serious is the risk? <b>IMPACT</b> →		

### 2.3.6.2 Risk tolerance

In addition to defining bank's risk appetite, the entity can also define a level of variation to how it manages that risk. This is called risk tolerance, and it provides some flexibility whilst still keeping to the risk framework that has been developed.

## **Chapter: Three**

### **Risk management: some important issues**

#### **3.1 Risk Management Strategies**

The banks may adopt the following components (where appropriate to the nature, size and complexity of its business), among others, as part of its risk management strategy:

- a) reviews at senior management level of the bank's progress towards implementing stated ML&TF risk management objectives
- b) clearly defined management responsibilities and accountabilities regarding ML&TF risk management
- c) adequate staff resources to undertake functions associated with ML&TF risk management
- d) specified staff reporting lines from ML&TF risk management system level to board or senior management level, with direct access to the board member(s) or senior manager(s) responsible for overseeing the system
- e) procedural controls relevant to particular designated services
- f) documentation of all ML&TF risk management policies
- g) a system, whether technology based or manual, for monitoring the bank's compliance with relevant controls
- h) policies to resolve identified non-compliance
- i) appropriate training program(s) for staff to develop expertise in the identification of ML&TF risk(s) across the bank's designated services
- j) an effective information management system which should:
  - i) produce detailed and accurate financial, operational and compliance data relevant to ML&TF risk management
  - ii) incorporate market information relevant to the global AML&CFT environment which may assist the banks to make decisions regarding its risk management strategy
  - iii) enable relevant, accurate and timely information to be available to a relevant officer (for example, the AML&CFT Compliance Officer) within the banks
  - iv) allow the banks to identify, quantify, assess and monitor business activities relevant to ML&TF risk(s)

- v) allow the banks to monitor the effectiveness of and compliance with its internal AML&CFT systems and procedures
- vi) allow the banks to regularly assess the timeliness and relevance of information generated, together with its adequacy, quality and accuracy.

It should be noted that a bank can adopt other strategies in addition to taking into account of any of the above factors (where relevant), if it considers this approach is appropriate in accordance with its risk management framework.

### **3.2 Ongoing Risk Monitoring**

A bank's ongoing monitoring of its risk management procedures and controls may also alert the bank to any potential failures including (but not limited to):

- a) failure to include all mandatory legislative components
- b) failure to gain board and/or executive approval of the AML&CFT program
- c) insufficient or inappropriate employee due diligence
- d) frequency and level of risk awareness training not aligned with potential exposure to ML&TF risk(s)
- e) changes in business functions which are not reflected in the AML&CFT program (for example, the introduction of a new product or distribution channel)
- f) failure to undertake independent review (at an appropriate level and frequency) of the content and application of the AML&CFT program
- g) legislation incorrectly interpreted and applied in relation to a customer identification procedure
- h) customer identification and monitoring systems, policies and procedures that fail to:
  - i) prompt, if appropriate, for further identification and/or verification when the ML&TF risk posed by a customer increases
  - ii) detect where a customer has not been sufficiently identified and prevent the customer from receiving the designated service
  - iii) take appropriate action where a customer provides insufficient or suspicious information in relation to an identification check
  - iv) take appropriate action where the identification document provided is neither an original nor a certified copy

- v) recognize foreign identification documentation issued by a high risk jurisdiction
- vi) record comprehensive details of identification documents, for example, the date of issue
- vii) consult appropriate resources in order to identify high-risk customers
- viii) identify when an expired or old identification document (for example, a driver's license) has been used
- ix) collect any other name(s) by which the customer is known
- i) lack of access to information sources to assist in identifying higher risk customers (and the jurisdictions in which they may reside), such as PEPs, terrorists and narcotics traffickers
- j) lack of ability to consistently and correctly train staff and/or third parties, particularly in areas with high turnover in:
  - i) customer identification policies, procedures and systems
  - ii) identifying potential ML&TF risks
- k) acceptance of documentation that may not be readily verifiable.

### **3.3 Higher risk scenario**

When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially higher-risk situations include the following:

#### **a) Customer risk factors**

- The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer)
- Non-resident customers
- Legal persons or arrangements that are personal asset-holding vehicles
- Companies that have nominee shareholders or shares in bearer form
- Business that are cash-intensive
- The ownership structure of the company appears unusual or excessively complex given the nature of the company's business

**b) Country or geographic risk factors**

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML&CFT systems
- Countries subject to sanctions, embargos or similar measures
- Countries identified by credible sources as having significant levels of corruption or other criminal activity
- Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country

**c) Product, service, transaction or delivery channel risk factors**

- Private banking
- Anonymous transactions (which may include cash)
- Non-face-to-face business relationships or transactions
- Payment received from unknown or un-associated third parties.

**3.4 Lower risks Scenario**

There are circumstances where the risk of money laundering or terrorist financing may be lower. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially lower risk situations include the following:

**a) Customer risk factors**

- Banks – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations, have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements
- Public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable

means), which impose requirements to ensure adequate transparency of beneficial ownership

- Public administrations or enterprises.

**b) Product, service, transaction or delivery channel risk factors:**

- Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

**(c) Country risk factors**

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML&CFT systems
- Countries identified by credible sources as having a low level of corruption or other criminal activity. In making a risk assessment, countries or financial institutions could, when appropriate, also take into account possible variations in money laundering and terrorist financing risk between different regions or areas within a country.

Note that having a lower money laundering and terrorist financing risk for identification and verification purposes does not necessarily mean that the same customer poses lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions.

### **3.5 Risk variables**

When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels risk, a bank should take into account risk variables relating to those risk categories. These variables, either singly or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures. Examples of such variables include:

- The purpose of an account or relationship
- The level of assets to be deposited by a customer or the size of transactions undertaken
- The regularity or duration of the business relationship.



### **3.6 Counter Measures for Risk**

#### **3.6.1 Enhanced due diligence measures**

Banks should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, banks should be required to conduct enhanced due diligence (EDD) measures for higher-risk business relationships include:

- Obtaining and verifying additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner
- Obtaining and verifying additional information on the intended nature of the business relationship
- Obtaining and verifying information on the source of funds or source of wealth of the customer
- Obtaining and verifying information on the reasons for intended or performed transactions
- Obtaining and verifying the approval of senior management to commence or continue the business relationship
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

#### **3.6.2 Simplified CDD measures**

Where the risks of money laundering or terrorist financing are lower, the banks are allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures should be commensurate with the lower risk factors (e.g. the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring). Examples of possible measures are:

- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold)
- Reducing the frequency of customer identification updates
- Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold
- Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established. Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

### **3.7 Ongoing due diligence**

Banks should be required to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of customers.