Da Afghanistan Bank
Financial Supervision Department

ML/TF Risk Assessment Guideline

September 2019

Table of Contents

Abbreviations

ML	Money Laundering
TF	Terrorist Financing
AML-PC Law	Anti Money Laundering and Proceeds of Crime Law
AML	Anti Money Laundering
CFT	Combating Financing of Terrorism
FATF	Financial Action Task Force
IMF	International Monetary Fund
PEP	Politically Exposed Person
FXD	Foreign Exchange Dealer
MSP	Money Service Provider
NGO	Non Government Organization

INTRODUCTION

This Guideline is prepared to provide general guidance to banks operating in Afghanistan in order for them to assess their money laundering and terrorist financing risk they are exposed to. It is not mandatory for banks to adopt and follow the same mechanism in assessing their ML/TF risk and also the examples provided in this guideline are not mandatory requirements. The banks can adopt a ML/TF risk assessment mechanism which is commensurate with their business nature and complexity as well as its vulnerabilities to money laundering and terrorist financing risk, but the mechanism/method and process adopted and designed by the banks should be standard ones and should be in accordance with requirements of Anti Money laundering and proceeds of crime law and, relevant regulation

1. Background

As per Article 11 of Anti Money laundering and proceeds of crime law, Article 6 of AML/CFT Responsibilities and Preventative Measures Regulation and FATF recommendation, banks are required to conduct a business related risk assessment of their ML/TF risks. To conduct an AML/TF risk assessment, a bank should take appropriate steps to identify and assess the ML/TF risks related to customers, countries (geographic areas) products, services, transactions, and delivery channels.

A risk assessment enables the banks to focus on its AML/CFT efforts and to adopt appropriate measures to optimally allocate the necessary resources. The banks should document those assessments in writing and keep these assessments up to date. The nature and extent of ML/TF risk assessment should be appropriate to the nature, complexity and size of the business. Banks should always understand their ML/TF risks before providing any kind of products and services.

On the Basis of the assessments conducted, the banks should have controls, policies and procedures that enable them to manage and mitigate the identified risks effectively. The term "mitigate'' in this context means reducing the seriousness and extent of ML/TF risks. Banks should monitor the implementation of those controls and enhance them, if necessary. When assessing the ML/TF risks, banks should consider all the relevant risk factors before determining the level of overall risks and the appropriate level of mitigation to be applied. Banks may differentiate the control measures depending on the type and level of risk for the different risk factors. The risk assessment should be done for each group or type of customers, business relationships, products and services rendered by the banks within the business/operations.

Banks, regardless of their sizes and complexities, are expected to develop an adequate risk management system for ML/TF. This risk management system is to ensure that ML/TF risks

should be continuously and comprehensively identified, assessed, monitored, managed and mitigated accordingly. The control measures should be developed based on the nature and intensity of identified risk (Inherent risks) and strong control measures which would help in mitigating the risks to a great extent should be developed.

2. Objective

The objective of this guideline is to assist banks operating in Afghanistan in order to have high quality and effective ML/TF risk assessment and ML/TF risk management systems that is appropriate and proportionate to the risks. The AML/CFT control measures developed and devised should be commensurate to the risk to deter and prevent money laundering and terrorist financing by providing information on the following:

- A common understanding of what ML/TF risk assessment encompasses;
- Outlining the recommended steps involved in conducting ML/TF risk assessment;
- Providing general information about risks related with the customers, products, services, delivery channels and geographical locations;
- To develop policies, controls and procedures that enable them to manage and mitigate effectively the inherent risks that have been identified;
- Designing an organizational structure to execute ML/TF risk management controls;
- Process to systematically check and assess the adequacy of the control system; and
- Adopt additional measures to mitigate the ML/TF risk frequently.

3. Definitions

The terms and expression used in this guideline shall have the same meanings assigned to it in the above listed laws and regulations as the case may be, unless otherwise defined in this document.

3.1. Money Laundering' shall mean the offence set forth in Article 4 of Anti Money Laundering and Proceeds of Crime law.

3.2. Terrorist Financing' the offense as defined in Article 4 of Combating Financing of Terrorism Law.

3.3. FATF' refers to the Financial Action Task Force, an intergovernmental body that establishes the international Anti Money Laundering/Combating the Financing of Terrorism and proliferation standards.

3.4. 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.

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

- Products or services risks;
- Customer risks;
- Business practices and/or delivery method risks; and
- Country or jurisdictional/geographical risks.

3.6. Regulatory risk is associated with not meeting the obligations and requirement of AML-PC law, AML/CFT responsibilities and preventative measures regulations and DAB circulars.

3.7. 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.

3.8. PEP (politically exposed person) means any natural person who is or was entrusted with a prominent public function in the Islamic Republic of Afghanistan or a foreign country; or a person who is or has been entrusted with a prominent function in an international organization, , or a key figure of political parties including family members and close associates.

3.9. Customer' in relation to a transaction or an account includes:

(i) the person in whose name a transaction, business relationship, or account is arranged, opened or undertaken;
(ii) a signatory to a transaction, business relationship, or account;
(iii) any person to whom an account, or rights or obligations under a transaction has been assigned or transferred;
(iv) any person who is authorised to conduct a transaction, or to control a business relationship or an account; or
(v) Such other persons as having ties to the account.

4. The Purpose of ML/TF Risk Assessment

The key purpose of ML/TF risk assessment is to drive improvements in money laundering and terrorist financing risk management process through identifying and understanding the ML/TF risk banks facing, determining how these risks are mitigated by banks' AML/CFT program controls and relevant measure.

The results of a risk assessment can be used for a variety of reasons, including to:

- Identify gaps or opportunities for improvement in AML/CFT policies, procedures and processes;
- Make informed decisions about risk appetite and implementation of control efforts, allocation of resources, technology spend;
- Assist management in understanding how the structure of a business unit or business line's AML compliance program aligns with its risk profile;
- Develop risk mitigation strategies including applicable internal controls;
- Ensure senior management are made aware of the key risks, control gaps and remediation efforts;
- Assist senior management with strategic decisions in relation to commercial exits and disposals
- Ensure regulators are made aware of the key risks, control gaps and remediation efforts across the banks; and
- Assist management in ensuring that resources and priorities are aligned with identified ML/TF risks.

5. ML/TF Risk Assessment of the Business

In this context the risk is defined as ''a function of likelihood of occurrence of risk events and the impact of the risk events''. The likelihood of occurrence is a combination of threat and vulnerabilities, or in other words, risk events occur when a threat exploits vulnerabilities. Accordingly, the level of risks can be mitigated by reducing the size of the threats, vulnerabilities or their impact.

In order to establish the banks' exposure to ML/TF and the efficient management of that risk, the banks must to identify every segment of its business operations where a ML/TF threat may emerge and to assess their vulnerability to that threat. It is necessary that ML/TF risks are continuously identified at all management levels, from the operational level to the executive board, and to include all organizational units/departments of the banks. The size and complexity of the banks plays a crucial role in how attractive and vulnerable they are for ML/TF attempts. For example, a large organization is less likely to know a customer personally, who thereby can be more anonymous than a customer of a smaller one. An organization that

provides international services might be more attractive to money launderers than a domestic organization that offers limited products and services.

Business-wide risk assessments should help banks understand where they're exposed to ML/ TF risk and which areas of their business they should prioritize in the fight against ML/TF. To that end, institutions should identify and assess the ML/TF risk associated with the products and services they offer, the jurisdictions they operate in, the customers they attract and the transaction or delivery channels they use to service their customers. The steps banks take to identify and assess ML/TF risk across their business must be proportionate to the nature and size of each firm. Banks that do not offer complex products or services and that have limited or no international exposure may not need an overly complex or sophisticated risk assessment.

Upon identifying the ML/TF risks, the banks need to adequately assess those risks exposure by implementing effective risk management system, which would enable them to evaluate the likelihood of adverse effects arising from that risk and the potential impact of that risk on the realization of business objectives.

The banks should conduct the risk identification and analysis for all new and existing products, activities and processes. An effective process of ML/TF risk identification and analysis serves as basis for establishing an effective system of ML/TF risk management and controls and consequently for reaching the ultimate goal, minimizing possible adverse effects arising from those risks.

An assessment of ML/TF risks initiates from the assumption that the different products and services offered by banks as part of their day-to-day business operations or different transactions executed by them, are not equally vulnerable to be misused by criminals. The purpose of a risk assessment is to apply control measures proportionate to the identified Ml/TF risk. This allows banks to focus on the customers, countries, products, services, transactions and delivery channels that constitute the greatest potential inherent ML/TF risk.

The process of ML/TF risk assessment has four stages:

- Identifying the area of the business operations vulnerable to ML/TF;
- Conducting an analysis to assess the likelihood and impact of ML/TF;
- Managing the Ml/TF risks by developing policies, procedures and process; and

Regular monitoring and reviewing the ML/TF risks. The first stage of ML/TF risk assessment is to identify the varying threat and vulnerability to ML/TF which arises from customers, products, services, transactions and geographic exposures to the institution as they pertain to the specific characteristics of a particular delivery channel, customer, product, service, and transaction.

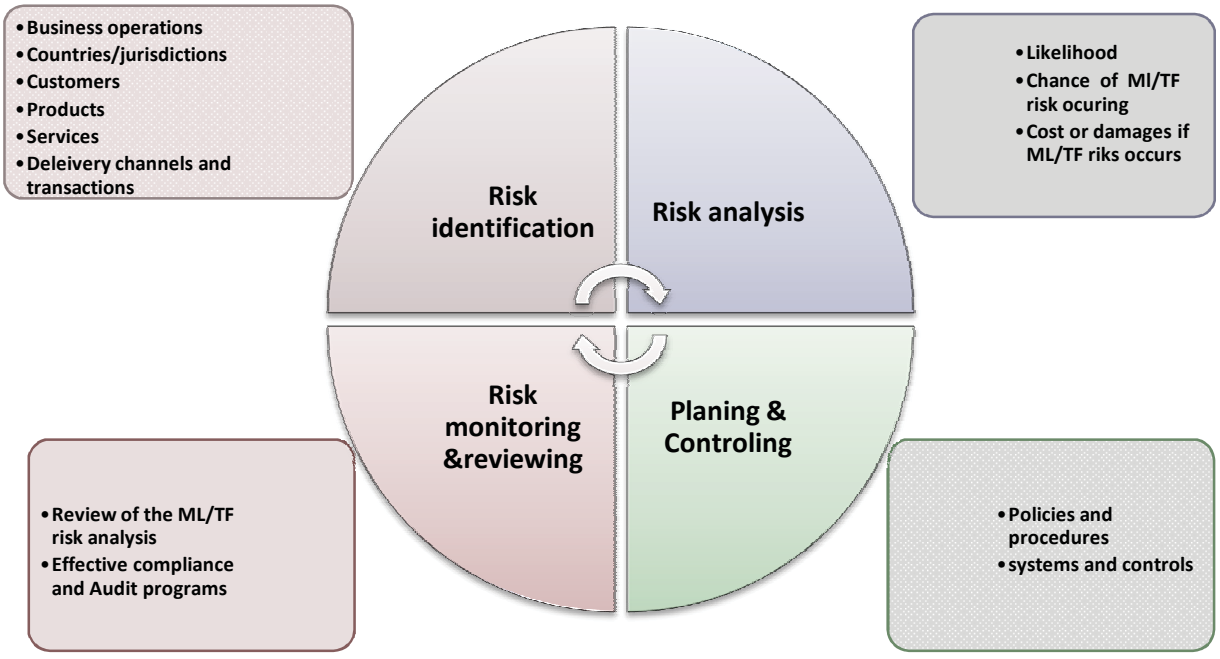
In the second stage, the money laundering and terrorist financing risks that can be encountered in a bank need to be analyzed as a combination of likelihood that the risks will be occurred and the impact of cost or damages if the risks occur. This impact can consist of financial loss to the

business from the crime, monetary penalties from regulatory authorities or the process of enhanced mitigation measures. It can also include reputational damages to the business or the bank itself. The analysis of certain risk categories and their combination is specific for each bank, so that the conclusion on the total level of inherent risk must be based on the relevant information available.

In the third stage, once the inherent risk is identified, assessed and analyzed, the banks should apply Ml/TF risk management strategies and implement policies and procedures accordingly. In addition to mitigate the inherent risk effectively, adequate system and controls should be devised and implemented.

Fourth stage, in this ML/TF risks policies, procedures have to be monitored and reviewed regularly. A bank can do this by developing a monitoring regime through its compliance and audit programs. The assessment of ML/TF risks must be revised periodically, based on the extent of changes in ML/TF risks or the bank's operations or strategic changes**.**

5.1. The ML/TF risk assessment life cycle is depicted in the following diagram:



In view of the fact that the nature of the terrorism financing differs from that of money laundering, the risk assessment must cover an analysis of the vulnerabilities of terrorism financing too. Since the funds used for terrorism financing may originate from legal sources, the nature of the sources may vary depending the given factors. When the source of terrorism financing originate from criminal activities, the risk assessment related to money laundering is also applicable to terrorism financing.

Many of the CFT measures banks have in place will overlap with their AML measures. These may cover, for example, risk assessment, CDD checks, transaction monitoring, escalation of suspicions and liaison relationships with the authorities. The guidance provided in these guideline, therefore, applies to CFT as it does to AML, even where this is not explicitly mentioned.

6. ML/TF Risk Identification and Analysis

In the ML/TF risk assessment process, the first step is to identify certain risk categories, i.e., customers, countries or geographical locations, products, services, transactions and delivery channels specific for the bank. Depending on the specificity of operations of a bank, other categories could be considered to identify all segments in which ML/TF risk may emerge. The significance of different risk categories may vary from bank to bank, i.e., a bank may decide that some risk categories are more important to it than others.

Banks should find out which ML/TF risks they are, or would be, exposed to as a result of entering into a business relationship or carrying out an occasional transaction.

In identifying ML/TF risks associated with a business relationship or occasional transaction, its important banks consider relevant risk factors including who their customer is, the countries or geographical areas they operate in, the particular products, services and transactions the customer requires and the channels the firm uses to deliver these products, services, and transactions.

Where possible, information about these ML/TF risk factors should come from multiple sources, whether these are accessed individually or through commercially available tools or databases that pool information from several sources. RFI's should determine the type and numbers of sources on a risk-sensitive basis.

For the analysis, the bank should identify the likelihood that these types or categories of costumers will likely misuse the banks for money laundering and terrorism financing purposes. This likelihood is for instance high if it can occur several times in a year, medium if it can occur once in a year and low if it is unlikely, but not impossible. In assessing the impact, the banks can for instance look at the financial damage from the crime itself or from regulatory sanctions or reputational damages to the banks. These impacts can vary from minor if there are only short term or low cost consequences to (very) major when there are high cost and long term consequences that affect the proper functioning of the bank.

The table below indicates a three-point scale. The banks can decide on a more detailed scale for this purpose.

Rating	Likelihood
High	Probably occurs several times per year
Medium	Probably occurs once per year
Low	Unlikely to occur but not impossible

Rating	*Impact*

Major Impact	Long term, high cost consequences affecting functioning
Moderate Impact	Medium term consequences with some costs
Minor Impact	Short term or low cost consequences

6.1. Customer Risk

In order to conduct ML/TF risk assessment, the banks should define if a type of customer carries a high ML/TF risk. Based on their own criteria, banks will determine whether a customer poses higher ML/TF risk.

Some category of customers that indicate a higher risk with respect to ML/TF that should trigger higher level of KYC, CDD and EDD are:

- PEPs;
- FXDs and MSPs;
- NGOs;
- Lawyers;
- Other customer as enunciated in the AML/CFT Responsibilities and Preventative Measures Regulations; and
- Customers who are on FinTRACA watch list;

The bank will describe all types or categories of customers that it provides business to and should make an estimate of the likelihood that these types or categories of customers will misuse the bank for money laundering or terrorism financing, and the consequent impact if indeed that occurs.

Example on few types of customers

Small and Medium Enterprises:

The small and medium business enterprise customers usually are domestic companies with simple ownership structures. Most of these businesses deal with cash and multiple persons can be acting on their behalf. The likelihood that funds deposited are from illegitimate source is

medium. Because of the large number of SME customers the impact can be major. The risk assessment is high.

International Corporations:

Customers that are international corporations have complex ownership structures with often foreign beneficial ownership. Although there are only few of those customers, most are located in offshore locations. The likelihood of ML is high, but because of the limited number of customer the impact will be moderate. The risk assessment is Medium.

These descriptions can result in a table as below:
Example

Type of customer	Likelihood	Impact	Risk analysis
Domestic and retail customer,	Medium	Moderate	Medium
Private banking customer	High	Major	High
Small business	Medium	Moderate	Midium
International corporation	High	Moderate	Medium
FXDs and MSPs	High	Major	High
PEP	High	High	High
Occasional customer	High	Medium	Medium
Company listed on stock exchange	Low	Minor	low

The above risk analysis is a general one for types or categories of customers. It is the starting point for the risk classification of an individual customer. Based on the circumstances of an individual customer, such as its background or information provided, the risk classification of an individual customer can be adjusted. Based on that individual risk classification, customer due diligence measures should be applied.

6.2. ML/TF Risk of Transaction, Product and Service

A comprehensive ML/TF risk assessment must take into account the potential risks arising from the transactions, products and services that the bank offers to its customers and the way these products and services are delivered to the customer. The bank should pay attention to ML/TF risk which may arise from the application of new technologies in the process of offering the banking products and services to its customers. In identifying the risks of transactions, products, and services, the following factors can be taken into accounts:

- Services identified by internationally recognized and credible sources as being a higher-risk, such as international correspondent banking services and (international) private banking activities;
- Services involving banknotes and precious metal trading and delivery;
- Services that inherently promote anonymity or can readily cross international borders, such as online banking services, prepaid cards, private investment companies and trusts;
- New or innovative products or services that are not provided directly by the bank, but are provided through channels of the bank;
- Products that involve large payment or receipt in cash;
- Purchase of valuable assets or commodities (real estate, race horses, vehicles, gems, precious metals, etc.);
- Gaming activities (horse racing, internet gambling, etc.);
- Non face-to-face transactions or services; and
- One-off transactions.

Moreover, specific lease products, consumer loans or savings products have a low inherent risk because of the long term to realize benefits. Other products, such as back-to-back loans, trade finance, real estate transactions and other high-quality and complex products may produce a higher risk because of their complexity or lack of transparency.
For the risk assessment, the bank should describe all products and services that it provides and make an estimate of the likelihood that customers will misuse that product for money laundering or financing of terrorism, and the impact thereof.

Example

Description of types of products, transactions and services

Life insurance:

The life insurance products are simple and premiums tend to be very low. Premiums can only be paid through a bank account and no cash is involved. The life insurance products are only sold to resident persons. The likelihood that insurance products are used for ML/TF is low as will be the impact if it is. Risk assessment is low.

Prepaid cards:

Prepaid cards are a new product and its usage is not clear yet. Funds tend to be loaded through cash deposits and sometimes it is not necessary for the customers to have a bank account. The likelihood that prepaid cards are used for ML/TF is high and since it is a new product, will make its ML/TF risk high. Prepaid cards by nature are issued for business travel purpose. There is a possibility that these cards are used as Debit Cards for cash withdrawals, in merchant establishments, for other personal expenses. Also the transactions or the cards being used in high risk jurisdictions.

The description can be shown in a table as below:

Example

Type of transaction	Likelihood	Impact	Risk analysis
Betting transaction	High	Moderate	High
Online Transaction	High	Major	High
Domestic bank transfer	Medium	Moderate	Medium
Prepaid card	High	Major	High
Life insurance	Low	High	Low
Security account	Low	Medium	Low

6.3. Delivery Channels Risk

Delivery channels risk are the risks that arise from the channels used to deliver and provide products and services to a bank customer. The delivery channels play a crucial role when assessing the ML/TF risk. The extent to which the bank work with customers directly or through intermediaries or correspondent institutions, or establishes business relationships without customers being physically present are important factors to be taken into account in assessing the risk by considering the risk associated with delivery channels.

6.4. Country or Geographical Risk

In the process of ML/TF risk assessment, the country or geographical risk may arise because of the location of a customer, the origin of destination of transactions of the customer, business activities of the banks and their geographical location ". Country or geographical risk, combined with other risk categories, provides useful information on potential exposure ML/TF.

There exist no general definition on the basis of which countries or geographical areas can be categorized as low, medium or high risk. The factors which may define if a specific country or geographical area is more vulnerable to money laundering and terrorism financing, may include different criteria depending on a particular circumstances.

The main factors that may show a high risk are as follow:

- Countries or geographic areas subject to sanctions, embargoes, or comparable restricted measures issued, for instance, by United Nations, The European Union or the OFAC;
- Countries and geographical area identified by credible sources (e.g., the FATF, the IMF or the World Bank) as lacking AML/CFT system. reference is made to the ICRG process' (International Co-operation Review Group) of FATF publishes list of the countries which in its opinion lack an effective system of combating money laundering and terrorism financing;
- Countries and geographical area identified by credible sources as providing funding for or otherwise supporting terrorist activities; and
- Countries and geographical area identified by credible sources as having a level of corruptions, or criminal activities etc.

7. Risk Matrix

In order to assess the risk of money laundering and terrorism financing, the banks are to establish whether all identified categories of risks pose a low, medium, high or unacceptable risk to the business operations. The banks must review different factors, e.g., number and scope of transactions, geographical location and nature of the business relationship. In doing so, the banks must also review the differences in the manner in which the bank establishes and maintains a business relationship with a customer (e.g., direct contact or non face-to-face). It is due to the combination of these factors and the variety of their combinations, that the level of money laundering and terrorism financing differs from bank to bank. The geographical risk should be seen in correlation with other risk factors in order to come up with an assessment of the total money laundering and terrorism financing risk. Thus, for example, a low risk product in combination with a customer from a high risk country will combined carry a higher ML/TF risk. Banks can use a risk matrix as a method of assessing risk in order to identify the types or categories of customers that are in the low-risk category, those that carry somewhat higher risk, but still acceptable risk, and those that carry a high or unacceptable ML/TF risk. In classifying the risk, the bank, taking into account its specificities, may also define additional levels of ML/TF risk. The development of a risk matrix can include the consideration of a wide range of risk categories, such as the products and services offered by the bank, the customers to whom the products and services are offered, the banks size and organizational structure, etc. A risk matrix is not static: it changes as the circumstances of the bank change.

A risk analysis will assist a bank to understand the fact that ML/TF risks may vary across customers, products, and geographic areas and thereby focus its efforts and resources on high ML/TF risk areas in its business/operations.

Below is an example of a risk matrix, but banks should develop their own risk matrix based on their own risk analysis results.

Example only

Customer Transaction	International wire transfer	Online transaction	Domestic transfer	Prepaid card	Life insurance	Securities account
Domestic retail customer	High	Medium	Medium	Medium	Low	low
Private banking customer	High	High	Medium	High	Medium	Medium
SME business customer	Medium	High	Medium	high	Medium	Medium
International corporation	High	High	Medium	High	Medium	Medium
PEP	High	High	low	High	Medium	Medium
Occasional transactions	high	High	Medium	High	Medium	Medium

The banks must ensure that the risk identification and analysis is properly documented in order to be able to demonstrate it as the basis of the AML/CFT policies and procedures, and to be able to provide the risk assessment information to the supervisory authorities.

8. ML/TF Risk Management

Each bank's ML/TF risk is specific and requires an adequate risk management approach and methods corresponding to the level and structure of the risk and to the size and complexity of the bank. The objectives and principles of ML/TF risk management should enable banks to establish a business strategy, risk appetite, risk tolerance, adequate policies and procedures, promote high ethical and professional standards and prevent their selves from being misused, intentionally or unintentionally for criminal activities.

To manage the ML/TF risk effectively requires attention and participation of several business units with different competences and responsibilities. It is important for each departments/business unit to precisely know its role, level of authority and responsibility within the bank's organizational structure and within the structure of ML/TF risk management.

It would be desirable for managers of different lines of business, responsible for risk management at the level of their organizational unit, to develop ML/TF risk management procedures, corresponding to the specific tasks of the organizational unit in question, which must be harmonized with the objectives and principles of ML/TF risk at the level of the bank as a whole.

8.1. Roles and Responsibilities of Board

Board of supervisors should give direction to its business activities by setting the risk appetite, formulating objectives and making strategic choices from which subsequently policy and procedures are derived and developed. Management should be able to determine the ML/TF risks of the business and take these into consideration in the bank's ultimate goals and strategies. Documentation and communication of strategy, policies and procedures are important for their actual implementation. Tools in this respect are, for instance, mission statements, business principles or strategic views. Management will also give direction to setting up, implementing and monitoring the ML/TF control framework and will be responsible for the strategic choices to be made and decisions to be taken in that respect.
Management should be actively involved in analyzing and recognizing ML/TF risks and take adequate control measures (e.g., by allocating sufficient resources to setting up an adequate monitoring system or training programs and workshops). Management will thereby receive support from functions (compliance, security, risk management, commercial functions, etc.) that possess relevant knowledge and experience. Management should also determine the risk tolerance while guarding against the bank accepting customers or providing products and services on whom or which the bank has no knowledge or experience. It should ensure that sufficient account is taken of ML/TF risks in the development and pre-introduction phase of new products and services. It is important in this respect that members of the management team involved in the decision-making process have sufficient authority and powers to take and implement the necessary decisions (or have these implemented).

Banks' Management's leadership abilities in performing its responsibilities effectively and commitment to the prevention of money laundering and terrorism financing are very crucial aspects of implementing the risk-based approach to AML/CFT. Management must encourage regulatory compliance and ensure that employees abide by internal procedures, policies, practices and processes aimed at M/TF risk mitigation, management and control. Management should also promote an ethical business culture and ethical behavior. Ethical behavior is a professional, individual responsibility, where individuals should be aware of the rights, interests and wishes of other stakeholders and conscientiously take them into account, have an open and transparent mind-set, and be willing to take responsibility and be held accountable for their decisions and actions. An ethical business culture indicates a climate and atmosphere in which an bank, also in a broader sense, behaves or acts in a way it can explain and account for. A culture in which this professional, individual responsibility is stimulated and rewarded, and which not only respects the letter of the law, but also its spirit. The elements underpinning this

culture are: balancing of interests, balanced and consistent actions, openness to discussion, leading by example, enforcement and transparency.

8.2. AML/CFT Policies and Procedures

Once the processes of identification and risk analysis of inherent ML/TF risk are completed the strategy of ML/TF risk management is applied to enable the bank to implement adequate policies and procedures for reducing the inherent risks and bringing it down to an acceptable level, with a view to avoiding reputational risks, operational risks, risks of sanctions imposed by a regulatory body and other forms of risk.

The policies and procedures are approved by management and are applicable to all business units/branches . They should allow for sharing of information between branches with adequate safeguards on confidentiality and use of information exchanged. By assessing the risks and developing policies and procedures the bank ensures the continuity of ML/TF risk management controls despite any changes in the management or staff composition or structure.

The policies and procedures should enable the bank to effectively manage and mitigate the identified risks (inherent risk) by the right control measures and focus its efforts on areas in its business which are more vulnerable to ML/TF misuse. The higher the risk, the more control measures have to be applied. A bank can implement adequate ML/TF risk controls for higher risk products by setting transaction limits and/or a management approval escalation process. Also, the development and application of risk categories for customers together with customer due diligence and transaction monitoring measures based on those risk categories is one of the strategies for managing potential ML/TF risks posed by customers. Specific policies and procedures will therefore need to be developed with respect to customer due diligence, transaction monitoring, recordkeeping and reporting to FinTRACA.

9. ML/TF Risk Monitoring and Review

Banks' Management should be able to adequately manage ML/TF risks to verify the level of implementation and functioning of the ML/TF risk controls and to ascertain that the ML/TF risk management measures correspond to the bank’s risk analysis. The bank should therefore establish an appropriate and continuing process to monitor and review the ML/TF risk. This process will be done by the business control function to ensure on a regular basis that all processes are implemented; the compliance function to periodically monitor if the policies are adhered to and systems are in place; and the audit function to assess if the AML/CFT policies and process are conform the law and are performed in an adequate way.

9.1. Monitoring Process

Banks' management should receive regular reports containing the results of the monitoring process, findings of internal controls, reports of organizational units/departments in charge of compliance and risk management, reports of internal auditing, reports of the person authorized for detecting, monitoring and reporting any suspicious transactions to FinTRACA, as well as the

findings contained in the supervisory authorities on-site examination reports on AML/CFT. Management should be provided with all important information which will enable it to verify the level AML/CFT controls, as well as possible consequences for the banks' business if controls are not functioning properly and effectively.

The ML/TF risk reports should indicate if appropriate control measures are established and adequate and fully implemented for the bank to protect itself from possible ML/TF misuse. The monitoring and review process should include the appraisal of ML/TF risk exposure for all customers, products and activities, and ensure the implementation of proper control systems, with a view to identifying and indicating problems before any negative consequences for the bank's business occur. This process may also alert the bank to any potential failures, for instance failure to include mandatory legislative components in the AML/CFT policies and procedures, insufficient or inappropriate customer due diligence, or level of risk awareness not aligned with potential exposure to ML/TF risks.

9.2. Review of the ML/TF Risk Assessment

The bank must keep the ML/TF risk assessment up to date by setting up and describing the process of periodically reviewing the risk assessment. The bank must therefore also stay up-to-date with ML/TF methods and trends, international developments in the area of AML/CFT, and domestic legislation. Such a review can also include an assessment of the risk management resources such as funding and staff allocation and may also identify any future needs relevant to the nature, size and complexity of the bank's business.

In addition, the review should also be conducted when the business strategy or risk appetite of a bank changes or when deficiencies in the effectiveness are detected. When the bank is to introduce a new product or activity, an ML/TF risk analysis of that product is to be conducted before offering that new product or services to existing or new customers.

10. Effective Date

This guideline will be applicable and effective once it is approved by the Supreme Council of Da Afghanistan Bank and published.