عزیزی بانک
Azizi Bank

Anti-Money Laundering/Counter Financing of Terrorism

&

Customer due Diligence Policy

December 2020

Version 2.0

عزیزی بانک
Azizi Bank

Contents

List of Acronyms

ML/TF	Money Laundering/ Terrorist Financing
AML/ CFT	Anti-Money Laundering/ Combating Financing of Terrorism
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
DAB	Da Afghanistan Bank
KYC	Know Your Customer
Fin TRACA	Financial Transactions & Report Analysis Center of Afghanistan
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
OFAC	Office of Foreign Asset Control
UNSC	United Nation Security Council
EU	European Union
PEP	Politically Exposed Person
GOA	Government of Afghanistan
DPRK	Democratic People's Republic Korea (North Korea)
LCTR	Large Cash Transaction Report
STR	Suspicious Transaction Report
SAR	Suspicious Activity Report
NGO	Non-governmental Organization or Non-Profit Organization
TIN	Taxpayer Identification Number
MOCI	Ministry of Commerce & Industry
JV	Joint Venture

NOC	**No Objection Certificate**
CEO	**Chief Executive Officer**
COO	**Chief Operation Officer**
Dy. CEO	**Deputy Chief Executive Officer**
LEA	**Law Enforcement Agency**
AGO	**Attorney General Office**
TT	**Telegraphic Transfer**
AML & PC Law	**Anti-Money Laundering and Proceeds of Crime Law**
FATCA	**Foreign Account Tax Compliance Act**

Anti-Money Laundering /Counter Financing of Terrorism and Customer Due Diligence Policy

1. Background

In compliance with Afghanistan anti-money laundering & proceeds of crime laws, Afghanistan counter financing of terrorism laws, Afghanistan AML/ CFT responsibility & preventative measures regulation & counter financing of terrorism regulation, Azizi bank has adopted a comprehensive approach to manage the risk of money laundering/terrorist financing and has developed an AML/ CFT/ CDD framework articulated in this policy document.

These legislations require banks to develop effective frameworks, preventive measures, systems, controls, and practices to manage their potential money laundering/terrorist financing (ML/TF) risks. It has been emphasized that financial institutions licensed to operate in Afghanistan have adequate controls and procedures in place so that they know the customers with whom they are establishing business relationships and dealings.

The policy provides governing principles for managing the AML/CFT/KYC framework, and shall be further supported with relevant procedures and methodologies for identification, assessment, control and monitoring of such risks keeping in view the Bank's business and regulator specific compliance requirements.

The policy aims at managing money laundering and terrorist financing risks and also oversees its implementation besides ensuring that issues arising out of these activities are resolved effectively and expeditiously.

2. Introduction

This policy has been developed in the basis of the provisions of Afghanistan banking law, Afghanistan AML/ CFT laws & regulations, specially, in light of article 5.2 of Afghanistan AML/ CFT regulation, in order to;

- Meet the requirements of concerning laws/ regulation,
- Protect bank & its system from being used by money launderer & terrorist financer &
- Safeguard the integrity of the country's financial system.

This policy at the macro level is an embodiment of the bank's approach to understand, identify, measure, mitigate & manage the risk of money laundering and terrorist financing. It aims at ensuring the availability of adequate procedures that are required to fight money laundering & terrorist financing.

3. Definition of Money Laundering & Terrorist Financing

3.1. Money Laundering:

Money Laundering is the process by which criminals attempt to disguise the true origin of the proceeds of their criminal activities by the use of the financial system so that after a series of transactions, the money, its ownership and the income earned from it appear to be legitimate. According to FATF, money laundering is the processing of criminal proceeds in order to disguise their illegal origin. This process is often achieved by converting the original illegally obtained proceeds from their original form, usually cash, into other forms such as deposits or securities and by transferring them from one financial institution to another using the account of apparently different persons or businesses.

Generally, the money laundering process consists of three "stages":

Placement: The introduction of illegally obtained monies or other valuables into financial or non-financial institutions.

Layering: Separating the proceeds of criminal activity from their source through the use of layers of complex financial transactions. These layers are designed to hamper the audit trail, disguise the origin of funds and provide anonymity.

Integration: Placing the laundered proceeds back into the economy in such a way that they re-enter the financial system as apparently legitimate funds.

These "stages" are not static and overlap broadly. Financial institutions may be misused at any point in the money laundering process.

The terms used in above definitions are defined as follow:

a) "Proceeds of crime" means any funds or property derived from or obtained directly or indirectly through the commission of a predicate offence. This also includes income or benefits derived from such proceeds, proceeds obtained from the investment of such funds or the funds or property that have been transferred into other types of assets, whether partially or in whole.

b) "funds or property" means assets of every kind, whether material or immaterial, corporeal or incorporeal, movable or immovable, tangible or intangible, however, acquired, and legal documents or instruments, including electronic or digital, evidencing title to, or interest in, such assets including but not limited to money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets;

3.1. Terrorist financing

Terrorist financing is the financing of terrorist acts, and of terrorists and terrorist organizations. The term terrorist refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully; (ii) participates as an accomplice in terrorist acts ; (iii) organizes or directs others to commit terrorist acts ; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the

contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

4. Anti-Money Laundering and Combating Terrorist Financing

Bank is required to establish effective customer due diligence program that is based on the requirement of local laws & regulations as well as international standards & best practices, to prevent money laundering and terrorist financing.

Bank should know the true identity of their customers, detect and examine suspicious transactions, and report any such suspicions to the Fin TRACA-Afghanistan/ FIU. It shall establish its customer due diligence (KYC) procedures & minimum criteria in their CDD program that is to be observed in its customer relationships applying the risk-based approach to be able to demonstrate to the supervisor how it assesses the risks of money laundering related to its customer relationships and activities, and how it identifies its customers and knows and monitors their transactions and use of services.

4.1. Necessary Steps in AML & CFT

a) Detect

1. Out of pattern transaction Monitoring
2. Identification of suspicious transactions / Customers
3. Reporting of suspicious transactions to Compliance Department & Compliance Department further reporting it to FIU/FINTRACA
4. Screening of customer accounts at the time of opening new account/data of existing accounts and transactions with list of prescribed entities/individuals under the top 4 and powerful sanctioned lists - UNSC resolutions, OFAC, EU Financial Sanctions, HM Treasury & Fin TRACA watch-list.

b) Deter

1. Exercising Due Diligence for opening new accounts and dealing with existing customers
2. Understanding KYC policy

3. DAB Laws & Regulations and internal Policies on AML /CFT
4. Guidelines for account opening
5. Appointment of Compliance Officers
6. Periodic updating of customer's information (KYC Renewal)
7. Regular review of daily transactions
8. Refuse bank services/active assistance in transactions which in the opinion of the bank are suspected to be associated with money derived from illegal activities.

c) Prosecute

Money laundering offences are prosecuted by government through establishment of Financial Intelligence Unit (FIU) in the DAB with active assistance of government agencies like (Attorney General (Saranwali), National Directorate Security / Riasat Amniat Milli etc.).

5. AML/ CFT Legal and Regulatory Framework in Afghanistan

The existence of legal and regulatory framework to combat money laundering and terrorist financing is the crucial and an integral element of a sound anti money laundering and terrorist financing regime. Financial Action Task Force recommends that countries should criminalize money laundering and terrorist financing with a view to include the widest range of predicate offenses.

Afghanistan AML/ CFT legal and regulatory framework has enabled financial institutions and designated non-financial business and professions inside the country to develop their policies and procedures in fighting money laundering and terrorist financing.

Da Afghanistan Bank is the primary financial regulator/ financial supervisory authority in the country which was established in 1318 in the capital (Kabul) operating under the law of Da Afghanistan Bank.

The basic responsibilities of Da Afghanistan bank are to;

- Formulate, adopt and execute the monetary policy of Afghanistan,
- Formulate, adopt and implement currency policy and Afghanistan currency arrangements,

- Hold and manage the official foreign exchange reserves of Afghanistan,
- Print, mint and issue Afghani banknotes and coins,
- Act as banker and adviser to, and as fiscal agent of the State,
- License, regulate and supervise banks, foreign exchange dealers, money service providers, payment system operators, securities service providers, and securities transfer system operators,
- Establish, maintain and promote sound and efficient systems for payments, for transfers of securities issued by the State or DAB, and for the clearing and settlement of payment transactions and transactions in such securities.

Azizi bank's AML/ CFT & CDD policy has been developed on the basis the following laws & regulations, & is subject to the review and supervision of the regulator.

1. Anti-Money Laundering and Proceeds of Crime law
2. Counter Financing of Terrorism law.
1. Counter Financing of Terrorism Regulation
2. AML/CFT Responsibilities and Preventative Measures Regulation
3. Fit and Proper Regulation
4. Corporate governance Regulation

5. Objectives, Scope and Application of the Policy

The primary objective of the Policy is to prevent our branch network from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. The policy is proposed to serve the following purposes:

i. To prevent criminal elements from using our branches for money laundering activities
ii. To enable the branches to know/ understand the customers and their financial dealings better which, in turn, would help to manage risks prudently
iii. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.
iv. To comply with applicable laws and regulatory guidelines.
v. To ensure that the concerned staff are adequately trained in KYC/AML/CFT procedures.

vi. To prevent the Bank from being exposed to reputational damage and financial loss in relation to non-compliance with applicable AML-CFT standards.

vii. To detect, deter and prevent money laundering, associated predicate offences and terrorism financing

viii. To protect the integrity of the Bank from illegal activities and illicit fund flows.

ix. To ensure effective monitoring of the measures implemented and decisive actions against ML/TF threats.

This Policy shall be applicable to all the branches/offices of the Bank and shall be read in conjunction with related operational guidelines issued from time to time.

6. Responsibilities of Top Management

The Top Management of the Bank shall be ultimately responsible for ensuring compliance with applicable statutes, regulations, internal policies and guidelines and ethical standards. In case of cross-border businesses the Top Management shall be responsible for ensuring compliance with applicable laws and regulations prevailing in various jurisdictions where the business is undertaken. The Top Management of the Bank shall be responsible for implementation of the Bank's AML/ CFT Policies, procedures and its associated requirements. They shall also be responsible for the adequacy of processes, systems, policies and procedures that would create an appropriate environment for managing AML/ CFT & compliance risks.

a. The bank's Board of Management is responsible for establishing AML/ CFT & compliance policies that contains the basic principles to be approved by the Board of Supervisors and explains the main processes by which AML/ CFT & compliance risks are to be identified and managed through all levels of the organization.

b. The compliance department should advise the Board of Supervisors and Board of Management on the bank's compliance with applicable laws, rules and standards and keep them informed of developments in the area. It should also help educate staff about compliance issues, act as a contact point within the bank for compliance queries from staff members, and provide guidance to staff on the appropriate implementation of applicable laws, rules and standards in the form of

policies and procedures and other documents such as compliance manuals, internal codes of conduct and practice guidelines.

c. To be effective, the compliance department must have sufficient authority, stature, independence, resources and access to the Board of Supervisors. Board of Management should respect the independent duties of the compliance function and not interfere with their fulfillment.

7. Responsibilities of Chief Compliance Officer

The Chief Compliance Officer of the Bank shall be appointed with the recommendation of the Board of supervisors and prior approval of the regulator i.e. the DAB. He shall be a senior executive.

The Chief Compliance Officer shall report to the board of supervisors and shall be responsible for ensuring effective implementation of the AML/ CFT & Compliance Policies and procedures, and other compliance initiatives, coordinating the identification and management of the Bank's AML/ CFT & compliance risks and supervising the activities of other Compliance staff.

The Chief Compliance Officer shall assist the Bank's Top Management in managing effectively the AML/ CFT & compliance risks faced by the Bank and would be responsible for providing clarifications on issues or concerns relating to the Bank's AML/ CFT & compliance policies, guiding the compliance staff in performance of risk assessments and reviewing the results of the AML/ CFT risk assessments, compliance risk reviews and compliance monitoring and testing programs.

The Chief Compliance Officer shall be responsible for developing and maintaining the AML/ CFT & compliance Policies including the approval/reporting of exceptions thereto, maintaining oversight of the activities of the Compliance department of Bank and implementation of the AML/ CFT & compliance policy and compliance risk management framework across the Bank.

Further, the Chief Compliance Officer shall be responsible for maintaining a relationship with the regulators supervising the Bank and act as the key interface between the Top Management of the Bank and the regulators.

Furthermore; The Chief Compliance Officer shall participate in the discussion between the Bank and the DAB if any.

8. Responsibilities of Compliance Department

The Compliance department shall work with the Business Units, Internal Audit, and Legal department to ensure that compliance activities are aligned with business objectives. It would provide an independent and objective perspective on emerging compliance issues. The Compliance staff will have a reporting relationship to the Chief Compliance Officer and would be responsible for implementing the compliance framework across the Bank.

The responsibilities of the Compliance department shall be to vet/disseminate regulatory guidelines/instructions to business units, provide guidance in the implementation of the AML/ CFT & compliance policies and compliance framework to the compliance staff and respond to AML/ CFT & compliance related requests/queries of employees.

The Compliance department shall also be responsible for developing and maintaining the compliance calendar for all regulatory reporting, disseminating the same to the relevant Business Units, monitoring the implementation of the findings from AML/ CFT & compliance risks reviews or regulatory inspections, providing guidance to the Business Units on corrective action to be taken for identified AML/ CFT CDD & compliance breaches/incidents, and tracking the breaches/incidents and their appropriate resolution.

The Compliance department shall identify compliance failures in the bank using the internal audit and concurrent audit as a feedback mechanism. Synopsis of all audit reports will be marked to Chief Compliance Officer. It will go through the synopsis of all audit/inspection reports and rectification reports regularly to enable it to identify compliance failures in the bank.

The Compliance department shall monitor and test compliance by performing sufficient and representative compliance testing and report the results thereof to the Senior management.

9. Policies and procedures

The Bank shall have and effectively implement internal policies, procedures, systems, controls and customer acceptance policy that clearly indicates situations when a customer will be rejected.

This policy is inter alia intended to address the following:

I. Risk evaluation of the customer, products, services, geographic locations, and delivery channels as well as transactions.
II. Identification and verification of the customer and beneficial owner including walk-in/occasional customers, and politically exposed person(s).
III. Application of customer due diligence measures
IV. Maintaining records and information obtained in the CDD process and information of transactions.
V. Monitoring of transactions, including monitoring to identify unusual or suspicious transactions.
VI. Reporting to FINTRACA of threshold transactions.
VII. Reporting to FINTRACA of suspicious transactions.
VIII. Ensuring that internal policies, procedures, systems and controls are subject to independent testing and review.
IX. The appointment of a Chief Compliance Officer at Senior Management level to ensure compliance with the provisions of the Anti-Money Laundering and Proceeds of Crime Law and the DAB's Regulation thereon.
X. Ensuring high standards as set out in fit and proper requirements while recruiting employees. This shall include separate fit and proper requirements for employees in management positions or in positions perceived to have greater exposure to money laundering or terrorist financing.
XI. Establishing training programs and providing on-going trainings to all new and existing employees, directors, board members, executive or supervisory management.

XII. Other arrangements as prescribed by the DAB and/or FINTRACA.

The Bank shall ensure that all of its internal policies, procedures, systems and controls remain consistent with the risks and complexity of operations and are adopted by the bank's Board of Supervisors and shall be applicable to all domestic and foreign branches if any.

The Bank shall designate one individual as "Chief Compliance Officer" having primary responsibility for development and implementation of the anti-money laundering measures contained in the DAB regulation. Another individual shall be designated as "Chief Internal Auditor" having responsibility for auditing the implementation by the Chief Compliance Officer of the policies and procedures developed. In particular, the system of internal controls shall ensure that the necessary reports are filed with the FINTRACA. The audit function shall report directly to the Audit Committee/Board of Supervisors and its reports shall include examples, if any, of the Chief Compliance Officer's failure to implement these measures.

10. Customer Acceptance/ Rejection

10.1. Acceptance

Bank shall accept only those clients whose identity is established by conducting due diligence/ enhanced due diligence appropriate to the risk profile of the client as set out in other part (s) of this policy.

The bank is prohibited from establishing relationship with the customers given in the sub-point# 2 of this point#10.

10.2. Rejection

The bank has defined several types of customers who have unacceptably high risk and has decided to preclude such customers from establishing a business relationship.

10.2.1. List of customers (natural and/ or legal) not accepted by bank

1. Client who refrain from providing information about their identity, source of income, purpose of the account opening & other necessary information or any part of it as per the KYC forms
2. Client who cannot provide mandatory/ required KYC documents as per the account opening checklist considering type of the Client
3. Client who has been recognized by bank having background of fraud, forgery & other such activities that are against bank's policies
4. Client with negative media from reliable source
5. Client engaged in illegal activities (such as human trafficking, drug dealing, fraud, bribery etc.)
6. Client convicted for a crime included in the predicate offences
7. Organization undertaking military missions, i.e. mercenary missions
8. Online casino or an online pharmacy
9. Client dealing with dating or adult entertainment
10. Issuer or dealer of virtual currency (e.g. Bitcoin) or involved in converting traditional currency in virtual currency or vice versa or provides related services (software providers, payment processing services, card acquirers)
11. Client who fails to provide adequate identification information or disclose its economic operations
12. Shell banks & companies or bank which deals with shell banks or a shell company
13. Client who requests/ insists to have accounts in the name of anonymous or fictitious persons or accounts (including secret accounts and numbered accounts) or accounts that do not bear the complete name of the beneficiary as shown in the identification documents of the Client.
14. Client from a political regime not recognized by the United Nations
15. Client who is subject to specific sanctions (i.e. EU, UN, OFAC, HM Treasury, Fin TRACA watch list), including close family members and close associates
16. An Online Gaming company
17. An entity operating in the production and/or wholesale trading of nuclear related raw materials, products and services.
18. A non-profit organization / charity or foundation for charity purposes, which is not registered/ licensed.

19. An organization providing armed security services, without license & or permission of ministry of interior affairs.
20. Entities operating in the defense/arms/military industry which are not licensed by competent GOA ministry.
21. A legal entity with a complex structure, where there is no transparent and legitimate economic reason for its complexity.
22. Off-shore Companies
23. Additionally, the following transactions are also not accepted:
    a. The execution of transactions related to close family members, close associates or related entities (irrespective of % of ownership) of sanctioned entities/ individuals.
    b. Issuing of Master card for Iranians & North Koreans (DPRK)

11. ML/TF Risk Assessment

The Bank shall assess and understand its money laundering and terrorism financing risks, including of new products or technologies. The risk assessment and any underlying analysis and information shall be documented in writing be kept updated and readily available for Da Afghanistan Bank to review at their request.

The Bank shall document the risk assessments in order to be able to demonstrate their basis, keep the assessments updated, and make the documents of the processes and the risk assessment documentations available to Da Afghanistan Bank upon request.

11.1. 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.

Likelihood (threat and vulnerability) that a risk occurs	×	Impact (losses, damages) when a risk occurs	=	Risk level

In order to establish the banks' exposure to ML/TF and the efficient management of the risk, the banks need 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 constantly identified at all management levels, from the operational level to the executive board, and to include all organizational units of the banks. The size and complexity of the banks plays a crucial role in how attractive and susceptible the banks are for ML/TF. For example, a large organization is less likely to know a customer personally who hereby can be more anonymous than a customer of a small organization. And an organization that provides international services might be more attractive to money launderers than a domestic organization.

Upon identifying the risks, the banks need to adequately assess the ML/TF risk exposure, 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 bank 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 adequate system of risk management and control and consequently, for reaching the ultimate goal, minimizing possible adverse effects arising from that risk.

An assessment of ML/TF risks proceeds from the assumption that the different products and services offered by banks in 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 risk. This allows the bank to focus on the customers, countries, products, services, transactions and delivery channels that constitute the greatest potential risk.

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

I. Identifying the area of the business operations susceptible to ML/TF;
II. Conducting an analysis in order to assess the likelihood and impact of ML/TF;
III. Managing the risks; and
IV. Regular monitoring and reviewing the risks.

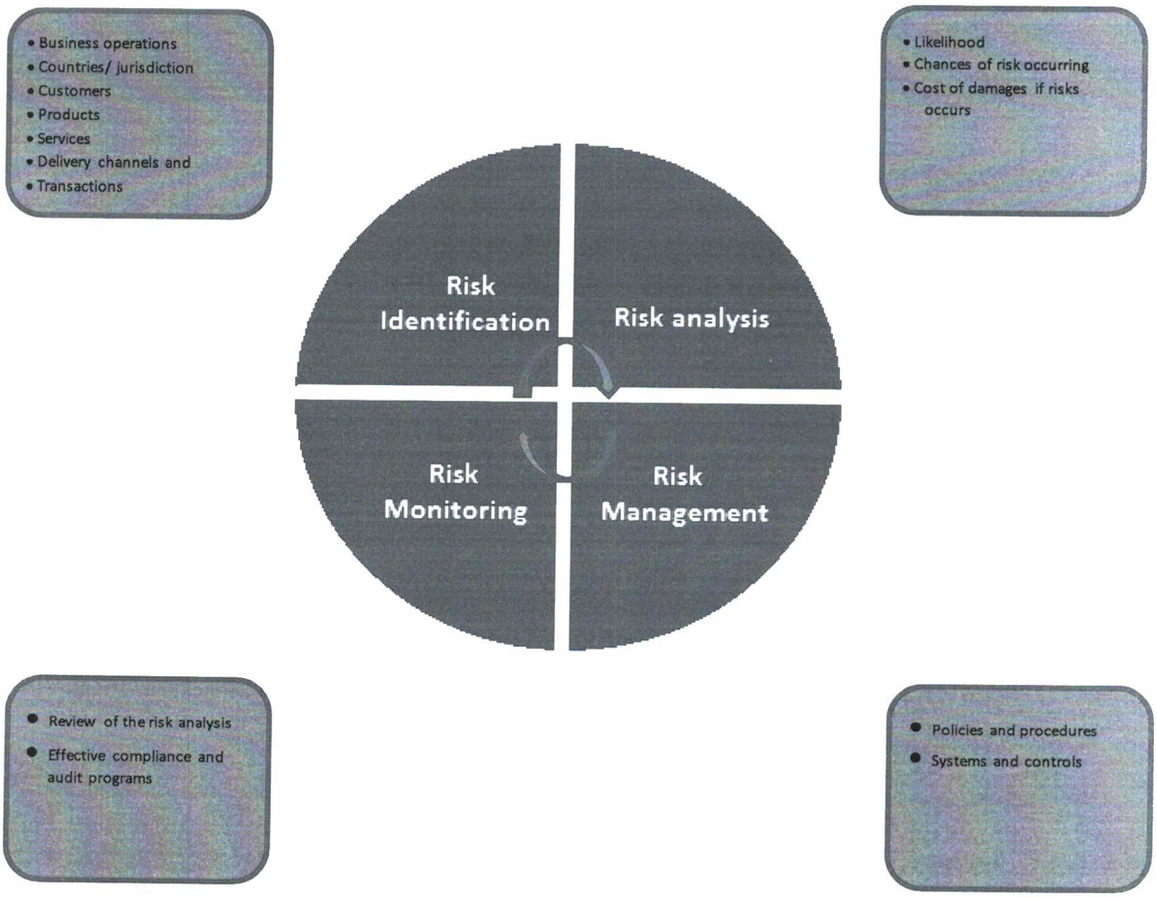
The first stage of ML/TF risk assessment is to identify customers, products, services, transactions and geographical location specific for the bank. Depending upon the specific characteristics of a delivery channel for particular customers, product, services and the transactions, the vulnerability to ML/TF risk.

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 of risks 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. 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 risk level must be based on the relevant information available.

In the third stage, the bank will, based on the analysis, apply risk management strategies and implement policies and procedures accordingly. To mitigate the risk effectively, adequate system and controls should be implemented.

Fourth stage, in the process the risks and the management of the risks 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, basis the extent of changes in risks or the bank's operations or strategic changes.

11.1.1. Method of ML/TF Risk Assessment



In view of the fact that the nature of the terrorism financing differs from that of money laundering, the risk assessment must include also an analysis of the vulnerabilities of terrorism financing. Since the funds used for terrorism financing may emanate from legal sources, the nature of the sources may vary. when the source of the terrorism financing originates from criminal activities, the risk assessment related to money laundering is also applicable to terrorism financing.

11.2. ML/TF Risk Identification and Analysis

The first step in assessing ML/TF risks 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.

For the analysis, the bank should make an estimate of the likelihood that these types of risk will 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. the impact 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 bank can decide on a more detailed scale.

Rating	Likelihood	Rating	Impact
High	Probably occurs more than 3 times in a year	**Major**	Long term, high cost consequences affecting functioning
Medium	Probably occurs once in a year	**Moderate**	Medium term consequences with some costs
Low	Unlikely to occur but not impossible	**Minor**	Short term or low cost consequences

11.2.1. Country or geographical risk

Country or geographical risk may arise because of the location of a customer, the origin and destination of transactions of the customer, business activities of the bank and their geographical location. Country or geographical risk, combined with other risk categories, provides useful information on potential exposure of money laundering and terrorism financing.

There is general definition based on which particular countries or geographical areas can be categorized as low 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.

The main factors that may indicate a high risk are as follows:

- Countries or geographic areas subject to sanctions, embargoes, or comparable restricted measures issued, for instance, by United Nations, OFAC, The European Union, or HM Treasury.
- 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 adequate 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 corruption, or criminal activities.

11.2.2. Customer Risk

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

Categories of customers that may indicate a higher risk with respect to ML/TF are:

- PEPs;
- FXDs and MSPs;
- NGOs

- lawyers; and
- Other customer as enunciated in the AML/CFT Responsibilities and Preventative Measures Regulations.

The delivery channels play a crucial role when assessing the customer 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 of a category of customers.

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

Description of 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:

Type of customer	Likelihood	Impact	Risk analysis
Domestic and retail customer	Medium	Moderate	Medium
Private banking customer	High	Major	High
Small business	Medium	Moderate	Medium
International corporation	High	Moderate	Medium

FXDS & 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 will be applied.

11.2.3. Transaction, Product and Service Risk

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 special attention to ML/TF risk which may arise from the application of new technologies. In identifying the risks of transactions, products, and services, the following factors can be considered:

- 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.

Specific lease products, life insurance policies with a low annual premium or a low single premium, 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, 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. 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. Funds tend to be loaded through cash deposits and it is not necessary to have a bank account. The likelihood that prepaid cards are used for ML/TF is high and the impact on the business, seeing that it is a new product, will be very high. Risk assessment is high.

This description can result in a table as below:

Type of transaction	Likelihood	Impact	Risk analysis
Betting transaction	High	Major	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

11.3. Risk Matrix

In assessing 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 risk.

Bank 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 zone, those that carry somewhat higher, but still acceptable risk, and those that carry a high or unacceptable risk of money laundering and terrorism financing. 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 recognize that ML/TF risks may vary across customers, products, and geographic areas and thereby focus its efforts on high risk areas in its business.

The following is the risk matrix of client-product combination basis the bank risk analysis:

Customer Transaction	Betting transaction	Online transaction	Domestic transfer	Prepaid card	Life insurance	Securities account
Domestic retail customer	High	High	Medium	High	Low	Low
Private banking customer	N/A	High	Medium	High	N/A	Medium
SME business customer	High	High	Medium	High	Medium	Medium
International corporation	High	High	Medium	High	Medium	Medium

Company Listed on stock exchange	High	High	Low	High	Low	Low
PEP	High	High	High	High	High	High
Occasional transactions	High	High	Medium	High	N/A	N/A

The bank must take care that this 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.

11.4. Risk Management

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

ML/TF risk management requires attention and participation of several business units with different competences and responsibilities. It is important for each 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 is 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.

11.4.1. Role of Management

Management gives direction to its business activities by setting the risk appetite, formulating objectives and making strategic choices from which subsequently policy and procedures are derived. Management should be able to determine the ML/TF risks of the business and take these into account 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). 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).

Management's leadership abilities in and commitment to the prevention of money laundering and terrorism financing are important aspects of implementing the risk-based approach. Management must encourage regulatory compliance and ensure that employees abide by internal procedures, policies, practices and processes aimed at M/TF risk mitigation 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 denotes a climate and atmosphere in which a 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.

11.4.2. AML/CFT Policies and Procedures

Once the identification and risk analysis processes are completed, the strategy of ML/TF risk management is applied to enable the bank to implement adequate policies and procedures for reducing the 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 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 Fin TRACA.

ML/TF Risk Monitoring and Review

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 risk management measures correspond to the bank's risk analysis. The bank should therefore establish an appropriate and continuing process for ML/TF risk monitoring and review. 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.

11.4.3. Monitoring Process

Regular reports to management should contain the results of the monitoring process, findings of internal controls, reports of organizational units 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 Fin TRACA, as well as the findings contained in the supervisor's on-site examination reports on AML/CFT. Management should be furnished 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.

The 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

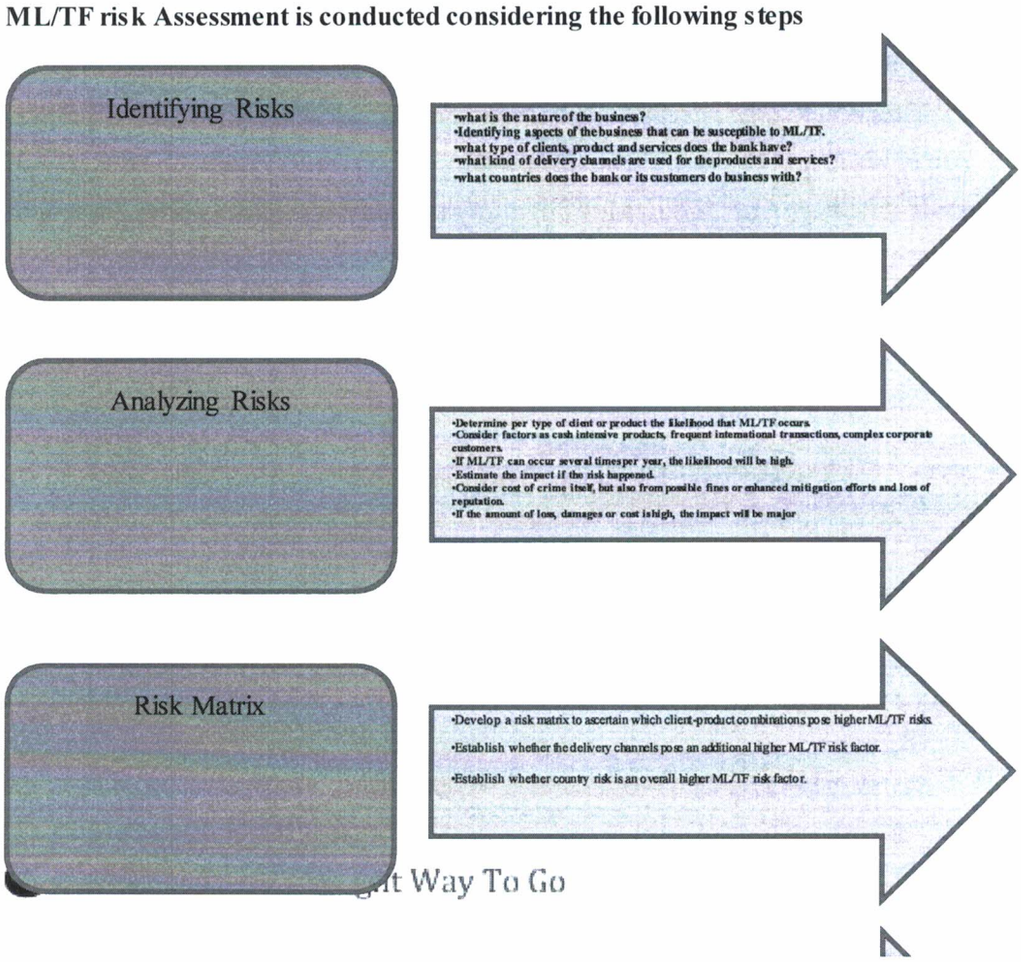
negative consequences for the bank's business occur. This process may also alert the bank to any potential failures, for instance failure to include mandatory legislative components in the AML/CFT policies and procedures, insufficient or inappropriate customer due diligence, or level of risk awareness not aligned with potential exposure to ML/TF risks.

11.4.4. 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.

Moreover, 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.

ML/TF risk Assessment is conducted considering the following steps



12. Customer/ Relationship Risk Assessments

The Bank shall categorize its customers as high, medium & low based on the risk they pose by assessing the five basic principles that is Customer type, products & services, geographic location, delivery channels and transactions. Bank shall further consider other risk factors which influences the risk categorization. Bank shall continuously monitor and evaluate the risk profile of its customers and shall change/transfer the risk from one category to another as and when the customers risk changes based on the other factors determining the risk.

The Bank shall consider the following factors & criteria among others in accordance with the pertinent information, when preparing the risk assessments:

a. Customer type i.e. nature of their business, nationality, occupation, cash intensive businesses, import/export companies, PEPs, Origin & source of the customer's funds and anticipated transaction activity etc.
b. Products and services i.e. the risks that arise from the products and services offered i.e. private banking, wealth management, international wire transfers, trade finance etc.
c. Geographic location i.e. countries or domestic geographic areas in which customers operate or the place of origination or destination of transactions or the jurisdictions that have been identified as having strategic AML/CFT deficiencies by FATF or any relevant international bodies.
d. Delivery channels i.e. the risks that arise from the channels used to deliver products and services
e. Transactions i.e. deposits, frequency of transactions, volume & size of transactions considering the usual activity and the profile of the customers

12.1. Other Factors to consider for Risk:

a) Length of Relationship
b) PEP's & Associated PEP's

c) Relationship history i.e. LCTR customer, subject of STR/SAR filing, subject of court orders, negative press etc.
d) Cash activity volume
e) Wire activity volume
f) Total volume
g) Country of residency
h) Country of incorporation
i) Transfers from and to Offshore tax heavens
j) Professional service providers acting on behalf of the customer (Lawyers, Auditors, Company service providers etc.)
k) The nature, scale, diversity and complexity of customer's business
l) Customers target market

The precise purpose of the transactions monitoring shall be to ascertain as to whether the transaction is outside the scope of expected normal transactions conducted by the customer or is it contradicting to the customer profile collected at the time of establishing the relationship or whether the transaction originated from or is destined for a high risk jurisdiction.

12.1. High Risk Category Customers

The bank has identified specific categories of customers whose inherent risk is usually high. The bank shall always exercise enhanced due diligence while dealing with such type of customers.

Customer Category	ML/ TF Risk
Politically Exposed Person, PEP	High
NGO/NPO/Trust	High
MSP/FXD	High
Lawyers / Auditors	High
Agency Banking Agent account	High
Nonresident customer	High
Suspicious transaction report raised in the last 12 months	High
Financial institutions	High
Bank Staff	High
PEP Associates	High

12.2. Conducting Customer Risk Categorization Via Risk Scoring Matrix

Risk scoring matrix is the easy & effective way that has been developed to categorize customer for ML/ TF risk, while opening account. The basic five principles that is Customer type, products & services, geographic location, delivery channels and transactions are included.

Bank shall follow RSM & manual & relevant instruction that is circulated to branches.

13. High Risk Situations Requiring Enhanced Due Diligence

The Bank has identified the following possible factors and potentially higher risk situations that shall attract the application of enhanced customer due diligence:

13.1. High risk situations identified for customer risk factors shall inter alia include the following:

i. The business relationship is conducted in unusual circumstances e.g. significant/unexplained geographic distance between the Bank's branch and the customer.
ii. Non-resident customers.
iii. Legal persons or arrangements that manage the assets of third parties.
iv. Companies that have nominee shareholders or shares in bearer form.
v. Activities those are cash-intensive or susceptible to money laundering or terrorism financing.
vi. The ownership structure of the company appears unusual or excessively complex with no visible economic or lawful purpose given the nature of the company's business.
vii. Business relationships and transactions conducted other than "face-to face".
viii. Business relationships conducted in or with the high risk countries.
ix. Politically exposed persons ("PEPs") or customers linked to PEPs.
x. High net worth customers or customers whose source of income or assets is unclear.
xi. Businesses/activities identified by the FIU, Da Afghanistan Bank or the FATF as of higher money laundering or financing of terrorism risk.

13.2. High risk situations identified for country or geographic risk factors shall inter alia include the following:

i. Countries classified by credible sources, such as mutual evaluation reports or published follow-up reports, as not having adequate AML/CFT systems.
ii. Countries identified by Da Afghanistan Bank or the FIU as high risk.
iii. Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations, OFAC, EU, HM Treasury
iv. Countries classified by credible sources as having significant levels of corruption or other criminal activity.
v. Countries or geographic areas classified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.

13.3. High risk situations identified for Products, services, transaction or delivery channel risk factors shall inter alia include the following:

i. Private banking.
ii. Anonymous transactions which may include cash.
iii. Accounts opened, business relationships or transactions conducted with customers that are not physically present for the purpose of identification.
iv. Payment received from unknown or un-associated third parties.
v. Complex trade financing products.

13.4. Red Flag Transactions

Further, The Bank has identified certain highly risky transactions as detailed hereunder and categorized as 'Red Flag' requiring special attention of all the dealing officials.

- A transaction which is complex, unusual or large, whether completed or not;
- Unusual patterns of transactions; and
- Insignificant but periodic transactions which have no apparent or visible lawful purpose.

- One-off transaction means transaction other than normal transaction carried out in the course of an existing business relationship.
- The parties to the transaction (owner, beneficiary, etc.) are from countries known to support terrorist activities and organizations.
- Inclusion of the individual or entity in the United Nations (1267 & 1988), OFAC, EU, HM Treasury Sanctions lists.
- Any account holder is linked to known terrorist organizations or is engaged in terrorist activities.
- Beneficial owner of the account not properly identified.
- Use of nominees, trusts, family members or third party accounts.
- Use of false identification Documents.
- Abuse of non-profit organization (NGOs).
- The use of funds by the non-profit organization (NGOs) is not consistent with the purpose for which it was established.
- The transaction is not economically justified considering the account holder's business or profession.
- A series of complicated transfers of funds from one person to another as a means to hide the source and intended use of the funds.
- Transactions which are inconsistent with the account holder's normal activity.
- Deposits were structured below the reporting requirements to avoid detection.
- Multiple cash deposits and withdrawals with suspicious references.
- No business rationale or economic justification for the transaction.
- Multiple cash deposits in small amounts in an account followed by a large wire transfer to another country.
- The client fails to provide satisfactory evidence of identity.
- Situations where it is very difficult to verify customer information.
- Situations where the source of funds cannot be easily verified.
- Client wants to re-sell Property shortly after purchase at a significantly different than the purchase price.

- Client gives power of attorney to a non-relative to conduct large transactions.
- Divergence from the type, volume or frequency of transactions expected in the course of the business relationship.
- The client fails to provide satisfactory evidence of identity.
- Situations where it is very difficult to verify customer information.
- Situations where the source of funds cannot be easily verified.
- Client wants to re-sell Property shortly after purchase at a significantly different than the purchase price.
- Client gives power of attorney to a non-relative to conduct large transactions.
- Divergence from the type, volume or frequency of transactions expected in the course of the business relationship.

14. Low Risk Situations Requiring Simplified Customer Due Diligence

The Bank has identified the following possible factors and potentially low risk situations that shall attract the application of simplified customer due diligence.

14.1. Low risk situations identified for customer risk factors shall inter alia include the following:

i. Companies listed on a stock exchange and subject to disclosure requirements either by law, or stock exchange rules or other binding Instructions or Regulations which define requirements to ensure disclosure of beneficial ownership.

ii. Public enterprises.

14.2. Low risk situations identified for country or geographic risk factors shall inter alia include the following:

i. Countries classified by credible sources, such as mutual evaluation reports, as having effective AML/CFT systems.

ii. Countries classified by credible sources as having a low level of corruption or other criminal activity.

14.3. **Low risk situations identified for Products, services, transaction or delivery channel risk factors shall inter alia include the following:**

i. Financial activity is carried out by a natural or legal person on an occasional or very limited basis such that there is a low risk of money laundering and terrorist financing and that are provided to a low risk customer for financial inclusion purposes.

ii. Financial products or services where there is a proven low risk of money laundering or terrorist financing which occurs in strictly limited and justified circumstances and it relates to a particular type of financial institution or activity.

15. Account opening Procedure

The bank shall identify and verify the customers of all forms before establishing a relationship. Bank shall apply simplified due diligence, enhanced due diligence or any other measures to identify and verify a customer before establishing the relationship.

Bank/ relevant department shall have in place proper procedure for batch interface/bulk-process of account opening. Bank has to obtain complete KYC documents & information prior to bulk-process of account opening, as per the provisions of this policy & relevant procedures issued by compliance department.

The bank shall take into consideration the following programs inter alia into its account opening procedure.

15.1. Customer Identification Program

The Bank has designed and implemented customer identification program taking into consideration the risks set out hereinabove. The bank shall collect all the required KYC documents to identify the identity of the customer. In addition to the KYC documents mentioned below the bank shall request for any other additional documents to identify the customer to its satisfaction. The Bank has required the branches/offices to adopt following measures to manage the risks:

a. To obtain additional information on the customer, beneficial owner, beneficiary and transaction.

b. To establish a risk profile on customers and transactions. The customer profile shall be based upon sufficient knowledge of the customer and beneficial owner(s) as applicable including the customer's anticipated business with the bank and where necessary the source of funds and source of wealth of the customer.
c. To apply enhanced customer due diligence to high-risk customers.
d. To update the KYC information on all customers at least annually.
e. To adopt other measures as may be prescribed by Da Afghanistan Bank or the FINTRACA.

15.2. Customer Identification Requirements

As per the Bank's policy the customer identification requirements shall inter alia include the following:

i. The Bank shall not maintain or open an anonymous account or an account in fictitious names.
ii. The Bank has already set up a system for the identification of the clients and to establish the identity of clients when performing any transaction for them.
iii. The Bank shall ensure to know the true identity of its customers including beneficial owners.
iv. Customer due diligence shall be carried out in the following cases:

a. Before establishing a business relationship with a customer or opening an account.
b. Before carrying out a transaction for an occasional or walk-in customer when the transaction involves an amount equal to or above 50000 AFN or its equivalent in other currencies, whether conducted as a single transaction or several transactions that appear to be linked. For the purpose of this policy the walk-in customer shall mean a customer who is not in an established business relationship with the Bank
c. Bank shall not carry out occasional/third party transactions in excess of AFN 500,000 on behalf of customers who refuse/or are unable to identify themselves at all or refuse to/or are unable to disclose and document the source of their funds.
d. Before carrying out domestic or international wire transfers.
e. Whenever doubts shall exist about the veracity or adequacy of previously obtained customer identification data; and
f. Whenever there is a suspicion of money laundering or terrorist financing.

v. The customer due diligence to be carried out by the Bank shall inter alia include the following:

- To identify and verify the identity of the customer and beneficial owner using reliable, independent source documents, data or information.
- To verify that any person acting on behalf of the customer is authorized to do so and identify and verify the identity of that person.
- To understand and obtain information on the purpose and intended nature of the business relationship.
- To the extent possible to obtain the customers' tax identification number (TIN) and tax statements and in addition, in the case of legal persons, audited financial statements and details as shall be specified by Da Afghanistan Bank or the regulatory agency.
- To monitor the business relationship on an ongoing basis and to examine any transactions carried out to ensure that they are consistent with the Bank's knowledge of the customer as also commercial activities and risk profile of the customer and the source of funds.
- Customer identification requirements for natural persons shall also be applied to identify customers who are legal persons and arrangements. Procedures established relating to the identification and verification of natural persons who are individual customers shall also be similarly applicable to beneficial owners of legal persons and arrangements.

vi. For legal persons, understanding and documenting the ownership and control structure of the customer.

vii. The Bank shall verify whether any natural person is purporting to act on behalf of a customer who is legal person or legal arrangement.

viii. Legible file copies shall be taken of the relevant identification and supporting documentation for all customers both natural and legal persons. The customer's signature or finger print shall be obtained on each page of such copies.

15.3. Identification of Natural Person Customers for account opening

For customers who are natural persons the Bank shall verify the identity using reliable, independent source documents, data, or information which shall inter alia include the following:

a. Full name, Father's Name including any aliases.
b. Business Name (in case of sole proprietorship).
c. Gender.
d. Copy of Tazkira or National Registration Card/Citizen Scrutiny Card/Passport
e. Copy of passport along with valid work permit for Non residents
f. Permanent and mailing address.
g. Copy of address proof
h. Date of birth.
i. Nationality.
j. Occupation.
k. Income and source of income. (In case of income source being from business, copy of business license), (source being rent of property, copy of rent), (source being salary, copy of employment letter/agreement), (source being a customs broker, copy of license from customs department/MOF) and any other relevant document to prove thee source of income
l. Phone number (if any).
m. Email address (if any).
n. Photo.

In the case of joint accounts, the Bank shall obtain the above information on all parties to the account.

15.4. Identification of Legal Person Customers for account opening

For customers who are Legal persons and Legal Arrangements including partnerships, limited liability partnerships and Trusts the Bank shall identify the customer and its beneficial owners, by understanding the nature of its business, and its ownership and control structure. The Bank shall obtain

and verify the information required using reliable, independent source documents, data, or information which shall inter alia include the following:

1. Name, legal form and proof of existence of the legal persons;
2. Location of the principal place of business of the legal person;
3. Board Resolution to open, operate and close bank accounts
4. Identification documents for Shareholders, Directors, individuals, authorized signatories who have authority to open, operate and close the account and Name & identification documents of relevant persons holding senior management positions.
5. Mailing and registered address of legal person including phone, fax and e-mail id.
6. Nature and purpose of the business;
7. The identity of the ultimate beneficial owner;
8. Address of head office.
8. Certificate of Incorporation/License (to be updated annually),), In case of joint venture, JV license from AISA+MOCI/Relevant ministry/authority, Memorandum of Association, Article of Association. (In case the license is under renewal then the process letter from relevant ministry and an undertaking letter from the company on official letter head sealed & stamped by the authorized signatories to provide the license copy as soon as they receive it)
9. Partnership Agreement
10. President & vice president have to be present. If the President or the vice president is outside Afghanistan, then an NOC from the absentee to be provided (the same has to be attested by the relevant embassy and Ministry of foreign affairs Afghanistan.) If they are in Afghanistan but in different cities they can be verified through Azizi banks nearest branch and his signature can be obtained once he returns back
12. Trust deed
13. Name and address of Board of directors (phone numbers & Email address, if available)
14. "Identification documents of Directors/Shareholders/Partners
15. "Identification documents of Settlors, Trustees, Protectors and beneficiaries with respect to trusts

The Bank shall verify the authenticity of the information provided by the company/business with the relevant license issuing authority.

For foreign incorporated or foreign registered business entities, comparable documents shall be obtained. The Bank shall make all efforts to verify the documents supplied including requiring that they be certified by the Office of Foreign Affairs and endorsed by the Embassy of Afghanistan.

15.5. Identification of Non-Government Organization for account opening

For Non-Government Organization (NGO) and Non-Profit Organizations (NPOs) the Bank shall verify the identity using reliable, independent source documents, data, or information which shall inter alia include the following:

1. Name of Non-Government Organization/Non-Profit Organization.
2. Full Address.
3. Certification of registration.
4. Constitution of the NGO/NPO.
5. Name and address of Executive committee.
6. Telephone No. and email address.
7. List of Directors/members
8. Executive committee's decision regarding open, operate & close bank account.
9. Identification documents of directors/senior officers of the NGO/NPO.
10. Authorization for the operation of accounts financial transactions.
11. Identification documents to identify the person authorized to represent the NGO/NPO in its dealings with the bank/financial institution.
12. Copy of the latest certified taxation return and related documentation.
13. Copy of the latest financial statement.

15.5.1. EDD on NGOs/ NPOs

Bank should conduct enhanced due diligence via EDD form as per **Annexure I**, while establishing relationship with Non-Governmental Organizations (NGOs)/Not-for-Profit Organizations (NPOs) to

ensure that these accounts are used for legitimate purposes and the transactions are commensurate with the stated objectives and purposes.

The Compliance review process shall include followings;

a. The CIF / KYC and EDD forms shall be filled for customers and shall be sent to Compliance Dep HO along with ID copies (Tazkira / Passport), license, TIN and other supporting documents (as defined in Account Opening Checklist).
b. Compliance Department shall independently check / review / scrutinize the documents and information provided.
c. Branch shall wait until the process is completed as it may take couple of days since the licenses need to be verified from the issuing authority.
d. Some exceptional cases might be there, where bank may stand the choice to consider some exemptions for particular customer if it already maintained other accounts in the past. For example; different currency account of an NGO that is recent & ministry confirmation is already sought etc.).

The accounts should be opened in the name of relevant NGO/NPO as per title given in constituent documents of the entity. The individuals who are authorized to operate these accounts and members of their governing body should also be subject to comprehensive CDD. Bank should ensure that these persons are not affiliated with any proscribed/ designated entity or person, whether under the same name or a different name.

In case of advertisements through newspapers or any other medium, especially when bank account number is mentioned for donations, Bank shall ensure that the title of the account is the same as that of the entity soliciting donations. In case of any difference, immediate caution should be marked on such accounts and the matter should be considered for filing STR.

Individual accounts shall not be allowed to be used for NGO/ NPO especially, for their charity purposes/collection of donations.

Account should be only opened in the jurisdictions where the NGO/ NPO operates/ runs its projects. For this purpose, the bank should know NGO's/ NPO's areas of the operation & shall obtain a list.

15.6. Identification of Associations & Social Institutions for account opening

For Associations & Social institutions the Bank shall verify the identity using reliable, independent source documents, data, or information which shall inter alia include the following:

1. Name of Association/Social Institution.
2. Full Address.
3. Certification of registration/License
4. Constitution of the Association/Social Institution.
5. List of Directors/members
6. Name and address of Executive committee.
7. Telephone No and email address. (If any)
8. Executive committees /Board of Directors decision regarding opening of account.
9. Identification documents of directors/senior officers of the Association/Social Institution.
10. Authorization for the operation of accounts financial transactions.
11. Identification documents to identify the person authorized to represent the Association/Social Institution in its dealings with the bank/financial institution.
12. Copy of the latest certified taxation return and related documentation.
13. Copy of the latest financial statement.

15.7. Identification of Money exchangers/Money service providers for account opening

For Money exchangers and money service providers the Bank shall verify the identity using reliable, independent source documents, data, or information which shall inter alia include the following:

1. Name of Money exchanger/Money service provider.
2. Full Address.
3. Certification of registration/License issued by DAB.
4. Telephone No. and email address. (If any)
5. Tin Certificate

6. Board resolution regarding open, operate & close bank account (signed & stamped on company's official letter head).
7. Identification documents to identify directors/senior officers /Authorized Signatories

15.8. Identification of Embassies and Consulates for account opening

For Embassies/Foreign Consulates the Bank shall verify the identity using reliable, independent source documents, data, or information which shall inter alia include the following:

1. Name of Embassy/Consulate.
2. Full Address.
3. Certification letter from ministry of foreign affairs certifying the ambassador/consul
4. Formal letter from the Ambassador/Consul/First secretary of the embassy/consulate stating the authorized signatory
5. Formal letter/Resolution from the Ambassador/Consul/First secretary of the embassy/consulate regarding open, operate & close bank accounts (signed & stamped on official letter head)
6. Telephone No. and email address. (If any)
7. Identification documents to identify the Ambassador/Consulates/Authorized Signatories

15.9. Identification of Travel & Tourist companies for account opening

For Travel & Tourism based companies the Bank shall verify the identity using reliable, independent source documents, data, or information which shall inter alia include the following:

1. Name of Tourist Company.
2. Full Address.
3. Certification of registration/License issued by the relevant ministry
4. Constitution/Articles of the Association of the company.
5. List of Directors/members
6. Telephone No and email address. (If any).
7. Board resolution to open, operate & close bank accounts

8. Identification documents of directors/senior officers of the tourist company
9. Identification documents to identify the person/s authorized to represent the tourist company in its dealings with the bank/financial institution.
10. Copy of the latest certified taxation return and related documentation.
11. Copy of the latest financial statement.

Note: A detailed checklist & requirements to open various type of account is given at the end of this document as **Annexure II**

15.10. Identification and Verification of Beneficial Owner

The Bank shall take reasonable measures to determine if a customer is acting on his/her own or on behalf of one or more beneficial owners. If the Bank determines that the customer is acting on behalf of one or more beneficial owners, *it shall* take steps to verify the identity of the beneficial owner(s) by using relevant information or data obtained from a reliable source such that the Bank is satisfied that it knows the identity of the beneficial owner(s).

If a customer is a company listed on a stock exchange, the Bank shall not be identifying and verifying the identity of any shareholder or beneficial owner of the company provided that the company is subject to adequate disclosure requirements to ensure transparency of beneficial ownership. In this case, the Bank shall only obtain customer identification documents on the company itself.

For customers that are other legal entities or legal arrangements i.e. other than the companies listed on a stock exchange the Bank shall take adequate measures to understand the ownership and control structure of the customer, including the ultimate natural person who owns or controls it as described hereunder:

1. With respect to such legal entities identification shall be made of each natural person that:
    - Owns or controls directly or indirectly more than 10% of the legal entity;
    - Is responsible for the management of the legal entity; or
    - Exercises control of the legal person through other means.

2. With respect to legal arrangements, identification shall be made of the settlor, trustee, protector and beneficiary or of persons in similar positions.

15.11. Due diligence of corresponding banks, banks providing counter bank guarantees in favor of Azizi bank, & treasury counter parties.

While establishing relationship with any corresponding bank, treasury counter party &, bank issuing counter-bank guarantee in favor of Azizi bank, bank should have in place, proper due diligence measures including followings; to mitigate the inherent money laundering and terrorist financing risk.

a) Performing background check on the entity
b) Sanction screening
c) Obtaining certificate of registration/ business license, or any equivalent document issued by competent authority of its country or origin, proving registration of the entity, country of registration & residence, and all relevant information. Also, type/ nature of business to be part of that document if not, validation from an independent authority.
d) Obtaining list of shareholders holding more than 10% of bank's shares including their nationality, date of birth, place of birth and address.
e) Obtaining list of Directors and Management members, along with nationality, date of birth, place of birth and address
f) Obtaining three years audited financial statements
g) Obtaining filled Azizi bank AML questionnaire in case of corresponding banking relationship.

16. Customer Screening Program

The bank shall use the following resources for screening customers:

i. UNSCs 1267 & 1988
ii. OFAC (Office of Foreign Asset Control)
iii. Fin TRACA Watch-list
iv. European Union

v. HMT (Her Majesty Treasury) of UK

vi. List of Entities Prohibited by DAD from depositing or withdrawing USD Banknotes

vii. Bank's own list of suspicious customers or customers with bad track record

17. Walk-in/Third Party Customers

Walk-in-customers shall only be entertained, once due diligence measures for transactions relating to such customers as given in below, have been exercised.

a) Bank shall obtain following information while performing any type of transaction for walk-in customers.
   a. Name
   b. Tazkira/ Passport No
   c. Contact information (cellphone no etc.)
   d. Father's name
   e. Date of birth full address
   f. Purpose of the transaction must be clearly maintained in system & relevant form(s).

b) In case of transactions above AFN 500,000 or equivalent in other currencies, the relationship between the depositor (who is walk-in customer) and account holder should be clarified in the 3rd party/ LCTR form & the branch shall obtain necessary information about the fund owner if different than depositor. Such as; Name, Father Name, ID number, contract information.

c) Purpose of the transaction must be clearly maintained in the relevant LCTR/ 3rd party form as per **Annexure III**

d) All walk-in customers must be screened into sanction & watch lists such as; EU, UN, HMT, OFAC, Fin TRACA Watch-list, List of Entities Prohibited by DAD from depositing or withdrawing USD Banknotes & the relevant item under LCTR/ Third party form shall be marked.

e) Necessary supporting must be obtained from the customer including documents concerning identification (i.e. Tazkira/ Valid Passport/ Valid Driving License) & source/ origin of fund documents as per circular# COM/2017/007 dated 12.02.2017.

f) Before carrying out any domestic/ cross-border wire transfer for walk-in customer, the CDD requirements as set out in the point#8 & its subsequent sub-points must be met.

For the purpose of this policy the walk-in customer shall mean a customer who is not in an established business relationship with the Bank.

18. Politically Exposed Persons and risk Measure

The Bank shall establish appropriate risk management systems to determine whether a customer or beneficial owner is a politically exposed person (PEP) and if so, shall apply the following additional customer due diligence measures:

- Obtain approval from senior management (CEO & Dy. CEO or COO in absence of CEO & Dy. CEO) before establishing or continuing a business relationship with such a person or beneficial owner;
- Take all reasonable measures to identify the source of wealth and funds of customers and beneficial owners identified as PEPs; and
- Apply enhanced ongoing monitoring to the business relationship.

Procedures for determining whether a customer or beneficial owner is PEP shall include:

i. Seeking relevant information from the customer or beneficial owner;
ii. Accessing and reviewing available information from any reliable source about the customer or beneficial owner;
iii. Accessing and reviewing commercial electronic databases of PEPs, if available.
iv. Accessing and reviewing the FINTRACA's non-confidential information if available on PEPs which shall not be the sole source of information.

19. Enhanced Customer Due Diligence ML/TF Risks Measures

The Bank shall examine, including by seeking additional information from the customer, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. The information to be obtained shall also include information on the nature or reason for the transaction.

Where the risks of money laundering or terrorism financing are higher, the Bank shall conduct enhanced CDD measures, consistent with the risks identified. In particular, the Bank shall increase the degree and nature of monitoring of the business relationship in order to determine whether those transactions or activities appear unusual or suspicious.

Enhanced CDD measures that shall be applied for higher-risk business relationships include, but are not limited to the following:

i. Obtaining additional information on the customer e.g. occupation, volume of assets etc. and updating more regularly the identification data of customer and beneficial owner.
ii. Obtaining additional information on the intended nature of the business relationship.
iii. Obtaining information on the source of funds or source of assets of the customer.
iv. Obtaining information on the reasons for intended or performed transactions.
v. Obtaining the approval of senior management (CEO & Dy. CEO or COO in absence of CEO & Dy. CEO) to commence or continue the business relationship.
vi. 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.
vii. Carrying out the first payment through an account in the customer's name with a bank subject to similar CDD measures.

Enhanced CDD shall be applied to higher risk customers at each stage of the CDD process and on an on-going basis.

Enhanced CDD procedures for business relationships with natural persons not physically present for the purpose of identification shall inter alia include:

- Certification of documents in line with relevant Laws and Regulations.
- Requisition of additional documents and development of independent verification measures and/or contact with the customer.

20. Simplified CDD ML and TF Risk Measures

The Bank shall apply simplified customer due diligence procedures upon undertaking a documented risk assessment of the customer relationship.

The general rule is that customers shall be subjected to the full range of customer due diligence measures as provided in this policy. In certain circumstances where the risk of money laundering or terrorist financing is lower, as determined by a risk assessment undertaken by the Bank where information on the identity of the customer and the beneficial owner of a customer is publicly available or where adequate checks and controls exist elsewhere in national systems simplified measures shall be employed.

The Bank shall not apply simplified CDD measures whenever there is a suspicion of money laundering or terrorism financing or when the customer has a business relationship with or in any of the following countries:

a. Countries classified by credible sources, such as mutual evaluation reports or published follow-up reports, as not having adequate AML/CFT systems.
b. Countries identified by Da Afghanistan Bank or the FIU as high risk.
c. Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.
d. Countries classified by credible sources as having significant levels of corruption or other criminal activity.
e. Countries or geographic areas classified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.

The simplified CDD measures shall be commensurate with the risk factors. Where the risks have been identified as low the possible simplified CDD measures could include, but are not limited to the following:

- Reducing the frequency of customer identification updates.
- Reducing the degree of on-going monitoring and scrutinizing transactions.

Where requested by DAB, the Bank shall submit the underlying risk assessment and basis for the application of simplified customer due diligence and shall make the documents of the assessment processes and procedures related to risk assessment available to Da Afghanistan Bank.

21. Delayed Customer Identification Verification

The Bank may engage in the business relationship with the customer prior to the completion of the customer verification process outlined in this policy provided all of the following circumstances are met:

i. When the verification occurs as soon as reasonably practicable.
ii. When it is essential not to interrupt the normal conduct of business.
iii. When the ML and TF risks are effectively managed.

The Bank shall adopt risk management procedures with respect to the conditions under which a customer may utilize the business relationship prior to verification. These procedures shall include a set of measures to manage the ML and TF risks and shall include:

- Limitation of the number, types and/or amount of transactions that can be performed;
- The monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship.

The Bank shall include in its risk management procedures concerning delayed customer verification a set of minimum requirements such as a limitation on the number, types or amount of transactions that can be performed by the customer.

22. Additional requirements for Customer Information

The Bank shall gather and maintain customer and beneficial owner(s) information throughout the course of the business relationship. Documents, data, or information collected under the CDD process shall be kept up to date and relevant by undertaking reviews of existing records at appropriate times especially when:

i. A significant transaction is to take place;
ii. There is a material change in the way the account is operated or transactions begin to deviate from the usual patterns;
iii. Information held on the customer is insufficient to enable the financial institution to understand the nature of the business relationship or transactions being conducted.

Further, in the case of legal persons, the Bank shall ensure that:

- Business and company registration and licensing documents are current and remain valid throughout the duration of the relationship.
- Updated financial statements are obtained from customers to the best extent possible
- Taxation information (copy of tax returns and certification) is obtained and updated on an annual basis. Declaration of tax clearance and tax exemption document as applicable example in case of NGO.

All transactions conducted by customers shall have to be accompanied by supporting documentation such as customs certifications confirming the value of the goods.

The Bank shall apply the CDD requirements to the existing customers on the basis of materiality and risk.

The KYC/ account opening forms shall be prepared by the Bank and filled out by customer in any of national languages of Afghanistan unless the customer is a foreign citizen.

The Bank shall renew/ update the KYC forms of any customer at least on yearly basis.

23. Ongoing Monitoring of Customer Transactions

The Bank shall implement systems to monitor on an ongoing basis customer transactions and the relationship with the customer. Monitoring shall inter alia include the scrutiny of customer transactions to ensure that they are being conducted in line with the Bank's knowledge of the customer and the customer risk profile and the source of funds and wealth, and the predetermined limits if any, on the amount and volume of transactions and type of transactions.

The Bank shall monitor customers' account activity, on a regular basis to be able to establish patterns, the deviation from which might indicate suspicious activity.

The Bank shall not allow business transactions in the personal accounts of the individuals.

24. Termination of Customer Relationship

If the Bank is unable to comply with the CDD required for a customer including, on the basis of materiality and risk in respect of the existing customer then it shall terminate the customer relationship and consider filing a report with the FINTRACA.

Individual accounts if they are used for business purpose despite multiple reminders/communications, then it shall terminate such individual customer relationship and advice the customer to open Corporate account to route such business transactions.

In case of a customer where multiple STRs are filed, then post filing of 3 STRs the bank shall terminate the customer relationship.

High Risk accounts – PEP/MSP/FXD/NGOs/Non-Resident customers wherein the account is in-operative for a period of 1 year with no transactions, such accounts will be reviewed and the bank shall initiate termination of the relationship to avoid unnecessary regulatory attention.

Where the Bank is unable to verify the identity of the customer and beneficial owner(s), it shall refrain from opening the account or commencing the business relationship or carrying out the transaction. In such cases, the Bank shall consider filing a suspicious transaction report to the FINTRACA.

25. Reliance on third parties

The Bank may rely on third party intermediaries to perform the CDD requirements of this policy if the following conditions are met:

- The Bank is satisfied that the third party is regulated, supervised or monitored for and has measures in place for compliance with the customer due diligence and record keeping requirements;
- The Bank can immediately obtain all required customer due diligence information; and
- The Bank is satisfied that copies of identification data and other documents relating to customer due diligence measures will be made available from the third party upon request and without delay.

Before entering into a relationship with a third party the Bank shall have regard to the money laundering and terrorist financing risk associated with the country in which the third party is based.

Notwithstanding the above the ultimate responsibility for customer identification and verification shall remain with the Bank only.

26. Agency Relationship (Branchless Banking)

Bank may inter into agency relationship for the sake of either/ more of the following activities permitted by DAB, provided that all requirements as per Branchless Banking Regulation of Afghanistan are met.

1. Account opening (only individual current and saving accounts);
2. Collection of deposit and cash disbursement as per defined threshold in contract;
3. Micro and small value loan application process on behalf of financial institutions;
4. Bill payments;

5. Facilitating domestic fund transfer;
6. Micro and small value loan disbursement and repayment collection as per defined threshold in contract;
7. Collect check books, and payment cards order and distribute them; and
8. Any other services specified by DAB circular from time to time

27. Shell Banks

The Bank shall not enter into or continue a correspondent or business relationship with a shell bank and it shall satisfy itself that respondent financial institutions do not permit their accounts to be used by shell banks.

For the purpose of this policy, Shell bank is a bank that exists on paper only and that has no physical presence in the country where it is incorporated or licensed, and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision.

28. Offshore Companies

The Bank shall not enter into a relationship with Offshore Companies.

For the purpose of this policy, Offshore Company refers a Corporation, LLC or similar class of entity formed in a foreign country foreign to that of the principals of the organization. It also refers to a company or an entity that can only operate outside of its country of formation.

29. Correspondent Banking Relationship

Before entering into a cross-border correspondent banking relationship or other similar relationships, in addition to performing normal customer due diligence measures the Bank shall:

i. Gather sufficient information about the respondent bank.
ii. Understand the nature of the respondent's business.

iii. Evaluate the reputation of the respondent institution and the quality of supervision to which it is subject, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action.

iv. Evaluate the anti-money laundering and combating the financing of terrorism controls implemented by the respondent bank.

v. Obtain approval from senior management before establishing new correspondent relationships.

vi. Clearly understand and document the respective anti-money laundering and combating the financing of terrorism responsibilities of each bank.

vii. Obtain copies of correspondent banks policies & procedures with regard to compliance, AML/CFT, customer acceptance, internal control measures etc.

With respect to payable-through accounts, the Bank shall satisfy itself that the respondent bank:

- has performed CDD obligations on its customers that have direct access to the accounts of the correspondent bank;
- is able to provide relevant CDD information upon request to the correspondent bank.

These requirements shall also be applied to cross border correspondent banking and similar existing relationships.

30. Policies and Procedures on Wire Transaction

30.1. Cross Border Wire Transfers/International Wire Transfers

The Bank while engaging in cross border wire transfers of 1 AFN and above and in other currencies, shall include accurate originator and beneficiary information on wire transfers and related messages and ensure that the information remains with the wire transfer or related messaged throughout the payment chain. The information accompanying all wire transfers shall always contain:

1. The full name of the originator;

2. The originator account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction;
3. The originator's address, or customer identification, or date and place of birth;
4. The name and address of the beneficiary and the beneficiary account number or a unique identification number where such an account or number is used to process the transaction.

The Bank shall obtain necessary supporting documents, in addition to information obtained as above, in case of cross border wire transfers equal to or exceeding AFN 500,000 or its equivalent in other currencies.

For cross border transfers 1 AFN and above and in other currencies, the Bank shall ensure that they are always accompanied by:

1. Name of originator and
2. Account number or unique transaction number.

If the Bank is unable to comply with these requirements, it shall not execute the wire transfer and consider submitting a suspicious transaction report to the FINTRACA.

Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries the Bank may not apply requirements in respect of originator information, provided that the originator's account number or unique transaction reference number which permits traceability of the transaction is included and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country.

30.1.1. Procedures on processing cross-border wire transfer applications

1. Branch managers shall conduct a branch level primary review of all TTs applications, sign, stamp & then send the same to head office "payment & compliance Dept" for further process.

2. No payments to High risk, restricted, non-cooperative & sanction jurisdictions shall be processed with the exception of a certain grey listed country subject to enhanced due diligence and prior approval of compliance department.

   The list high risk, restricted, non-cooperative & sanction jurisdictions shall be published by Compliance department on a periodic basis.

3. Branches must ensure that, customers KYC files are updated & complete (i.e. updated & verified business license/Registration Certificate, TIN, Tazkira/Passport, Contact Details, Address, Tax Clearance, Source of Income/Turnover, Article of association, Nature of business, Beneficial owner, Verification of identity" prior to processing any outward payment application).
4. All parties involved in fund transfer "sender, beneficiary & beneficiary bank" shall be screened in accordance with point 16 of this policy.
5. All fields of application form "TT form" must be filled properly.
6. Purpose of the payment within TT form "field 70" should be clear and should always contain the name & description of the items which are being imported or the service being provided. Writing vague information such as: business transaction, import of goods, invoice ref no…" in the purpose filed have to be avoided.
7. All documents have to be relevant, reliable & clearly visible/ readable at the time of processing and should contain all required information as per the checklist enclosed as **Annexure IV.**
8. All supporting documents such as; Invoice, Contract, Bill of lading, Packing List" shall be in English language. In case of other languages, the certified English version/ translation shall be provided to bank.
9. For all payment against import of goods, relevant supporting documents & information such as; custom document, bill of lading, packing list etc. should be provided at the time of processing fund transfer. In case of advance payment, the undertaking/acknowledgment letter shall be collected from concerning customers on their stamped letterhead for providing relevant documents. The concerning branch/payment officer shall follow up to obtain the documents based on the amount remitted, goods/items and country, before the next payment is processed for the customer and in exceptional cases maximum within 3 months. In the time frame of 3 months, customer may be allowed maximum 3 payments subject to proper justification and

prior approval of Compliance department. In no case, SWIFT department shall exceed processing 3 payments of same customer, if the customer has not provided relevant supporting documents for their previous payments and account restriction (debit freeze) would be placed for such customers.

10. An acknowledgment letter shall also be collected from customer (s) to confirm that, all documents provided by the customer "invoice, contract, custom document, bill of lading..." at the time of fund transfer, are true & genuine.
11. Customer signature/stamp/ fingerprint shall be obtained on all documents such as; TT form, invoice, contract, custom document, bill of lading etc.
12. In case of any suspicion on the customer or the documents provided, the same shall be reported to compliance department on urgent basis.
13. The initial review at branch level based on the checklist (enclosed as Annexure IV) will save time, and customer will not face any inconvenience if the payment is rejected by compliance/ payment department after probable delay. It would be more convenient if the deficiencies of the TTs are identified and rectified at branch level

30.2. Domestic Transfers including Credit card & Debt card transactions

For domestic wire transfers including transactions using a credit or debit card as a payment system to affect a money transfer it shall be ensured that the ordering institution includes either:

- Full originator information in the message or payment form accompanying the wire transfer; or
- Only the originator's account number, where no account number exists, a unique identifier, within the message or payment form.

Information on wire transfers shall be made available by the Bank within three business days of receiving the request either from the beneficiary financial institution or from the FINTRACA.

The Bank shall ensure that non-routine wire transfers are not batched where this would increase the risk of money laundering or terrorism financing.

For cross-border wire transfers, the Bank while playing the role of processing an intermediary element of the payment chain shall keep all wire transfer information including originator and beneficiary information.

Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with related domestic wire transfer information, the Bank while acting as an intermediary financial institution shall keep a record, for at least five years, of all the information received from the ordering financial institution or another intermediary financial institution.

The Bank's policy has effective risk-based procedures for determining:

- When to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information and considering reporting to the FINTRACA;
- The appropriate follow-up action which may include restricting or terminating business relationships.

The Bank while acting as a beneficiary financial institution for wire transfers shall verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with the record keeping requirements of the DAB.
Here "Beneficiary" means the natural or legal person who is identified by the originator as the receiver of the requested wire transfer and also refers to the term "recipient" as it appears in the AML & PC law article 3.3.2. And the "Beneficiary financial institution" means the financial institution which receives the wire transfer from the ordering bank directly or through an intermediary financial institution and makes the funds available to the beneficiary.

31. Compliance independent review of credit fund & non-fund base facilities

The dedicated compliance officer to credit dept. shall conduct weekly independent review of credit fund & non-fund base facilities of equal to or exceeding USD 50,000 (or equivalent in other currencies) which has/ have been newly sanctioned, renewed/ extended in the last week. He/ she shall

on weekly basis, generate report of all such facilities issued/ renewed in the previous week from system & ask credit department for providing the relevant files for Compliance post-facto review.

The review shall be conducted based on the checklists (enclosed as Annexure V.a, V.b, & V.c) & the relevant compliance officer shall ensure that credit facilities are issued/ renewed in line with bank policies / procedures & relevant laws/ regulations. He/ she shall disclose report of findings (if any) with credit department for immediate remedial action.

It is also the responsibility of the relevant compliance officer to closely follow outstanding observation (s) with respective dept. for rectification. The status of outstanding observations will be informed to BOS on monthly basis/ as when the BOS meeting is held.

For the purpose of this procedure, credit fund base facilities mean commercial loans in the form of overdraft & term loan while credit non-fund base facilities mean Bank guarantee (including counter bank guarantee), FOBC "Foreign Bill for Collection" & LC "letter of credit".

32. Western Union & MoneyGram fund transfers

The bank shall maintain all the Western Union & MoneyGram transfers Inbound/Outbound and shall monitor on daily basis. In case any suspicion arises, the issue is further investigated/observed and screened. Once the suspicion is confirmed the same shall be forwarded to DAB/FinTRACA as STR/SAR without any delay, and shall be shared with the Western union & MoneyGram officials as well.

The required documents for sending and receiving money through Western Union & MoneyGram are as follow:

a) Tazkira (Afghan National ID) / Passport.
b) Passport with valid visa for non-residents

32.1. Information to be collected for transactions

a) Purpose of transaction
b) Source of fund
c) Relationship between the remitter & receiver

32.2. Other applicable procedures for transfers

a) Customer sent transactions are limited to four numbers in a month (i.e. Four remittance & four receipts)
b) Enhanced due diligence on scenarios where the sender is one but the receivers are many
c) Enhanced due diligence on scenarios where receiver is one but the senders are many
d) Enhanced due diligence on scenarios where the sender is always one and the receiver is always the same.
e) Enhanced due diligence on customers who send money to many countries without any rationale
f) Sender is foreigner & receiver is local or receiver is foreigner & sender is local
g) CRI form on customers to be completed for all unusual/suspicious transactions in case of Western Union Transfer
h) Maximum amount per remittance is USD 5,000/day in the Western Union & USD 48,000 in six months via MoneyGram

33. Concentration (Special-use, Omnibus, Settlement) Accounts

Concentration accounts are internal accounts established to facilitate the processing and settlement of multiple or individual customer transactions within the bank, usually on the same day.

Money laundering risks can arise in concentration accounts if the customer-identifying information, such as name, transaction amount and account number is separated from the financial transaction. If separation occurs, the audit trail is lost, and accounts may be misused or administered improperly.

Department (s) that use concentration accounts should implement adequate, procedures and processes covering operation and record-keeping for these accounts, including:

a) Capturing customer transactions in the customer's account statements.
b) Prohibiting direct customer access to concentration accounts.
c) Prohibiting customers' knowledge of concentration accounts or their ability to direct employees to conduct transactions through the accounts.
d) Retaining appropriate transaction and customer identifying information.
e) Reconciling accounts frequently
f) Establishing a timely discrepancy resolution process.
g) Identifying and monitoring recurring customer names.

34. Suspicious Transaction Reporting

The Bank shall as soon as possible but no later than 3 working days, after forming a suspicion that any transaction or attempted transaction, regardless of value involves proceeds of crime or funds related or linked to or to be used for money laundering or terrorism financing, report to the FINTRACA.

The Bank shall report details of suspicious transactions to the FINTRACA in the prescribed form as set out in the guidelines issued/to be issued by FINTRACA.

Suspicious transaction report shall be submitted to FINTRACA in one of the official languages of Afghanistan together with all necessary supporting documents including but not limited to: updated customer's KYC and account opening forms, updated account/s statement/s, identification documents such as Tazkira or passport, Business license etc. and other relevant documents supporting the reasons for forming suspicion about the customer.

While forming suspicion about a customer, the Bank shall conduct preliminary analysis on the customer based on all information available to it including the records of its previous transactions and other documents provided to it by the customer since establishment of its business relationship with the Bank and include the result of such analysis in its report to FINTRACA.

The Bank is aware that if FINTRACA determines that the STR quality is not at a level satisfactory to work on it, or missing necessary supporting documents it may reject the receipt of the STR and notify the reasons of such rejection, and the Bank shall rectify the deficiencies and inform the FINTRACA.

The branches have already been provided with the checklist containing information required for compiling suspicious transaction/activity reports as detailed hereunder:

34.1. Information required for drafting STR/SAR for Suspected Individual Customer

- Tazkira Number/ Afghan National ID
- Customer Name

- Date of birth
- Participant Role (Principal, Proxy, Beneficiary)
- Phone Number
- Full Address
- Evidence if obtained
- Full narration of the situation

34.2. Information required for drafting STR/SAR for Suspected Legal Entity

- Full name
- TIN or License number
- Participant Role
- Entity's phone number
- Entity's full address
- Evidence if obtained
- Full information of president and vice president of the entity
- Full narration of the situation
- Following information is also required from the President/Vice president (Shareholder – only if he is a suspect):
    a) Position
    b) Tazkira/ National ID
    c) Customer Name
    d) Date of birth
    e) Phone number
    f) Full address

34.3. Information required for drafting STR/SAR for Suspected NGO

- NGO's Name
- Participant Role

- NGO`s phone number
- NGO`s full address
- Evidence if obtained
- Full Information of Account holders
- Full narration of the situation
- Following information is also required from the president/Vice president (Shareholder – only if he is a suspect) :
    g) Position
    h) Tazkira/ National ID
    i) Customer Name
    j) Date of birth
    k) Phone number
    l) Full address

34.4. Information required for drafting STR/SAR for Suspected Walk-in Customers

- Tazkira Number
- Customer Name
- Date of birth
- Participant Role (Principal, Proxy, Beneficiary)
- Phone Number
- Full Address
- Evidence if obtained
- Full narration of the situation

34.5. Identification, Evaluation & Reporting of STR/ SAR

Identification of suspicious transaction/suspicious activity is very crucial for the bank to mitigate the risk and depends upon the detection mechanism in place.

Process of identification of suspicious transactions /suspicious activity should be started identifying unusual transaction and activity. An unusual transaction may be unusual in terms of complexity of transaction, nature of transaction, volume of transaction, time of transaction etc.

Generally, the detection of unusual transactions/activities may something be sourced as follows:

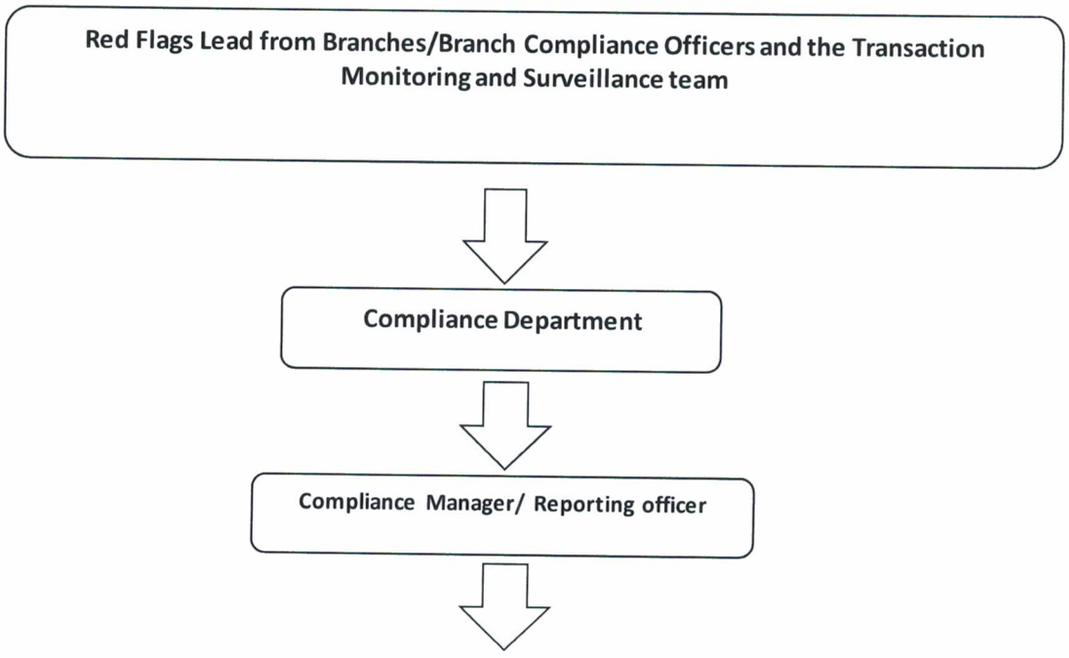
The 5 W's (Who, When, Where, What, Why) and H(How) is followed for identification and reporting of Suspicious transaction activity.

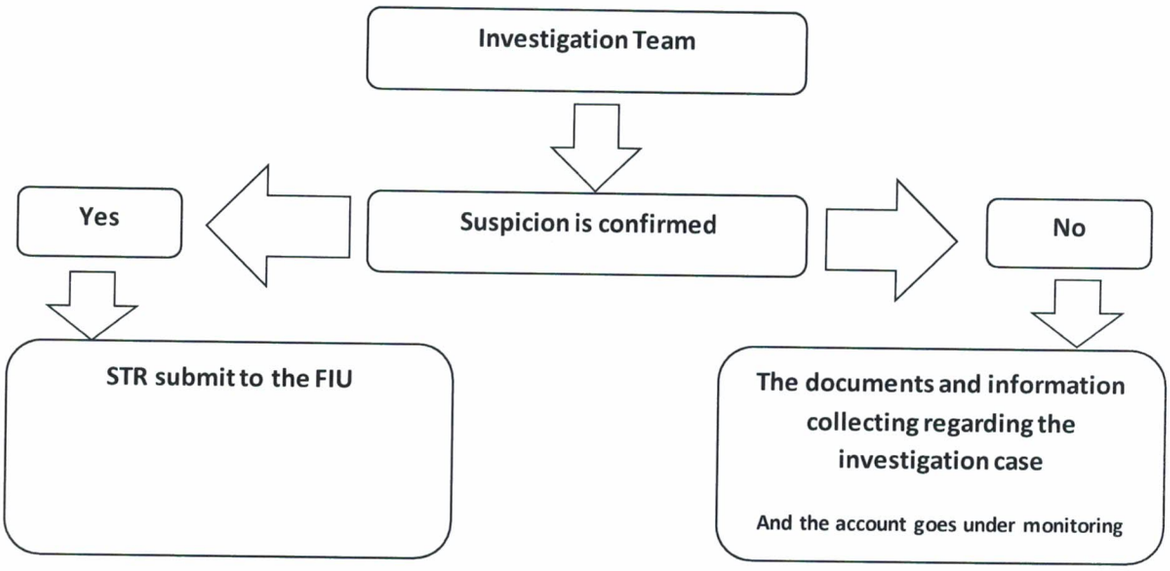
- Comparing the KYC profile, if any inconsistency is found and there is no valid reasonable explanation.
- By monitoring customer transactions including transaction conducted via cards (pre-paid, credit, debit)
- By using red flag indicators.

Any transaction/activity which is consistent with the provided information by the customer can be treated as normal and expected. When such transaction/activity is not normal and unexpected, it may treat as unusual transaction/activity.

Identification process of suspicious transaction is shown in flow chat.

Suspicious Transaction Reporting Flowchart





In case of reporting of STR/SAR, the following 3 stages should be conducted:

a) Identification:

Identification of suspicious transaction is very vital for STR/SAR reporting. Every officer who deals directly with customer should be vigilant in regards to KYC and sources of funds of the customer to identify STR/SAR.

Identification of suspicious transaction lies with officers of the bank who directly deals with customers at Head Office or at branches and the officer who approve/authorize the transaction. At branch level & Head office, person initiating the transaction should make sure he has taken correct and complete information of the customer as per requirement of AML/CFT policy and procedures, and the person authorizing/approving the transaction must ensure all proper documentation has been taken and the transaction is not suspicious.

b) Evaluation:

The initial evaluation shall take place at branch level and further evaluation at investigation section of Compliance department, before submitting/ reporting same to Fin TRACA/ FIU.

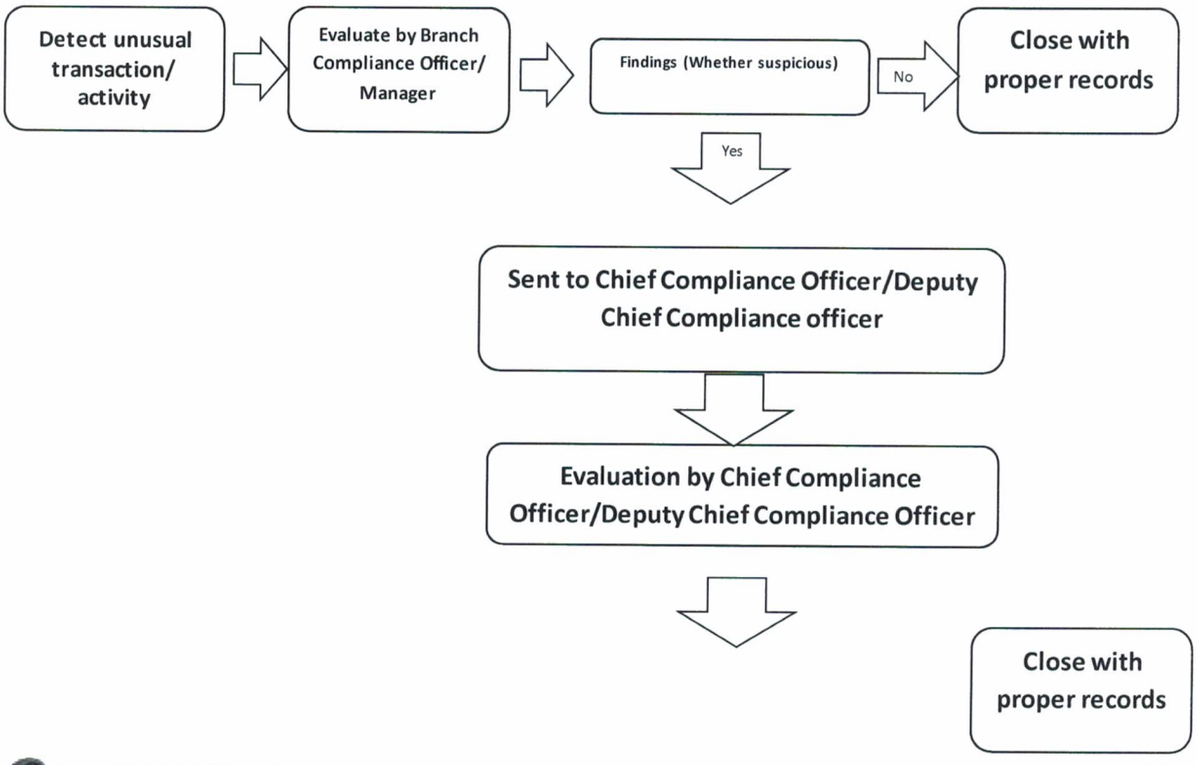
After identification of STR/SAR, at branch level Branch Compliance officer/ Manager should evaluate the transaction/activity to identify suspicion by interviewing the customer, collecting additional document and information or through any other means. At Head office level, Head of the monitoring

and investigation section will evaluate the identified STR/SAR in evaluation stage concerned Branch Compliance officer/ Manager and Head of monitoring and investigation section must be tactful considering the tipping off provision of the AML/ CFT Law &/ Regulation. If Branch Compliance officer/ Manager and Head of monitoring and investigation section is not satisfied, he/ she should forward the report to Chief Compliance Officer/Deputy Chief Compliance Officer. After receiving report from branch, Chief Compliance Officer/Deputy Chief Compliance Officer should also evaluate the report whether the STR/SAR report should be sent to Fin TRACA/ FIU or not. If he/ she is satisfied that reported suspicious transaction/activity is valid and reportable to Fin TRACA/ FIU, he/she shall instruct the relevant officer to directly file STR/ SAR with FIU considering all other provisions of article 24 & its sub articles of this policy. At every stage of evaluation (whether reported to FIU or not) the bank should keep records in a proper manner.

c) Disclosure:

This is the final stage where the bank should submit STR/SAR to Afghanistan Financial Intelligent Unit office if it is still suspicious.

For simplification, the flowchart given below shows STR/SAR identification and reporting procedures:



34.6. Identification, Evaluation & Reporting of STR/ SAR on Card Based Transactions

Cards are basic and popular financial instrument all over the world, and they have inevitably been used in all three stages of money laundering, mostly in the layering and integration stages.

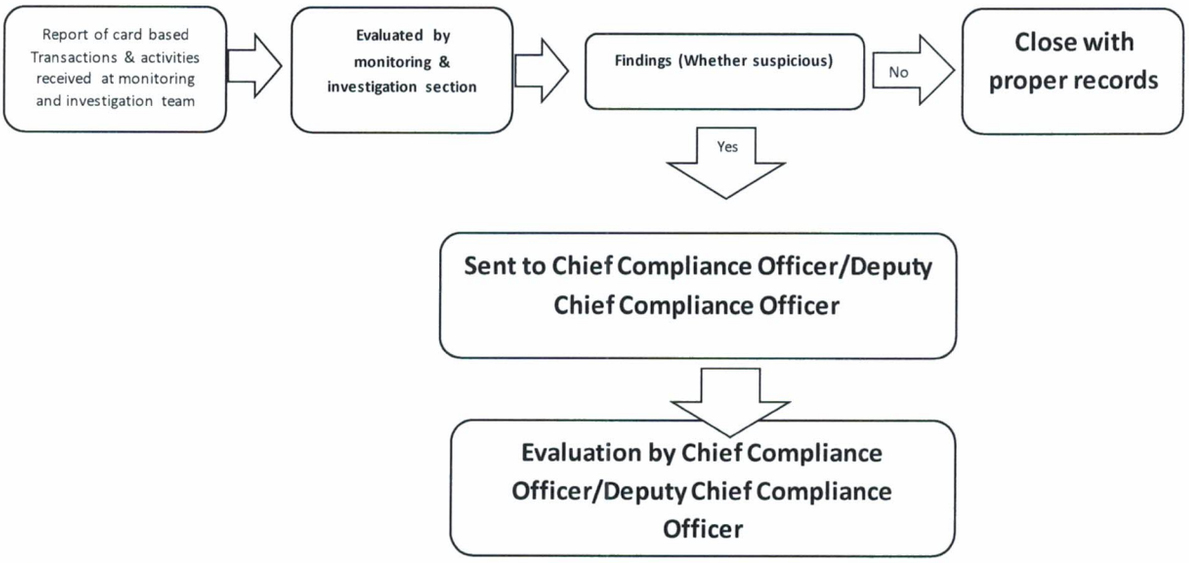
In recent years, along with new technologies adopted in the financial system, and payments have become very convenient and efficient option, particularly in Asia-pacific countries and regions where cards are widely used in not only cash withdrawal but also purchase transactions.

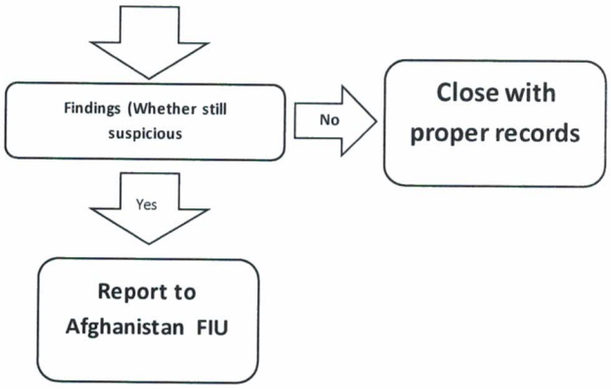
Portability, high value and wide cope of acceptability are the features of a card that increases risk of money laundering and terrorist financing in this product.

The monitoring and investigation section of compliance department shall receive regular reports of all transactions/ activities conducted via cards (credit, debit & prepaid). The section further need to carefully review all transactions and make sure these in line with customer KYC profile.

Unusual transactions need to be promptly reported to Fin TRACA-Afghanistan, in line with AZB AML/ CFT & CDD policy.

The flowchart in the next page shall be considered while reporting card based STR/ SAR.





34. Some RED FLAGS or indicators of STR

Following are some of the indicators or red flags which may help officers of DBH to identify suspicious transaction and suspicious activity.

a) Moving Customers

A customer who moves every month, particularly if there is nothing in that person's information suggesting that frequent changes in residence is normal, could be suspicious.

b) Suspicious Customer Behavior

- Customer has an unusual or excessively nervous demeanor.
- Customer discusses your record-keeping or reporting duties with the apparent intention of avoiding them.
- Customer threatens an employee in an effort to discourage required record-keeping or reporting.
- Customer is reluctant to proceed with a transaction after being told it must be recorded.
- Customer appears to have a hidden agenda or behaves abnormally, such as turning down the chance to obtain a higher interest rate on a large account balance.

- Customer who is a public official opens account in the name of a family member who begins making large deposits not consistent with the known source of legitimate family income.
- Customer who is a student uncharacteristically transacts large sums of money.
- Agent, attorney or financial advisor acts for another person without proper documentation such as a power of attorney.

c) Suspicious Customer Identification Circumstances

- Customer furnishes unusual or suspicious identification documents and is unwilling to provide personal data.
- Customer is unwilling to provide personal background information when opening an account.
- Customer asks many questions about how the financial institution disseminates information about the identification of a customer.
- A business customer is reluctant to reveal details about the business activities or to provide financial statements or documents about a related business entity.

d) Suspicious Cash Transactions

- Customer opens several accounts in one or more names, then makes several cash deposits under the reporting threshold.
- Customer conducts large cash transactions at different branches on the same day, or orchestrates persons to do so in his/her behalf.

e) Suspicious Non-Cash Deposits

- Customer deposits large numbers of consecutively numbered pay orders or round figure amounts.
- Customer deposits cheques and/or pay orders that are not consistent with the intent of the account or nature of business.
- Funds out of the account are not consistent with normal business or personal items of the account holder

- Funds deposited are moved quickly out of the account via payment methods inconsistent with the established purpose of the account.

f) Suspicious Activity in Credit Transactions

- A customer's financial statement makes representations that do not conform to accounting principles.
- Customer suddenly pays off a large problem loan with no plausible explanation of source of funds.
- Customer purchases certificates of deposit and uses them as collateral for a loan.

g) Suspicious Commercial Account Activity

- Business customer presents financial statements noticeably different from those of similar businesses.
- Large business presents financial statements that are not prepared by an accountant.

Branches shall download useful STR guidelines from the following link that also contains bundle of red flags & indicators.

https://www.fintraca.gov.af/assets/Guideline/STR%20Guideline.pdf

35. Consequence of failing to report Suspicious Transaction or activity

Failure to report suspicious transaction/ activity where the bank or its employee (s) has the requisite knowledge of suspicion, is a criminal offense subject to penalty and enforcement action as per article 51 of Afghanistan AML & PC law.

1.1. Penalty for the person who intentionally fails to report a suspicion as provided in article 18 of Afghanistan AML & PC law

a) Natural person: imprisonment for not less than six months and not more than one year or a fine of not less than 5,000 Afghani and not more than 50,000 Afghani, or both,
b) Corporate entities: a fine of not less than 25,000 Afghani and not more than 125,000 Afghani.

36. Threshold Reporting Requirements

The Bank shall report the particulars of transactions (deposits, withdrawals or transfers) in excess of AFN 1,000,000 or its equivalent to other currencies in a day or across 2 consecutive working days to the FINTRACA no earlier than the first business day of the month and no later than the fifth business day of a month following to the month during which the transaction occurred.

For Branchless Banking transactions the bank shall report particulars of transactions (deposits, withdrawals) in excess of AFN 10,000 or its equivalent to other currencies in a day or across 2 consecutive working days to FINTRACA no earlier than the first business day of the month and no later than the fifth business day of a month following to the month during which the transaction occurred.

The Bank shall report details of transactions to the FINTRACA in the prescribed form as set out in a guideline issued/to be issued by FINTRACA from time to time.

The Bank shall include all details required by FINTRACA in a precise manner.

37. Tipping-off Offences

The Bank, its directors and employees are prohibited from disclosing to a customer or any other person the fact that a report has been submitted under Article (18) of AML & PC law to FINTRACA or any information related to the FINTRACA or to any money laundering or terrorism financing investigation. However, this shall not preclude disclosures or communications between other banks and related professional associations and among directors and employees of the bank in addition to lawyers, competent authorities, and the public prosecution.

If the bank forms a suspicion that transactions relate to money laundering or terrorist financing, the bank shall take into account the risk of tipping-off when performing the customer due diligence process. If the bank reasonably believes that performing the customer due diligence process will tip-off the customer or potential customer, the bank shall abstain from the customer due diligence process, and shall file an STR.

38. Staff Safety

All the staff of the bank, employees, officers and related person's information and details; who conducts/conducted STR, SAR and related investigations & report against a money laundering or terrorist financing suspect shall be protected against disclosing their names and details to any third parties.

No criminal, civil, disciplinary or administrative proceedings for breach of banking or professional secrecy or contract shall lie against the Bank its directors, principals, officers, partners, professionals or employees who in good faith have submitted suspicious reports or provided information to FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

39. New products and business practices

Before launching new products, services and business practices or using new technologies the concerned department shall obtain sign off from Compliance department in the New products, |Services and Technologies approval form by submitting all the relevant supporting documents for their review. The department shall identify, assess and take appropriate measures to manage and mitigate the money laundering or terrorism financing risks that may arise in relation to:

- the development of new products, services and new business practices including new delivery mechanisms for products and services; and
- The use of new or developing technologies for both new and existing products.

40. FATCA (Foreign Account Tax Compliance Act)

The Foreign Account Tax Compliance Act (FATCA) is an important development in U.S on its efforts to combat tax evasion by U.S. persons holding accounts and other financial assets offshore. Reporting under FATCA is not yet applicable in Afghanistan as there is no government level bilateral agreement between US & Afghanistan on exchanging information under FATCA.

41. Internal Policies, Procedures, Systems and Controls

The Chief Compliance Officer and other compliance staff shall have timely access to customer identification data and other CDD information, transaction records, and other relevant information. The Chief Compliance Officer shall have the authority to act independently and to report directly to the Board of Supervisors.

The Board of Supervisors of the Bank shall periodically review the Bank's compliance with the requirements of the Anti-Money Laundering and Proceeds of Crime Law and the DAB's Regulation on AML & PC. Such regular reports to the Board of Supervisors shall include a statement on all suspicious transactions detected, implications and measures taken by compliance staff to strengthen the financial institution's AML/CFT policies, procedures, systems and controls. Reports on suspicious transactions shall be general and not include any information on specific transactions or customers.

The Board of Supervisors shall also be informed of the results of any onsite inspections conducted by Da Afghanistan Bank, including remedial actions required to be implemented by the Bank.

The Bank shall maintain an adequately resourced and independent audit function to ensure that the Chief Compliance Officer and staff of the Bank are performing their duties in accordance with the bank's AML/CFT internal policies, procedures, systems and controls.
The Bank's external auditors shall report on the adequacy of the bank's internal control systems and include an explicit opinion on the Bank's adherence to all applicable local laws, ministerial decisions and Da Afghanistan Bank regulations and Instructions, as well as the Bank's adherence to its own

policies, procedures, systems and controls. This report shall be made available to the Da Afghanistan Bank on request.

The Bank shall establish screening procedures when hiring employees. Such screening procedures shall include fit and proper requirements to be applied when hiring employees. More stringent fit and proper requirements are required for employees in management positions or in positions perceived to have greater exposure to money laundering or terrorist financing. Employee screening procedures and fit and proper requirements shall inter alia ensure that:

1. Employees have the high level of competence necessary for performing their duties as set out in their job descriptions;
2. Employees have appropriate ability and integrity to conduct the business activities of the bank,
3. Potential conflicts of interests are taken into account, including the financial background of the employee;
4. Fit and proper and code of conduct requirements are defined;
5. Persons convicted of offences involving fraud, dishonesty, money laundering or other similar offences are not employed by the bank.

a. Revision, Revival & Approval of the policies

The bank shall revise its policies once in a year or as and when a material change occurs in the AML/CFT laws and regulations of Afghanistan or in the International arena. The policy will be drafted as per the regulations of DAB and relevant regulators; the same shall be put in forth for Board of Supervisors approval prior to submitting the copy to DAB for their review and concurrence.

42. Record Keeping Requirements

The Bank shall maintain records of the following information:

1. Copies of all records obtained through the customer due diligence process under including documents evidencing the identities of customers and beneficial owners, account files and business correspondence, for at least five years after the business relationship has ended or a transaction with a customer who does not have an established business relationship with the bank has been carried out;

2. All records of transactions, domestic and international, attempted or executed for at least five years after:

- the attempt or execution of the transaction;
- the business relationship has ended
- Transaction with a customer who does not have an established business relationship with the bank has been carried out; which is the longest.

3. Such records shall be sufficiently detailed to permit the reconstruction of each individual transaction;

4. Copies of suspicious transactions reports sent and related documents for at least ten years and for other reports and its related documents at least five years after the date the report was made to the FINTRACA;

5. The risk assessment and any underlying information for a period of five years from the date the assessment was carried out or updated.

6. All other necessary information and documents that bank/ relevant department presumes to be necessary including records related to the staff rewards, records of the trainings events such as; attendances, training materials & certificates of participation, staff attendance records etc. for the period of not less than five years.

7. Customer account opening/transaction records wherein there is an enquiry/investigation/court case such records shall be maintained till the case is closed.

The bank shall keep all records in the archives of the bank. Main branch (including VIP hall) & all departments in the head office shall keep their records in the archive department located at head office. Branches shall keep all records as per point 1-5 above, in their branch related archives.

43. Counter Measures on High Risk Countries

The Bank shall implement measures imposed by Da Afghanistan Bank which may include, but are not limited to the following:

- Applying specific elements of enhanced due diligence such as obtaining additional information on the customer, purpose of transactions, nature of the business relationship and the source of funds or wealth of the customer
- Obtaining Senior Management approval to continue the relationship
- Increased monitoring of transactions
- Reviewing, amending or if necessary terminating Correspondent banking relationships.

The Bank shall report any transactions with countries identified under Article 14 paragraph (4) of the AML & PC Law to the FINTRACA.

44. Compliance with CFT Law/Regulation

The Bank shall take the best international practices into consideration for the effective implementation of the Law on Counter Financing of Terrorism, DAB's Regulation on CFT and the management of its functions.

The Bank shall have a system in place that searches and ensures whether any designated person and their associates are into its database immediately after the publication of the list and the freeze orders on the website of the National Security Council and the Official print media.

The Bank shall immediately freeze the properties or funds of designated person in accordance with Article 11 of the Law on Counter Financing of Terrorism and the DAB's Regulation on CFT if it finds such funds or properties while making a search in its database.

When a freeze order issued by the Attorney General Office or a listing of designated person comes to the attention of the Bank it shall, as soon as practicable, conduct a search of its records to determine whether it is holding any property for or on behalf of the person, entity or organization that is the subject of freeze order or the designation.

If, upon conducting a search referred to hereinabove the Bank considers that it is holding funds or property for or on behalf of person, entity or organization that is the subject of freeze order or the designation that is referred to in that freeze order or designation it shall immediately:

- Take steps to ensure that the funds or property frozen pursuant to Article 11 of the Law on Counter Financing of Terrorism and the DAB's Regulation on CFT is secured and that it cannot be dealt with or disposed of in any way;
- Provide the following information to the Financial Intelligence Unit:

  i. particulars of the funds or property frozen;
  ii. Any information known about the ownership or control of the property;
  iii. Details of the steps taken to give effect to the freeze pursuant to Article 11 of the Law on Counter Financing of Terrorism.
- Upon completion of the requirements set out in CFT Law the Bank shall give notice of the implementation of the freeze pursuant to Article 11 of the said law upon any person reasonably believed to have an interest in the frozen property.

The Bank shall also:

- Freeze without delay funds, property and assets held by the Bank including in safe custody, in response to directions received from competent authorities pursuant to the Counter Financing of Terrorism Law;
- Monitor attempted access by customers or other parties to the funds, property or assets;
- Allow access to the funds, property or assets held in response to directions from competent authorities;

- Unfreeze funds, property or assets in response to directions from competent authorities.
- Submit a report without delay to FINTRACA in relation to any attempt to access the funds, property or assets which are subject to an order under the Counter Financing of Terrorism Law.

45. Confidentiality

The Bank and its staff shall maintain confidentiality, and not disclose any information concerning anti-money laundering activities to the clients or to others except to the FINTRACA.

In particular, the Bank shall not disclose to clients that they have filed suspicious transactions reports about their activity. The Bank shall maintain signage in a prominent place and/or hand out written notices to its customers that they are required to report all large cash transactions to the Financial Intelligence Unit. Staff may also orally advise each customer at the time the transaction is initiated.

However, the Bank shall disclose to other financial institutions or to professional associations information about potential clients or transactions which it has refused.

46. Staff Training

The Bank shall ensure adequate training to staff in the requirements of this policy and shall continually update the skills of the staff as per the requirements and change in situations. The training shall include real-world examples of transactions that constituted money laundering and terrorist financing, and an awareness of the role that staff play in the overall process of detecting and punishing money launderers and terrorist financers.

46.1. Content, Scope & Frequency

Compliance department shall provide adequate AML/ CFT & CDD trainings (such as AML/ CFT & CDD laws, regulations, policies, procedures, international best practices & standards) at least annually, to all relevant departments, branch managers, local and provincial branches' staff (based on training

department schedule and plan), compliance officers at head office & branches, respected members of board of supervisors and, board of management.

It shall also provide on the job trainings while visiting the branches.

The HR/ training department shall conduct an assessment (i.e. training need assessment/ TNA) every year as to gather sufficient information about the trainings & to identify all areas where the employees need to be trained and developed.

Induction training to be provided to new hires before they resume responsibility.

All employees of the bank to undergo mandatory Compliance classroom training once in a year.

All trainings are followed by feedback for attendees and assessment. The passing score/percentage is 50%.

47. Employee awareness & preventive actions against Money Laundering & Terrorist financing

The compliance department of the bank shall have the responsibility to enhance the awareness in terms of money laundering, terrorist financing and its prevention. The bank shall ensure that the compliance staff will have sound understanding of AML/CFT laws, rules regulations and international best practices. The bank's compliance department shall have its annual training plan focusing on employee awareness on AML/CFT laws, rules regulations and CDD/EDD measures to prevent money laundering and terrorist financing and mitigate any compliance risk thereof. The bank shall strive to enhance the compliance culture in overall activities of the bank.

48. Cooperation with Law Enforcement

The Bank shall cooperate and coordinate its anti-money laundering activities with FINTRACA and cooperate with the FINTRACA in any freezing or transferring the deposits of clients, according to the relevant provisions in law and regulation.

Annexures

Annexure I. a

EDD Form for MSP, FXD, NGO, NPO, Charitable Trust/ Organization

Enhance CDD for High Risk Customers:
MSP, FXD, NGO, NPO, Charitable Trust/Organizations

Account No:		
Branch Name:		
Title of Account:		
Account Opening Date:		Re-KYC Date:
Establishment date of entity:		

S. No	INFORMATION			
1	Account Type A/c Category (Ind/Corp):	Current ☒	Saving ☐	Fixed Deposit ☐
2	**Principle place of business (Head Office):** House/Apartment: Dis: Street name/No: Province: Country:			
3	**Contact Details:** Phone: Website: Email Address:			
4	**Entity branches (Resident & Non-resident):** Please name entity's branches with addresses. A- Address: B- Address: C- Address:			
5	**What is the Source of fund of customer?**			
6	**Does the customer have any relation with PEPs, if yes please describe?** Yes: ☐ No: ☒			
8	**Nature of Business:**			
9	**Other business details:** Incase if customer has other businesses, please describe: Entity name: Date of establishment: Address:			

COMPLIANCE - The Right Way To Go Page 1 of 3

عزیزی بانک
Azizi Bank

عزیزی بانک
Azizi Bank

12	**Customer is maintaining accounts with other banks:** If YES, please give the following information. a. Bank Name: Account No: b. Bank Name: Account No:
13	**Name of directors and shareholders of the entity: (partnership, Limited liability, NGO/NPO, Public, Charities, Society, Club, Association) others:**

Name	Position	Pass/ TZ No	Address	Nationality	Phone

14	**Turnover of the Customer:** Monthly Turnover: Annual Turnover:
15	**Account risk categories:** Risk level: Reason for risk level:
16	**Documents Obtained:**

S/N	Document Name	Yes/No	Remark
1	Tazkira/Valid Passport.		
2	Proof of address.		
3	TIN Certificate(Individual and Corporate)		
4	Source of Income		
5	License Verification		
6	Board of Resolution Letter		
7	Article of association		
8	Letter from Ministry of Economy For NGO		
9	Others		

17	**Entity/Customer screening in EU, UN and OFAC:** Entity along with related parties is screen out from the list above.
18	**Branch Comment:**

Account Name		Account Number	
Prepared By Branch Compliance Officer/ Zonal Compliance Officer		**Reviewed & Approved By Chief Compliance Officer/ Dy. Chief Compliance officer**	
Name		Name	
Date:		Date:	
Signature		Signature	

Note:
Hard copy of this EDD Form (duly filled & signed) should invariably be retained at compliance Department along with system generated KYC Form for Audit Trail purpose, and it's soft copy be scanned in the archive for easy retrieval purposes.

Annexure I. b

EDD Form for Non-Resident and High Risk other than PEP, NGO/ NPO, MSP, FXD Charitable Trust/ Organization

Enhance CDD for High Risk Customers:
Non Resident and Other High Risk

Account No:			
Branch Name:			
Title of Account:			
Account Opening Date:		Re-KYC Date:	
Establishment date of entity:			

S. No	INFORMATION			
1	**Account Type** **A/c Category (Ind/Corp):**	Current ☒	Saving ☐	Fixed Deposit ☐
2	**Principle place of business (Head Office):** House/Apartment: Dis: Street name/No: Province: Country:			
3	**Contact Details:** Phone: Website: Email Address:			
4	**Category of High Risk:** 1. Non Resident ( ) 2. Bank Staff ( ) 3. Export Import ( ) 4. Others **Please Specify:**			
5	**What is the Source of fund of customer?**			
6	**Does the customer have any relation with PEPs, if yes please describe?** Yes: ☐ No: ☒			
8	**Nature of Business:**			

COMPLIANCE - The Right Way To Go

Page 1 of 3

عزیزی بانک
Azizi Bank

عزیزی بانک
Azizi Bank

9	**Other business details:** Incase if customer has other businesses, please describe: Entity name: Date of establishment: Address:
12	**Customer is maintaining accounts with other banks:** If YES, please give the following information. a. Bank Name: Account No: b. Bank Name: Account No:
13	**Name of directors and shareholders of the entity: (partnership, Limited liability, NGO/NPO, Public, Charities, Society, Club, Association) others:**

Name	Position	Pass/ TZ No	Address	Nationality	Phone

14	**Turnover of the Customer:** Monthly Turnover: Annual Turnover:
15	**Account risk categories:** Risk level: Reason for risk level:
16	**Documents Obtained:**

S/N	Document Name	Yes/No	Remark
1	Tazkira/Valid Passport.		
2	Proof of address.		
3	TIN Certificate(Individual and Corporate)		
4	Source of Income		
5	Valid Visa		
6	Work Primed Card		
7	Others		

17	**Entity/Customer screening in EU, UN and OFAC:** Entity along with related parties is screen out from the list above.
18	**Branch Comment:**

COMPLIANCE - The Right Way To Go

Account Name	
Prepared By Branch Compliance Officer/ Zonal Compliance Officer	
Name	
Date:	
Signature	

Account Number	
Reviewed & Approved By Chief Compliance Officer/ Dy. Chief Compliance officer	
Name	
Date:	
Signature	

Note.
Hard copy of this EDD Form (duly filled & signed) should invariably be retained at compliance Department along with system generated KYC Form for Audit Trail purpose. and it's soft copy be scanned in the archive for easy retrieval purposes.

COMPLIANCE - The Right Way To Go

Annexure I. c

EDD Form for Politically Exposed Person

ENHANCED DUE DILIGENCE FORM FOR PEPs
(POLITICALLY EXPOSED PERSONS)

Account No:		
Branch Name:		
Title of Account (Individual/Corporate)		
Account Opening Date:		Re-KYC Date:

No	INFORMATION	Yes / No
1	**Account holder himself/herself is PEP?**	
	If No in the above, what is the relationship of customer with the PEP? a) Family member b) Close Associate c) Other Relationship **Please Specify:**	
2	**Category of PEP:** a) Politician b) Ambassador c) Civil Worker d) Military Official e) Judiciary Personnel f) Others **Please Specify:**	
3	**In case of politician, what is the current official position of the PEP /or ever held in the past?** a) Senior Executive of State-Owned Entities. b) Provincial Minister, Senior Government Judicial or Military Officials. c) Member National/ Provincial Assembly Senior Politicians. d) Senator. e) All family members of such persons above. f) Close Associate who have business or financial relationship with PEP. g) Others:	
4	**Mention the name of the political party customer is associated with:**	
5	**Beneficial Owner of the account is someone other than the customer himself/herself?**	
	If Yes in the above, provide the below mentioned information regarding beneficial owner of account and please obtain his/her identification documents. Name: Tazkira/Passport Number: Relationship with the Customer:	

COMPLIANCE - The Right Way To Go

6	**Is the account being operated other than the customer?**	
	If Yes in the above, provide the below mentioned information regarding third party authorized person / operator / authorized signatory of the account: Name: Tazkira/Passport: Relationship with the Customer:	
7	**What is the source of income of the customer?** Salary: Business: Others:	
8	**Business details:** In case, a PEP has other business, please obtain below information. Name of the Business: Nature of the business: Address of the business:	
9	**Is the customer referred by Azizi Bank Staff, if yes, mention the name of the bank staff?** Name: Designation:	
10	**Has the customer been screened from EU, UN and OFAC sanction lists?** Please affix OFAC/UNSC Stamp or write the acknowledgement on this form Remark:	
11	**Mention the details of other accounts /financing facilities availed by the customer from Azizi Bank:** a. Bank Name: Account No: b. Bank Name: Account No: c. Bank Name: Account No:	
12	Estimated Monthly Account Turnover: Estimated Annual Account Turnover:	

13 Documents Obtain:

S/N	Document Name	Document Obtain YES or NO	Remark
1	Tazkira / Passport of the Customer Or Beneficial Owner (if any)		
2	Source of income:		
3	PEP Identification:		
4	Source of Wealth proof (Individual/Corporate)		
6	Others if any:		

14	**Branch Comments:**

Address: Zanbaq square, opposite Turkish Embassy, Kabul- Afghanistan
Web-site: www.azizibank.af, www.azizibank.com
E-Mail: info@azizibank.af, customercare@azizibank.af

Account Name		Account Number	
Prepared and recommended by Branch Compliance officer / Zonal Compliance Officer		**Reviewed and Approved by Chief Compliance Officer/Dy. Chief Compliance Officer**	
Name:		Name	
Date:		Date	
Signature		Signature	

Note:
Hard copy of this EDD Form (duly filled & signed) should invariably to be retained by compliance department along with system generated KYC Form for Audit Trail purpose, and it's soft copy be scanned in the archive for easy retrieval purposes.

Address: Zanbaq square, opposite Turkish Embassy, Kabul- Afghanistan
Web-site: www.azizibank.af, www.azizibank.com
E-Mail: info@azizibank.af, customercare@azizibank.af

Annexure II

Account Opening Checklist

Individual Accounts:

NO	Required documents to open the account
1	Original request letter to open a bank account
2	Copy of Tazkira or Valid Passport for Afghans
3	Copy of Passport + Valid Visa and valid work permit for foreigners
4	In case of income source being from business, copy of business license
5	In case of income source being from rent of property, copy of Rent/Lease agreement
6	In case salaried employee, copy of employment letter/Agreement
7	In case custom broker, copy of work permit/license from custom department of MOF
8	In case of Income being from other sources any other valid supporting documents
9	Copy of Proof of address
	Identification & verification requirement
1	Copy of the Tazkira/passport/visa/copy of business license/copy of rent/lease agreement/employment letter(agreement)/work permit/License of customs department of MOF/proof of address and or all KYC documents obtained from the customer shall have the signature of the customer and it must be verified with the original by the officer opening the account and affix the below information a) Date of original sighting b) Name & signature of the bank officer with employee code c) Banks stamp on all the KYC documents

Salary Accounts:

NO	Required documents to open the account
1	Original request letter to open a bank account from the Employer on letter head, signed & sealed
1	Original employer letter on letterhead duly signed & stamped or copy of employee ID card
2	Original approval letter from Salary department (in case list of employees has been provided before, then individual approval is not required)
3	Copy of Tazkira or Valid Passport for Afghans
4	Copy of Passport + valid visa and valid work permit for foreigners
5	Copy of proof of address
	Identification & verification requirement

	Copy of the employee ID/Tazkira/passport/visa /proof of address and or all KYC documents obtained from the customer shall have the signature of the customer and it must be verified with the original by the officer opening the account and affix the below information a) Date of original sighting b) Name & signature of the bank officer with employee code c) Banks stamp on the KYC documents

Minor Accounts:

NO	**Required documents to open the account**
1	Original request letter from the guardian to open a bank account
2	Copy of birth Certificate/Tazkira/Passport
3	Copy of passport with valid visa for foreign citizen
4	Copy of Court letter confirming the custodian of the minor (in case the guardian is other than the father or mother)
5	Copy of Tazkira or valid passport of the Guardian
6	Copy of passport with valid visa of the guardian being a foreign national
7	A letter from the Guardian (Father and Mother) if authorizing any third party in the account to operate (All KYC document to be collected from the father/mother and third party)
8	Copy of Proof of address
	Identification & verification requirement
	Copy of the birth certificate/Tazkira/passport/visa/court letter/visa/ proof of address/ and or all KYC documents obtained from the customer shall have the signature of the customer and it must be verified with the original by the officer opening the account and affix the below information a) Date of original sighting b) Name & signature of the bank officer with employee code c) Banks stamp on the KYC documents

PEP Accounts:

NO	**Required documents to open the account**
1	Original request letter from the guardian to open a bank account
2	Copy of Tazkira or Valid Passport + ID card for Local PEPs
3	Copy of passport with valid visa and valid work permit for Foreign PEPs
4	Enhanced Due Diligence form should be filled and signed by compliance as per Bank Format
5	Original Approval letter from Senior Management (CEO & Dy. CEO or COO in absence of CEO & Dy. CEO)
6	Copy of document for source of income

7	Copy of Proof of address
	Identification & verification requirement
	Copy of the Tazkira/passport/ID card for local pep/ passport + valid visa & work permit for foreign pep/ proof of address/ and or all KYC documents obtained from the customer shall have the signature of the customer and it must be verified with the original by the officer opening the account and affix the below information a) Date of original sighting b) Name & signature of the bank officer with employee code c) Banks stamp on the KYC documents d) EDD form filled & signed e) Approval letter from senior management (CEO & Dy. CEO or COO in absence of CEO & Dy. CEO)

MSP and Money Exchange:

NO	**Required documents to open the account**
1	Original request letter for account opening as per bank format printed on the letter head and should be stamped & signed
2	Copy of license issued by Da Afghanistan Bank (DAB)
3	Copy of TIN certificate (is must)
4	Copy of Tazkira or Valid Passport for Authorized signatories being Afghans
5	Copy of passport + valid visa and valid work permit for Foreigners being Authorized signatories
6	List of branches maintained inside or outside Afghanistan (if any)
7	Approval from Compliance Department before opening account
8	Proof of Address
9	Enhanced Due Diligence form should be filled and signed by compliance as per Bank Format
	Identification & verification requirement
	Copy of the Tazkira/passport/ passport + valid visa & work permit for foreign nationals/ proof of address and or all KYC documents obtained from the customer shall have the signature of the customer and it must be verified with the original by the officer opening the account and affix the below information a) Date of original sighting b) Name & signature of the bank officer with employee code c) Banks stamp on the KYC documents

Sole proprietorship accounts:

No	**Required documents to open the account**

1	Original request for account opening as per bank format printed on the letterhead stamped(in case of no letterhead it can be printed on plain paper and (stamp if any)
2	Copy of Tazkira or valid passport for Afghans
3	Copy of passport +valid visa and valid work permit for foreigners.
4	Copy of License (from ministry of commerce and industry, Municipality or any other authority)
5	In case of foreigner, copy of valid passport along with valid visa and valid work permit.
6	Original sole proprietorship declaration as per bank format (duly signed & stamped)
7	TIN certificate issued ministry of finance.
8	Copy of Proof of address
Identification & verification requirement	
	Copy of the Tazkira/passport/ license/Tin/ passport + valid visa & work permit for foreign nationals/ proof of address and or all KYC documents obtained from the customer shall have the signature of the customer and it must be verified with the original by the officer opening the account and affix the below information a) Date of original sighting b) Name & signature of the bank officer with employee code c) Banks stamp on the KYC documents

Government Entities Accounts:

NO	**Required documents to open the account**
1	Original request letter for Account Opening executed on the official letterhead of the related office (clearly stating that purpose of account opening and introducing authorized signatories with mode of operation) and same should be stamped and signed
2	Original approval letter from Treasury Department of MOF of Afghanistan (In provinces, approval letter from the governor of the concern province and finance department)
3	Original board Resolution in official letterhead signed & stamped for authorizing the Signatories
4	Copy of Tazkira or Valid Passport for Authorized signatories being Afghans + employee

	ID cards
5	Copy of address proof for Authorized signatories
Identification & verification requirement	
	Copy of the Tazkira/passport/ passport + valid visa & work permit for foreign nationals/ proof of address and or all KYC documents obtained from the customer shall have the signature of the customer and it must be verified with the original by the officer opening the account and affix the below information d) Date of original sighting e) Name & signature of the bank officer with employee code f) Banks stamp on the KYC documents Approval letter from senior management to be obtained

Company / Business Accounts:

NO	**Required documents to open the account**
1	Original request letter for account opening printed on the letterhead of the company matching the company's name on the license and should be stamped & signed by the authorized signatory.
2	Original Board Resolution (in case of a foreign firm, attested copy of the board resolution by the relevant embassy and ministry of foreign Affairs Afghanistan) on company letterhead with signature and stamp
3	Copy of valid license (MOCI and or from the Relevant ministry) (In case the license renewal is under process then an original letter to that effect from relevant authority proving the same)
4	
5	Tazkira or passport copies of the shareholders, signatories and directors
6	In case of locals, Tazkira Or Passport of the authorized signatories and they should be physically present (in case anyone of them is outside Afghanistan, letter from the absent person, issued by him/ her duly attested by concern embassy and MOFA of Afghanistan Same letter should also contain transfer of authority to another person who resides inside Afghanistan. Or in case he is in other city of Afghanistan he can be verified through Azizi Bank nearest branch, and his signature can be obtained once he returns Back)
7	In case of foreigner copy of valid passport along with valid visa and valid work permit of the authorized signatories.
8	Copy of Articles of Association and Memorandum of Association (if any)
9	Copy of Tin
10	Copy of Proof of address
Identification & verification requirement	
	Copy of the Tazkira/passport/ passport + valid visa & work permit for foreign nationals/license/Memorandum & Articles of association/ proof of address and or all KYC documents obtained from the customer shall have the signature of the customer and it must be verified with the original by the officer opening the account and affix the below information

	a) Date of original sighting b) Name & signature of the bank officer with employee code c) Banks stamp on the KYC documents

Accounts of corporation:

NO	Required documents to open the account
1	Original request for account opening printed on the letterhead of the company matching the company's name on license and should be stamped & signed by the authorized signatory
2	Original Board Resolution (in case of a foreign firm, attested copy of the board resolution by the relevant embassy and ministry of foreign Affairs Afghanistan) on company letterhead with stamp & signature from authorized signatory
3	Copy of valid license (from Relevant ministry) (In case the license renewal is under process then an original letter to that effect from relevant authority proving the same)
5	Tazkra or passport copies of the shareholders and (Directors if any)
6	In case of locals, Tazkera or Passport of the authorized signatories and they should be physically present (in case anyone of them is outside Afghanistan, letter from the absent person, issued by him/ her duly attested by concern embassy and MOFA of Afghanistan Same letter should also contain transfer of authority to another person who resides inside Afghanistan. Or in case he is in other city of Afghanistan he can be verified through Azizi Bank nearest branch, and his signature can be obtained once he returns Back)
7	In case of foreigner copy of valid passport along with valid visa and valid work permit of the authorized signatories.
8	Copy of Memorandum and Articles of Association (if any)
9	Copy of proof of address
	Identification & verification requirement
	Copy of the Tazkira/passport/ license/Memorandum and articles of association/passport + valid visa & work permit for foreign nationals/ proof of address and or all KYC documents obtained from the customer shall have the signature of the customer and it must be verified with the original by the officer opening the account and affix the below information d) Date of original sighting e) Name & signature of the bank officer with employee code f) Banks stamp on the KYC documents

NGO/Association Accounts:

NO	Required documents to open the account
1	Original request letter for account opening printed on the letterhead of the organization matching the organization's name on license and should be signed & stamped.

2	Original Board resolution (in case of a foreign firm, attested copy of the board resolution by the relevant embassy and ministry of foreign Affairs Afghanistan) on company letter head with sign & stamp
3	Copy of Valid license issued from the relevant issuing authority.
4	List of directors (with their details / particulars like title / positions etc.) attested by relevant ministry.
5	In case of local, Tazkira or passport of the authorized signatories and they should be physically present (in case anyone of them is outside Afghanistan, letter from the absent person, issued by him/ her, duly attested by concern embassy and MOFA of Afghanistan. Same letter should also contain transfer of authority to another person who resides inside Afghanistan. Or in case he is in other city of Afghanistan he can be verified though Azizi Bank nearest branch, and his signature can be obtained once he returns bank)
6	In case of foreigner copy of valid passport along with valid visa and valid work permit of the authorized signatories.
7	Copy of Memorandum & Articles of association
8	Copy of Tazkira or passport copies of the directors (visa & work permit for foreign nationals)
9	Article of association copy of the NGO duly Certified from the issuing authority.
10	Copy of Proof of address
11	Prior approval from compliance before opening the account
	Identification & verification requirement
	Copy of the Tazkira/articles of association/passport/ passport + valid visa & work permit for foreign nationals/ proof of address and or all KYC documents obtained from the customer shall have the signature of the customer and it must be verified with the original by the officer opening the account and affix the below information a) Date of original sighting b) Name & signature of the bank officer with employee code c) Banks stamp on the KYC documents

Social institution

No	Required documents to open the account
1	Original request letter for account opening as per bank format printed on the letterhead signed & stamped(in case of no letterhead it can be printed on plain paper with signature and (stamp if any)
2	Copy of Tazkira or valid passport for Afghans
3	Copy of passport +valid visa and valid work permit for foreigners.
4	Copy of License from relevant ministry
5	In case of foreigner, valid passport along with valid visa and valid work permit.
6	TIN certificate issued ministry of finance.
7	Copy of Proof of address
Identification & verification requirement	
	Copy of the Tazkira/passport/license/ passport + valid visa & work permit for foreign nationals/ proof of address and or all KYC documents obtained from the customer shall have the signature of the customer and it must be verified with the original by the officer opening the account and affix the below information a) Date of original sighting b) Name & signature of the bank officer with employee code c) Banks stamp on the KYC documents Approval letter from senior management to be obtained

Tourist Companies:

No	Required documents to open the account
1	Original request for account opening as per bank format printed on the letterhead stamped(in case of no letterhead it can be printed on plain paper and (stamp if any)
2	Copy of Tazkira or valid passport for Afghans

3	Copy of passport +valid visa and valid work permit for foreigners.
4	Copy of License from relevant ministry
5	In case of foreigner, copy of valid passport along with valid visa and valid work permit.
6	Copy of TIN certificate issued ministry of finance.
7	Copy of Proof of address
Identification & verification requirement	
	Copy of the Tazkira/license/tin/passport/ passport + valid visa & work permit for foreign nationals/ proof of address and or all KYC documents obtained from the customer shall have the signature of the customer and it must be verified with the original by the officer opening the account and affix the below information a) Date of original sighting b) Name & signature of the bank officer with employee code c) Banks stamp on the KYC documents Approval letter from senior management to be obtained

Embassies

No	Required documents to open the account
1	Original request for account opening as per bank format printed on the letterhead stamped
3	Copy of passport +valid visa and valid work permit for foreigners/signatories
4	Official letter from relevant embassy
5	Copy of valid passport along with valid visa and Employee ID Card
7	Copy of Proof of address of authorized Signatories
Identification & verification requirement	
	Copy of passport + valid visa proof of address and or all KYC documents obtained from

	the customer shall have the signature of the customer and it must be verified with the original by the officer opening the account and affix the below information a) Date of original sighting b) Name & signature of the bank officer with employee code c) Banks stamp on the KYC documents Approval letter from senior management to be obtained

Notes:

- Any deviations from the above policies must have an approval from compliance department
- All CDC's (Community Development Council) and sub-accounts opening are subject to operation policy.
- Accounts which are not listed in this circular will require further approval/ clearance from Compliance Department.

Annexure III

LCTR Form / Third Party Form

1. **Deposited by Bank Customer (AZB Account Holder):** ☐ Date: ...../...../.....

Branch Name: ..... **Branch Code:** .....

Depositor Name: ..... **Depositor CIF or A/C No:** .....

Name of Account Holder	Account Number	Deposit/Transfer Amount

Purpose of Deposit/ Transfer:

.....
.....

عزیزی بانک
Azizi Bank

Supporting Documents Taken as Source of fund:

.....

2. Deposited by Walk – in Customers (Non A/C holder): ☐

In case transaction performed by Non AZB account holder (Walk-in Customers) below information should be obtained for all transactions above 500,000 AFN and equivalent in other currencies.

Name: ..... **Father's Name:**
.....

TZ/Passport No: ..... **Date of Birth:**
.....

Phone No: ..... **Full Address:**
.....

Customer screened in OFAC/ UN, HMT, EU, Fin TRACA & DAB sanction lists: ☐

Acknowledged that all above information which I provided are accurate and confirmed:
Customer Signature: .....

3. **Clarify the relationship of the depositor and Account holder:**
.....
.....

4. **Declare beneficial ownership of the fund,** (if the fund belongs to the someone else kindly obtain the below information):

Individual:

Name: ..... Father Name: ..... TZ No: ..... Phone No: .....

Corporate:

Comp Name: ..... License No: .... TIN: ..... Phone No: .....

Note: The particulars of all large cash transactions (Deposits/ withdrawals/remittances etc. in excess of AFN 1,000,000 or equivalent in other currencies) are required under Afghanistan AML/ CFT regulation to be reported to the financial intelligence unit.

Acknowledged that all above information which I provided are accurate and confirmed:
Customer's Signature.....

Annexure IV

Compliance Checklist for Outgoing/ outward SWIFT Payments

No	Information/Document Title	Afs ≥500,000/ USD ≥7,500	Afs ≤500,000/ USD ≤7,500
1	**Ordering Customer (Sender) Details on TT form**	**Status**	**Status**
	✓ Source of Fund/Income	Must	Must
	✓ Name/Account Title "as per system & ID/License"	Must	Must
	✓ Account number	Must	Must
	✓ Proper & update address "area, dis, province & country"	Must	Must
	✓ Date of Birth (DOB) "as per customer valid TZ/PP"	Must "In case of Individual"	Must "In case of Individual"
	✓ Place of Birth & Nationality	Must "In case of Individual"	Must "In case of Individual"
	✓ Tazkira or Valid Passport No	Must "In case of Individual"	Must "In case of Individual but priority to be given to passport"
	✓ Established Date "as per business license"	Must "In case of Corporate"	N/A
	✓ Business license Number	Must "In case of Corporate"	Must "In case of Corporate"
	✓ Place & Date of Issue & Expiry	Must "In case of Corporate"	Must "In case of Corporate"
	✓ Valid/Active Phone Number	Must	Must
	✓ Email address	Shall be obtained(if available)	Shall be obtained(if available)
2	**Beneficiary (Receiver) on TT form as per (Invoice)**		
	✓ Beneficiary Full Name without Abbreviation as per Business license & Invoice "in case of abbreviation on license, proper clarification must be provided by on letter stamped letter head of beneficiary or by official email"	Must	Must

	✓ Beneficiary Proper & update address "area, dis, province & country"	Must	Must
	✓ Beneficiary account name as per business license & Invoice	Must	Must
	✓ Beneficiary account number, swift code	Must	Must
	✓ IFSC, IBAN, Sort Code, Transit Number, BLZ Code, BSB Number, INN & KPP, BIN Number, Routing Number/BIC	As per beneficiary country	As per beneficiary country
	✓ Email, website & contact number	Must	Shall be obtained(if available)
3	**Beneficiary Bank Details**		
	✓ Full Name without Abbreviation	Must	Must
	✓ Full Address "area, dis, province & country"	Must	Must
4	**Other**		
	✓ Customer Signature & Stamp " on TT form	Must	Must
	✓ Customer signature wherever correction is don on TT form	Must	Must
5	**Supporting Document for a Wire Transfer**		
5.1	**Invoice: Invoice must include below information**		
	✓ Logo	Must	Must
	✓ Full Name & Address of issuer/Seller	Must	Must
	✓ Email & website	Must	Shall be obtained(if available)
	✓ Contact Number	Must	Shall be available(if available)
	✓ Fax Number	Optional	Optional
	✓ Invoice Number	Must	Must
	✓ Invoice Date	Must	Must
	✓ Invoice Due Date/Expiry Date	If any "must be valid" invoice after six month is not acceptable	If any "must be valid" invoice after six month is not acceptable
	✓ Currency	Must	Must
	✓ Goods/Service Description	Must	Must
	✓ Quantity of Goods/Items	Must	Must
	✓ Amount "unit price & Total"	Must	Must
	✓ Payment Terms and Condition "In case of partial payment	Must	Must
	✓ Full Name of buyer/consignee "as per business license and System account name"	Must	Must
	✓ Stamp of both seller & buyer	Must	Must

5.2	**Contract/Agreement: Containing below points**	As applicable	As applicable
	✓ Name of buyer & Seller	Must	Must
	✓ Contract Start Date & expiry Date	Must	Must
	✓ Terms of Agreement "Payment terms, delivery, quantity..."	Must	Must
	✓ Stamp & Signature of Seller & Buyer	Must	Must
5.3	**Custom Document & Bill of Lading**		
	✓ Custom document & Shipment document "Bill of lading, airway bill, Rail Freight, Consignment Note, Tracking Bill" of the particular payment	Should be obtained at the time of payment. In case of advance payment, it should be obtained before the next payment is processed for same customer. Customers may be allowed for maximum 5 payments subject to proper justification & genuine reason. Beyond 5 transactions if documents are not available and any payment to be processed the same to be referred to Compliance.	Should be obtained at the time of payments. In case of advance payment, it should be obtained before the next payment is processed for same customer. Customers may be allowed for maximum 5 payments subject to proper justification & genuine reason. Beyond 5 transactions if documents are not available and any payment to be processed the same to be referred to Compliance.
5.4	**Goods Related document**	Optional	Optional
	✓ Certificate of Origin	If available	If available
	✓ Certificate of Quality	If available	If available
	✓ Packing List	If available	If available
	✓ Insurance Document	If available	If available
5.5	**Beneficiary Identity**		
	✓ Business license/Registration Certificate	If available(in exceptional cases)	If available(in exceptional cases)
	✓ Type of business	If available(in exceptional cases)	If available(in exceptional cases)
5.6	**Document for Individuals**		
	✓ Sufficient supporting document for source of fund " more than limit of 7500 USD"	Must	Must
	✓ Copy passport for Beneficiary	To be obtained(In case of sanction match)	To be obtained(In case of sanction match)
	✓ Visa, ID	To be obtained(as	To be obtained(as

		applicable)	applicable)
	✓ Supporting document for purpose of payment	To be obtained(basis the purpose of payment)	To be obtained(basis the purpose of payment)

Annexure V. a

Compliance checklist for reviewing Term loan & Overdraft

Azizi bank **Compliance Department** Checklist for reviewing Term loan & Overdraft		
1	**Application Form**	Loan Application Letter
		The application form must be fully completed, signed and dated Via Loan Applicants.
2	**Business Loan Appraisal Form**	Complete description of business and promoters
		All information mentioned in the appraisal form should be proper and factual. The information given in appraisal form should be checked with supplementary docs provided by customers and obtained by credit department of the bank
		MPBF should be worked out properly
		Purpose of Loan should be clear / justifiable
		Company Major Buyers and suppliers of raw materials / finished goods
		Industry and borrower company's market (financial growth, business growth) position
		Position of the limit regarding prudential exposure limit of DAB (Da Afghanistan Bank)
		Approval of the Discretionary Authorities (CCO, Credit Committee, BOS)
		Supported by pre-renewal/sanction inspection reports
		Securities and Personal Guarantees as per practices in place
		Nature of business, line of activity, specialization of the company
		In case of renewal, irregularities found by DAB/ Risk Management Department & Corrective action taken
3	**Regd Documents**	Company License{Updated}
		Assas Nama , Article of Association/ By the Company law.
		Annual Income Tax Returns and or Tax Clearance Letters of MOF
		Copies of all Regd Documents Should be Signed by Customer
4	**Invoices/ Contracts**	Copy of contracts and projects.

		Invoices of sales and purchases
		Custom documents
5	**Bank Statements**	Require one year of personal and business bank statements to be submitted as part of a loan package.
6	**Reports**	Property Evaluation Reports
		Latest Audited & Projected Financial Statements/ reports as per practice in place
7	**Legal**	Collateral document that describes cost/value of personal or business property that will be used to secure a loan, as per Credit Policy
		Legal Opinion of legal Advisor
	Documents	Property Deeds (Qabala-Waseqa-Wakalatnama etc.)
		Azizi Bank's letters to court and court confirmation bai-e-jaize via letter
		Report from the security department as per practice
8	**No Dues certificates**	No-dues certificate from other banks/ PCR Reports
9	**KYC Documents & Forms**	Tazkira/ Passport/ ID Docs of promoters
		AOF & CIFs (Individual & Corporate)
		TIN & Proof of address of the promoters
		Copies of all KYC Documents Should be Signed by Customer

Annexure V.b

Compliance Checklist for the review of Bank Guarantees (including CBGs) > 50,000 USD (or equivalent in other currencies)

Compliance Department
Head Office, Kabul – Afghanistan

Compliance Checklist for Due Diligence of Bank Guarantees (Including CBGs) equal to or greater than 50,000 USD (or eq. in other currencies)

The dedicated compliance officer to credit department has to review & check for the followings;

1. Review & ensure that KYC due diligence has been performed on the counter bank in case of CBG
2. Review dully filled appraisal form for BGs with USD ≥ 50,000 (or equivalent in other currencies).
3. Review & ensure that update KYC has either been ensured/ obtained from customer at the time of issuing BG (s) i.e. update business license, article of association/ by-law, Tazkira/ update Passport of the applicant (in case individual), promoters (owners) & authorized persons.

4. Review & ensure that BG/ CBG application has been issued & processed by company's authorized person (s) (i.e. president, vice president, account authorizer etc.)

5. Review & ensure that Sanction Screening has been performed on the applicants and its promoters/ owners & authorized persons, beneficiary & guarantor (s) against sanction lists.

6. Review and ensure that Credit department has ensured for the related parties and the BG is issued within exposure limit set and prescribed by DAB (per party 15% of RC of the bank).

7. Review copies of Projects, Contracts and Acceptance Letter

8. Review availability of Risk department assessment report as & when required as per policy

Note:

2. Compliance department will not review Financial reports & Financial Statements analysis of the BG's applicants
3. Documents required under the checklist of risk management department are waived under compliance checklist in order to avoid duplication.

Annexure V. c

Compliance Checklist for Due Diligence of LCs & FOBCs

The dedicated compliance officer to credit department has to review & check for the followings;

1. Sanction Screening as per compliance requirements, on all parties involved (applicant, beneficiary, advising bank, issuing bank, confirming bank, negotiating bank or any other party involved). In case of applicant (who is Azizi bank customer), the sanction screening should be performed on the applicant, its promoters/ owners & authorized persons.
2. Update KYC of the applicant at the time of issuing FOBC (s)/ LC (s) i.e. update business license, article of association/ by-law, Tazkira/ update Passport of the applicant (in case individual), promoters (owners) & authorized persons

3. Review & ensure that FOBC/ LC application has been issued & processed by company's authorized person (s) (i.e. president, vice president, account authorizer etc.)
4. Review & ensure that following documents have been obtained;
   a) Proper Bill of Exchange
   b) Invoice (Proper format)
   c) Packing list
   d) Description of consignment
   e) Proper Bill of lading/AWB
   f) Proper Contract
   g) ACCD (Afghanistan Custom Clearance Document)

عزیزی بانک
Azizi Bank

Reviewed & Recommended by Chief Compliance Officer for Approval of BOS

Mr. Ravi Ramani Iyer
Chief Compliance Officer

Approved by the Board of Supervisors in their meeting Dated 28.12.2020

Mr. Sundaram Prabhu
Chairman of the Board of Supervisors